ETSI TR 102 862 V1.1.1 (2011-12)

Technical Report

Intelligent Transport Systems (ITS); Performance Evaluation of Self-Organizing TDMA as Medium Access Control Method Applied to ITS; Access Layer Part

Reference

DTR/ITS-0040021

Keywords

ITS, MAC, TDMA

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Intelligent Transport System (ITS).

Introduction

By introducing wireless communications between vehicles and between vehicles and road infrastructure or other fellow road users such as pedestrians and bicyclists, the road environment will become safer and potentially more environmentally friendly. Many different cooperative intelligent transport systems (ITS) applications have been suggested for the vehicular environment, both for road traffic safety and efficiency. Depending on application area, the resulting communication requirements are quite diverse. Different wireless access technologies have different features and different benefits and all cooperative ITS applications suggested for the vehicular environment cannot be solved with one single technology due to resource constraints and diverse requirements. Vehicular *ad hoc* networks (VANETs) based on, e.g. IEEE 802.11p [i.2], will be used for road traffic safety applications, [i.1], [i.2]. However, other wireless carriers such as cellular technology (e.g. 3G, LTE) will also be used to support different cooperative ITS applications in general.

The major difference between VANETs and cellular technology is that there is no central controller in the former. The central controller usually has perfect knowledge about the nodes within range and it can distribute and optimize the available resources. However, in cellular technology there is a central controller in the form of a base station present, otherwise communication is not possible. VANETs do not need coverage by base stations - instead if there is someone to communicate with, communication will take place directly in between any two nodes within range of each other. The *ad hoc* structure is advantageous, since it does not require coverage by base stations, but without a central control mechanism, problems with scalability may arise. Due to the lack of a central coordinator, all nodes typically transmit on a common frequency channel. This frequency channel, called the control channel, is known *a priori* to all nodes. For road traffic safety applications, this channel is where the most important data will be transmitted. To facilitate additional cooperative ITS applications with higher bandwidth requirements, two or more service channels are also available. However, the control channel is the core of a VANET.

Many emerging road traffic safety applications will be based purely on broadcast communication, [i.3], i.e. one-to-many. Due to the broadcast communication, the assurance of sufficient reliability is limited. A sender does not know if the transmitted data has arrived at the intended receiver because no acknowledgments of successful reception are possible in broadcast mode (receivers cannot send an acknowledgment to the sender since the number of intended receivers is not known and this may flood the network). One way to increase the reliability in broadcast mode is instead to repeat the same message several times.

Ultimately, cooperative ITS applications for enhancing road traffic safety should be designed taking the characteristics of a VANET into account. These characteristics can be summarized by: a decentralized network topology, a common control channel and broadcast as the preferable communication mode. The utilization of the control channel should be carefully designed so it can be used to its maximum. The medium access control (MAC) protocol schedules access to the shared control channel. A MAC protocol suitable for road traffic safety applications in VANETs should be decentralized such that it functions without a central controller, it should support broadcast such that channel access is fair and predictable for all participating nodes and it should aim to minimize interference between transmitters to maximize scalability. Further, as road traffic safety typically involves interaction with vehicles located in the vicinity of each other, the MAC method should maximize the packet reception probability for the closest neighbouring nodes.

ETSI has standardized a VANET protocol based on a profile of IEEE 802.11p [i.2], called ITS-G5 [i.1], which uses the MAC method carrier sense multiple access (CSMA). CSMA has some of the desired properties, i.e. it is decentralized and aims at minimizing interference between any transmitters. However, it does not necessarily maximize the packet reception probability for the closest neighbouring nodes or provide fair and predictable channel access for broadcast. The present document therefore scrutinize time slotted MAC protocols, to determine if these can utilize the common control channel more efficiently than the current proposed MAC from IEEE 802.11p [i.2].

1 Scope

The present document describes the use of time slotted MAC algorithms in VANETs. Two specific MAC methods, self-organizing time division multiple access (STDMA) and mobile slotted Aloha (MS-Aloha), are described in detail, not excluding other time slotted approaches. Time slotted approaches are suitable for road traffic safety applications as the maximum delay is predictable and channel access can be made fair among all participating nodes even during broadcast. However, time slotted approaches do require synchronization between nodes to build a common framing structure for transmissions, something that is not needed for non-time slotted approaches, e.g. CSMA as used by ITS G5 [i.1]. In the literature of time slotted MAC protocols for VANETs, synchronization is provided by a global navigation satellite system (GNSS) such as the global positioning system (GPS) or Galileo. The present document also describes the GNSS synchronization issue as well as proposals for dealing with synchronization when the GNSS signal is absent or weak, which can occur in urban environments and tunnels. Further, time slotted approaches use fixed-length time slots for transmissions, implying that packet lengths are fixed. However, as the physical (PHY) layer suggested for VANETs offers several transfer rates, this means that different packet sizes can be obtained in the fixed time slots. The analysis of the most preferable configuration in this context constitutes the second technical topic covered by the present document. Finally the present document also deals with the coexistence between CSMA and time slotted MAC approaches nodes. The backward compatibility and coexistence are of crucial importance since the first generation of VANETs will use CSMA technology. This represents the third and final topic of the present document.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI ES 202 663: "Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band".

[i.2] IEEE 802.11p: 2010: "IEEE Standard of Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements; Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications; Amendment 6: Wireless Access in Vehicular Environments".

[i.3] ETSI TR 102 638: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions".

[i.4] IEEE 802.11: 2007: "IEEE Standard of Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements; Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[i.5] ETSI TS 102 637-3: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service".

[i.6] ETSI TS 102 637-2: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service".

[i.7] ETSI TR 101 683: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; System Overview".

[i.8] ETSI TS 102 687: "Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part".

[i.9] ITU-R Recommendation M.1371-1:2001: "Technical characteristics for universal shipborne automatic identification system using time division multiple access in the VHF maritime mobile band".

[i.10] F. Tobagi, and L. Kleinrock, "Packet switching in radio channels: Part II - the hidden terminal problem in carrier sense multiple access and the busy tone solution", IEEE Transactions on Communications, vol. 23, no. 12, pp. 1417-1433, December, 1975.

[i.11] H. Lans, "Position Indicating System", US patent 5,506,587, issued 1996.

[i.12] ITU-T std G.811, G812, G.813; series G: "Transmission systems and media digital transmission systems - digital networks - design objectives for digital networks".

[i.13] S. Ganeriwal, R. Kumar, and M.B. Srivastava, "Timing-sync protocol for sensor networks", in Proc. of the 1st ACM Int. Conf. on Embedded Networked Sensor Systems (SenSys '03), Los Angeles, CA, USA, pp. 138-149, 2003.

[i.14] D. Mills, "Internet time synchronization: the network time protocol", in IEEE Transactions on Communications, vol. 39, no. 10, pp. 1482-1493, Oct. 1991.

[i.15] M. Maroti, B. Kusy, G. Simon, and Á. Lédeczi, "The flooding time synchronization protocol", in Proc. of the 2nd ACM Int. Conf. on Embedded Networked Sensor Systems (SenSys '04), Baltimore, Maryland, USA, Nov. 2004, pp. 39-49.

[i.16] J. Elson, L. Girod, and D. Estrin, "Fine-grained network time synchronization using reference broadcasts", in Proc. of OSDI '02 the 5th ACM Symp. on Operating Systems Design and Implementation, Boston, MA, USA, Dec. 2002, pp. 147-163.

[i.17] L. Schenato and G.Gamba, "Distributed consensus protocol for clock synchronization in wireless sensor network", in Proc. of the 46th IEEE Conf. on Decision and Control, New Orleans, LA, USA, Dec. 2007, pages 2289-2294.

[i.18] P. Hightower, "Motion effects on GPS receiver time accuracy", Instrumentation Technology Systems, 2008.

[i.19] B. Hoogvelt, N. Asseldonk, and R. Henny, "Measurement technology for a calibrating vehicle for multiple sensor weigh-in-motion system", in Proc. of 8th Int. Symp. on Heavy Vehicle Weights and Dimensions, Johannesburg, South Africa, March 2004.

[i.20] P. J. Mumford, "Relative timing characteristics of the one pulse per second (1PPS) output pulse of three GPS receivers", in Proc. 6th International Symposium on Satellite Navigation Technology Including Mobile Positioning & Location Services, Melbourne, Australia, July 2003.

[i.21] M. A. Lombardi, "The Use of GPS Disciplined Oscillators as Primary Frequency Standards for Calibration and Metrology Laboratories", in the Journal of Measurement Science, 2008.

[i.22] N.C. Helsby, "GPS disciplined offset-frequency quartz oscillator", in Proc. of the 2003 IEEE Int. Frequency Control Symp. and PDA Exhibition in conjuncation with the 17th European Frequency and Time Forum, Piscataway, NJ, USA, May 2003, pp. 435-439.

[i.23] J.A. Davis and J.M. Furlong, "Report on the study to determine the suitability of GPS disciplined oscillators as time and frequency standards traceable to the UK national time scale UTC(NPL)", in National Physical Laboratory Report CTM 1, June 1997.

[i.24] B.M. Penrod, "Adaptive temperature compensation of GPS disciplined quartz and rubidium oscillators", in Proc. of the 1996 IEEE 50th Int. Frequency Control Symposium, Honolulu, Hawaii, USA, June 1996, pp. 980-987.

[i.25] Research and Innovative Technology Administration (RITA), U.S. Department of Transportation, Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System, 2001.

[i.26] M.A. Lombardi, "Comparing LORAN timing capability to industrial requirements", in Proc.of the 2006 Int. Loran Association (ILA)meeting, 2006.

[i.27] T. Shioda, Y. Sekine and H. Otsuka, "High precision TCXO for rapid environmental temperature change", in Proc. of the 2003 IEEE Int. Frequency Control Symp. and PDA Exhibition in conjuncation with the 17th European Frequency and Time Forum, Piscataway, NJ, USA May 2003, pp. 444-449.

[i.28] U.L. Rohde and A.K. Poddar, "A novel voltage controlled crystal oscillator circuit", in Proc. of IEEE 13th Int. Symp. on Consumer Electronics (ISCE), Kyoto, Japan, May 2009, pp. 329-333.

[i.29] M. Rao, L. Lo Presti and J. Samson, "Improved GNSS positioning exploiting a vehicular P2P infrastructure", in Proc. of IEEE 5th Advanced Satellite Multimedia Systems Conf. and the 11th Signal Processing for Space Communications Workshop (ASMA/SPSC), Cagliari, Italy, Sept. 2010.

[i.30] M. Rao, L. Lo Presti and J. Samson, "Peer-to-peer equation augmentation for an altitude aided GNSS receiver", in Proc. of the IEEE 72nd Vehicular Technology Conference Fall (VTC 2010-Fall), Ottawa, ON, Canada, Sept. 2010.

[i.31] H.A. Cozzetti and R. Scopigno, "RR-Aloha+: a slotted and distributed MAC protocol for vehicular communications", in Proc. of the 1st IEEE Vehicular Networking Conference (VNC 2009), Tokyo, Japan, Oct. 2009.

[i.32] R. Scopigno and H. A. Cozzetti, "Mobile Slotted Aloha for VANETs", in Proc. of the IEEE 70th Vehicular Technology Conference (VTC Fall 2009), Anchorage, Alaska, USA, Sept. 2009.

[i.33] H.A. Cozzetti, R. Scopigno, L. Casone and G. Barba, "Comparative analysis of IEEE 802.11p and MS-Aloha in VANETs scenarios", in Proc. of the 2nd IEEE Int. Workshop on Vehicular Networking (VON 2009), Biopolis, Signapore, Dec. 2009.

[i.34] R. Scopigno and H.A. Cozzetti, "Evaluation of time-space efficiency in CSMA/CA and slotted Vanets", in Proc of the IEEE 71st Vehicular Technology Conference (VTC Fall 2010), Ottawa, Canada, Sept. 2010.

[i.35] R. Scopigno, and A. Cozzetti, "Signal shadowing in simulation of urban vehicular communications", Proc. of the 6th Int. Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, Sept. 2010.

[i.36] H.A. Cozzetti, A.Vesco, F.Abrate, R.M. Scopigno, "Improving Wireless Simulation Chain: Impact of Two Corrective Models for VANETs", in Proc. of the 2nd IEEE Vehicular Networking Conference (VNC 2010), Jersey city, New Jersey, USA, Dec. 2010.

[i.37] H.A. Cozzetti and R. Scopigno, "Scalability and QoS in slotted VANETs: forced slot re-use vs pre-emption", in Proc of the 14th Int. IEEE Conf. on Intelligent Transportation Systems (ITSC 2011), Washington, DC, USA, Oct. 2011.

[i.38] S. Makido, N. Suzuki, T. Harada, and J. Muramatsu, "Decentralized TDMA protocol for real-time vehicle-to-vehicle communications", in The Information and Processing Society of Japan (IPSJ) Journal, vol. 48, no. 7, pp. 2257-2266, 2007.

[i.39] Y. Tadokoro, K. Ito, J. Imai, N. Suzuki, and N. Itoh, "Advance transmission cycle control scheme for autonomous decentralized TDMA protocol in safe driving support system", in Proc. of the IEEE 2008 Intelligent Vehicles Symposium, Eindhoven, Holland, June 2008.

[i.40] M. Lenobl, K. Ito, Y. Tadokoro, M. Takanashi, and K. Sanda, "Header reduction to increase the throughput in decentralized TDMA-based vehicular networks", in Proc. of the 1st IEEE Vehicular Networking Conference (VNC 2009), Tokyo, Japan, Oct. 2009.

[i.41] L. Pilosu, F. Fileppo, and R. Scopigno, "RADII: a computationally affordable method to summarize urban ray-tracing data for VANETs", in Proc. of the 7th Int. Conf. on Wireless Communications, Networking and Mobile Computing (IEEE WiCOM 2011), Wuhan, China, Sept. 2011.

[i.42] IEEE 1609.4: "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation", Feb. 2011.

[i.43] ETSI TR 102 861: "Intelligent Transport Systems (ITS); STDMA recommended parameters and settings for cooperative ITS".

[i.44] 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.

[i.45] K. Sjöberg-Bilstrup, E. Uhlemann, E. Ström, and U. Bilstrup, "On the ability of the IEEE 802.11p MAC method and STDMA to support real-time vehicle-to-vehicle communication", in EURASIP Journal on Wireless Communications and Networking, vol. 2009, 13 pages, doi: 10.1155/2009/902414.

[i.46] K. Sjöberg-Bilstrup, E. Uhlemann, and E. Ström, "Scalability issues of the MAC methods STDMA and CSMA of IEEE 802.11p when used in VANETs", in Proc. of the ICC'10 Workshop on Vehicular Connectivity, Cape Town, South Africa, May 2010.

[i.47] K. Sjöberg, E. Uhlemann, and E. Ström, "Delay and interference comparison of CSMA and self-organizing TDMA when used in VANETs", in Proc. of the 7th Int. Wireless Communications and Mobile Computing Conference (IWCMC), Istanbul, Turkey, July 2011.

[i.48] L.Garelli, C.Casetti, C.F.Chiasserini, M.Fiore, "MobSampling: V2V Communications for , Traffic Density Estimation", in Proc. of the 2011 IEEE 73rd Vehicular Technology Conference, (VTC2011-Spring), Budapest, Hungary, May 2011.

[i.49] R. Kjellberg, "Analysis of an AIS Implementation in Tokyo Bay", Analyse Report.

NOTE: Available at http://www.gpc.se/tokyo/tokyo.htm.

[i.50] K. Sjoberg, E. Uhlemann, and E.G. Ström, "How sever is the hidden terminal problem in VANETs when using CSMA and STDMA?", in Proc. of the 4th IEEE Int. Symp. On Wireless Vehicular Communications (WiVEC), San Francisco, USA, Sept. 2011.

[i.51] F. Borgonovo, A. Capone, M. Cesana, L. Fratta, "ADHOC MAC: a new MAC architecture for ad hoc networks providing efficient and reliable point-to-point and broadcast services", in ACM Wireless Networks (WINET), vol. 10, no. 4, pp. 359-366, July 2004.

[i.52] A. Vesco, F. Abrate, and R. Scopigno, "Convergence and performance analysis of leaderless synchronization in Wi-Fi networks", in Proc. ACM 6th Performance Monitoring, Measurement and Evaluation of Heterogeneous Wireless and Wired Networks, Miami Beach, FL, USA, Oct. 2011.

[i.53] M.Z. Brodsky and R. T. Morris, "In defense of wireless carrier sense", in Proc. of SIGCOMM 2009, Barcelona, Spain, Aug. 2009.

[i.54] L. G. Roberts, "Aloha packet system with and without slots and capture", ACM SIGCOMM Computer Communication Review, vol. 5, no. 2, pp. 28-42, April 1975.

[i.55] N. Abramson, "The Aloha system - another alternative for computer communications", in Proc. of the AFIPS Joint Computer Conferences, Houston, TX, 1970, pp. 281-285.

[i.56] W. Crowther, R. Rettberg, D. Walden, S. Crustein, and F. Heart, "A system for broadcast communication: Reservation Aloha", in Proc. of the 6th Hawaii International Conference on System Sciences, Honolulu, HI, January 1973, pp. 371-374.

[i.57] A. Mann and J. Rückert, "A new concurrent slot assignment protocol for traffic information exchange", in Proc. of the 38th IEEE Vehicular Technology Conference (VTC'88), Philadelphia, PA, June 1988, pp. 503-508.

[i.58] W. Zhu, T. Hellmich, and B. Walke, "DCAP, a decentral channel access protocol: performance analysis", in Proc. of the 41st IEEE Vehicular Technology Conference (VTC'91), Orlando, FL, 1991, pp. 463-468.

[i.59] F. Borgonovo, A. Capone, M. Cesana, and L. Fratta, "RR-Aloha, a reliable R-Aloha broadcast channel for ad-hoc inter-vehicle communication networks", in Proc.of the 1st Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2002), Baia Chia, Italy, Sep. 2002.

[i.60] F. Borgonovo, A. Capone, M. Cesana, and L. Fratta, "ADHOC MAC: a new MAC architecture for ad-hoc networks providing efficient and reliable point-to-point and broadcast services", in ACM Wireless Networks (WINET), vol. 10, no. 4, pp. 359-366, July 2004.

[i.61] L. Miao, F. Ren, C. Lin, and A. Luo, "A-ADHOC: an adaptive real-time distributed MAC protocol for vehicular ad hoc networks", in Proc.of the 4th International Conference on Communications and Networking in China 2009 (CHINACOM), Xi'an, China, August 2009, pp. 1-6.

[i.62] H. A. Cozzetti and R. Scopigno, "RR-Aloha+: a slotted and distributed MAC protocol for vehicular communications", in Proc. of the IEEE Vehicular Networking Conference, Tokyo, Japan, Oct. 2009, pp. 1-6.

[i.63] Y. Günter, W. B., and H. P. Grossmann, "Medium access concept for VANETs based on clustering", in Proc.of the IEEE Vehicular Technology Conference, Baltimore, MD, Oct. 2007, pp. 2189-2193.

[i.64] S. V. Bana and P. Varaiya, "Space division multiple access (SDMA) for robust ad hoc vehicle communication networks", in Proc.of the IEEE Intelligent Transportation Systems Conference, Oakland, CA, August 2001, pp. 962-967.

[i.65] S. Katragadda, C. N. S. Ganesh Murthy, M. S. Ranga Rao, S. Mohan Kumar, and R. Sachin, "A decentralized location-based channel access protocol for inter-vehicle communication", in Proc.of the IEEE Vehicular Technology Conference, Jeju Island, Korea, April 2003, pp. 1831-1835.

[i.66] X. Chen, H. H. Refai, and X. Ma, "SDMA: on the suitability for VANET", in Proc. 3rd International Conference on Information and Communication Technologies (ICTTA 2008), Damascus, Syria, April 2008, pp. 1-5.

[i.67] 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. 4-13, January 2007.

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

ad hoc network: wireless networks based on self-organization without the need for a centralised coordinating infrastructure

broadcast: simplex point-to-multipoint mode of transmission

3.2 Symbols

For the purposes of the present document, the following symbols apply:

A	Symbol used to indicate a node in the examples
a	Sub-period of a period *c*, used for asynchronous MAC
AC_BE	Access Category Best Effort
AC_BK	Access Category Background
AC_VI	Access Category Video
AC_VO	Access Category Voice
B	Symbol used to indicate a node in the examples
b	Sub-period of a period *c*, used for synchronous MAC
c	Fixed period of time for the coexistence of two MAC methods
C	Symbol used to indicate a node in the examples
CW	Contention Window
CW_{max}	Maximum possible value of *CW*
CW_{min}	Minimum possible value of *CW*
D	Symbol used to indicate a node in the examples
E	Symbol used to indicate a node in the examples
F%	Percentage of slots perceived free by a node
F_1	Upper Threshold used by 2-SMtd to evaluate *F%* for the near-exhaustion condition
F_2	Lower Threshold used by 2-SMtd to evaluate *F%* for the unloaded condition
FI	Frame Indication
FI'	Extended Frame indication, including both *FI* and *STI*
FI_j	The j-th subfield of the *FI* field
j	Index used in the examples for the indication of slot number
J	The *j*-th slot in MS-Aloha's Frame
L1	Layer 1
L2	Layer 2
LA	Set of nodes receiving from node *A*
MB	Set of nodes receiving from node *B*
N	Number of slots in a period
P	Clock precision in ppm
ppm	Parts per million
PSF	Priority Status Field
SX	Equivalent number of slots required to transmit *X* Bytes
SLOT_n	Slot number n of MS-Aloha Frame structure
STATE	The field of each *FI_j* indicating the perceived state (*busy/free/collision/2-hop*)
STI	Short Temporary Identifier
T_{AIFS}	Arbitration interframe space period
TX	Time required to transmit *X* Bytes
Tg	Guard Time
Thr	MS-Aloha threshold used for *2SMt* and *2SMtd* algorithms
T_{slot}	Duration of a slot
X	Generic number of Bytes in a frame

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

2-SM	2-Hop Spatial Multiplexing
2-SMt	2-Hop Spatial Multiplexing with Threshold
2-SMtd	2-Hop Spatial Multiplexing with Dynamic Threshold
AC	Access Category
ACK	Acknowledgment
AIFS	Arbitration InterFrame Space
AIS	Automatic Identification System
AP	Access Point
ARQ	Automatic Repeat request
ATS	Average TimeSync Protocol
BS	Base Station
CAM	Cooperative Awareness Message
CCA	Clear Channel Assessment
CCH	Control Channel
CDMA	Code Division Multiple Access
CRC	Cyclic Redundancy Check
CSAP	Concurrent Slot Assignment Protocol
CSMA	Carrier Sense Multiple Access
CTS	Clear-To-Send
DCAP	Decentral Channel Access Protocol
DCC	Decentralised Congestion Control
DENM	Decentralised Environmental Notification Message
DTDMA	Decentralised TDMA
EDCA	EDCF Controlled Channel Access
FCS	Frame Check Sequence
FI	Frame Information
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GPSDO	Global Positioning System Disciplined Oscillator
HCCA	HCF Controlled Channel Access
HPOCXO	High Performance OCXO
HW	Hardware
ITS	Intelligent Transport Systems
LDM	Local Dynamic Map
MAC	Medium Access Control
MS-Aloha	Mobile Slotted Aloha
NI	Nominal Increment
NS	Nominal Slot
NSS	Nominal Start Slot
NTP	Network Time Protocol
NTS	Nominal Transmission Slot
PDR	Packet Delivery Ratio
PHY	Physical layer
PPM	Part Per Million
PPS	Pulse Per Second
PR-Aloha	Priority R-Aloha
PSF	Priority State Field
QoS	Quality of Service
RAIM	Receiver Autonomous Integrity Monitoring
R-Aloha	Reservation Aloha
RBS	Reference Broadcast Synchronization
RR	Report Rate
RR-Aloha	Reliable R-Aloha
RTS	Request-To-Send
RX	Receiver
SCH	Service Channel
SDH	Synchronous Digital Hierarchy

SDMA	Space Division Multiple Access
SI	Selection Interval
SINR	Signal-to-Interference-plus-Noise Ratio
STDMA	Self-Organizing Time Division Multiple Access
STI	STI stands for Short Temporary Identifier, which is stated in the Symbol list. What to do?
TDMA	Time Division Multiple Access
TPC	Transmit Power Control
TPSN	Timing-sync Protocol for Sensor Networks
TX	Transmitter
TXCO	Temperature-Controlled Crystal Oscillator
UTC	Universal Coordinated Time
V2V	Vehicle-to-Vehicle
VANET	Vehicular *Ad Hoc* Networks
VCO	Voltage Controlled Oscillator
VHF	Very High Frequency band
WLAN	Wireless Local Area Network

4 Introduction

4.1 Medium access control in VANETs

The MAC algorithm resides in the MAC sub-layer of the data link layer in the protocol stack of a communication system, see figure 1. It is responsible for scheduling transmissions in e.g. time, frequency or space. The objective is often to minimize interference and thereby increase reception probability at the receivers. Providing access to the shared medium, while at the same time enabling the quality of service (QoS) requested by the application is the most important but also the most challenging task of the MAC layer. There exist several different MAC methods tailored to the network topology in question (centralized or *ad hoc*). In centralized networks, an access point (AP) or a Base Station (BS) is usually responsible for scheduling the transmissions and share the resources equally among all nodes. The AP or the BS has perfect knowledge of which nodes that are associated to them. In centralized networks, AP and BS are single point of failures. The loss of an AP or BS, due to hardware failure or loss of power will result in outage because the nodes cannot self-organize. In the *ad hoc* topology, a decentralized MAC method is needed, such that the scheduling of transmissions is distributed among the nodes. The network self-organizes and the failure of one node does not necessarily affect the rest of the network. The *ad hoc* structure is advantageous, since it does not require coverage by BS or AP to function, but without a central control mechanism, problems with scalability may arise.

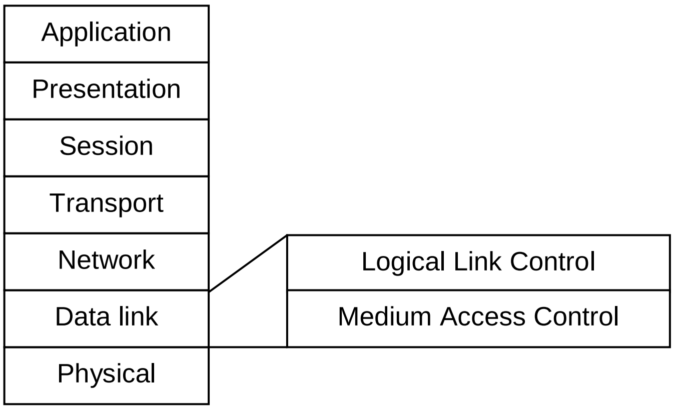


Figure 1: Generic protocol stack showing the logical position for the medium access control the sublayer

From ongoing standardization activities [i.1] and [i.2], it is clear that many road traffic safety applications will be based on 802.11p, forming *ad hoc* networks. Further, two types of messages are envisioned; decentralized environmental notification messages (DENM) [i.5] and cooperative awareness messages (CAM) [i.6]. DENM are event-driven messages that are generated as a result of a hazard, whereas CAMs are time-triggered and contain position, speed, heading, etc of each vehicle. CAMs are broadcasted regularly by every vehicle and are the foundation for the local dynamic map (LDM) [i.3] facility. These broadcasted warning and positioning messages imply a distributed control system, with concurrent requirements on high reliability and real-time deadlines.

To increase reliability in broadcast mode, the same message is repeated several times. This implies that the MAC method should be able to handle temporarily high network loads that may occur as the result of a hazard. To support real-time deadlines, the MAC method should be predictable such that the maximum delay before granting channel access is known. Further, the *ad hoc* network implies that the MAC method has to be decentralized. Note that in a VANET the number of nodes cannot be restricted and therefore the MAC method used in VANETs have to be self-organising, fair and scalable. A self-organising MAC algorithm implies that nodes are responsible for scheduling transmissions without the intervention of infrastructure such as AP or BS. i.e. the channel access scheduling is distributed. The MAC algorithm has to be fair in the sense that all nodes have equal right to access the wireless channel at least once during a limited time period. For example, in overloaded situations potential packet drops at transmitter due to congestion should affect all network members equally. Scalability is a key concept of road traffic safety applications and implies that the VANET has to support a varying number of nodes or a varying amount of data traffic without collapsing.

It can be concluded that the MAC protocol in VANETs supporting road traffic safety applications should be scalable (not block nodes from accessing the shared communication channel), predictable (to guarantee an upper bounded channel access delay for scheduling real-time data traffic), fair (in order for nodes, having the same type of data traffic to transmit, to have equal right to access the channel within each time interval), and of course it has to self-organize. Further, features like low complexity, high flexibility and ability to minimize interference between transmitters to maximize the packet reception probability for the closest neighbouring nodes are also desirable.

4.2 Requirements for road traffic safety applications

Cooperative road traffic safety applications are realized through communicating DENMs and CAMs. DENMs are generated in the event of a hazard and require high reliability since the hazard is critical. To increase the reliability, rebroadcast of the same message is performed until the hazard is no longer valid or has occurred. A low delay is also important since a notification about an upcoming dangerous situation should be handed over to the driver as soon as possible to increase the horizon of awareness for the driver and also to make room for carrying out necessary operations to avoid the dangerous situation. CAMs have modest reliability requirements since these are periodically transmitted and do not signal imminent hazard. However, also in the case of CAMs, a low delay will result in better performance - in this case in terms of better position accuracy. Note that even though a low delay is beneficial, CAMs and DENMs are more dependent on the maximum delay to function properly. If the maximum delay before granting channel access is longer than the period of the CAM, a new and more recent CAM will be available, and it is useless to transmit the older position information. Similarly, with DENMs, if channel access is not granted in time to avoid the hazard, the system performance is seriously degraded. Messages like CAMs and DENMs therefore have real-time deadlines and it is important that the MAC protocol supports these deadlines, both by having an upper bounded maximum delay, but also by having a low maximum delay. Due to the concurrent requirements on delay and reliability for CAMs and DENMs, the road traffic safety applications using them can be classified as distributed control systems. Requirements on the MAC layer stem from different parts of the cooperative ITS system namely (*i*), the *ad hoc* topology, (*ii*) road traffic safety applications and (*iii*) the overall ITS system. The list of requirements is quite extensive. However, many of the requirements are correlated and closely connected to the scalability issue.

The *ad hoc* topology enforces the following requirements on the MAC protocol:

- *Self-organizing*. The scheduling of transmissions have to be performed in a distributed manner. Any resources that no longer are used have to be reclaimed regularly.

- *Reactiveness*. The management of allotted resources should be flexible and fast enough to let the protocol react timely to topology changes due to mobility. In principle, a slower reactiveness may cause unintentional slot re-use and may affect reception rate. However the impact has to be evaluated. Conversely, how often allotted or unused resources are adjusted is a trade-off between robustness and complexity.

- *Scalability*. The number of vehicles participating in the VANET is unknown *a priori*. It is a number which, in the city centres, is expected to grow to several hundreds of nodes that are within radio range of each other (there exist studies which estimates over 600 nodes in less than 1 km^2). The adopted MAC protocol has to support transmissions by all these nodes - with priority on road traffic safety messages. This implies that the MAC protocol should be *non-blocking* such that new nodes or new data traffic always can be supported.

- *Mitigation of hidden terminal situations.* The hidden terminal problem is present in all VANETs regardless of MAC method; for each MAC protocol it is necessary to evaluate the impact of hidden terminals in terms of performance degradations. The hidden terminal problem is further discussed in clause 4.3 and in TR 102 861 [i.43].

The road traffic safety applications requirements on the MAC protocol are:

- *Delay*. Road traffic safety applications require a predictable channel access such that the maximum channel access delay is upper-bounded, implying that real-time deadlines can be supported. This calls for a predictable MAC method. Obviously a low delay is also beneficial.

- *Reliability*. The reliability issue depends on several layers in the protocol stack, but it is mostly addressed in the physical layer. However, if the MAC protocol schedules transmissions to minimize interference between nodes, reliability is also increased. A broadcast scenario excludes traditional automatic repeat request (ARQ) mechanisms to increase reliability and hence re-broadcast of the same message is used. This should be supported by the MAC protocol in use. Ability to minimize interference between transmitters to maximize the packet reception probability for the closest neighbouring nodes is also desirable.

- *Fairness*. All the nodes should be able to access the channel with equal probability within a limited time period, e.g. the CAM update frequency. This can be enforced by a predictable MAC method.

The overall ITS system includes other types of applications besides road traffic safety, which leads to the following requirements on the MAC protocol:

- *QoS differentiation*. All the nodes should be able to access the channel with equal probability considering the same type of messages, i.e. the same QoS class in every node generates equal access to the channel. For example DENMs should have higher priority than CAMs in event of hazard.

- *Efficiency.* This is a requirement which applies to any protocol where resources are likely to get exhausted - not only to VANETs. The protocol should be as efficient as possible: the complexity and protocol overheads should be kept low and increase only if required to solve some specific issue. Notably, in case of broadcast transmissions, the overhead should *not* be evaluated *at the transmitter* (as the ratio between payload and transmission time) but *at the receiver* (considering also the reception probability).

The CSMA and the time slotted MAC approaches will be compared with these requirements in mind.

4.3 Hidden terminal problem

The hidden terminal problem is often pointed out as being the major performance limiting factor in VANETs, but generally this is simply stated without any formal proof or study to verify this claim. In centralized networks using CSMA, the hidden terminal problem certainly affects performance since CSMA is a distributed algorithm that is not centrally controlled by the AP and further, the AP is involved in all transmissions. Thus if a hidden terminal situation occurs, all transmissions may be lost (they collide at the only receiver; the AP). This problem was defined and discussed already 1975 in [i.10]. In other centralized networks, where TDMA or centralized MAC approaches such as code division multiple access (CDMA) are used, the AP/BS controls channel access and the hidden terminal problem does not exist. In *ad hoc* networks, hidden terminals are always present regardless of MAC method due to the decentralized network topology, i.e. a decentralized *ad hoc* network requires a decentralized MAC algorithm. However, in a broadcast scenario in a VANET, the hidden terminal problem, although present, may not necessarily have a major impact on the overall performance. This is partly due to nodes being highly mobile and partly due to the fact that there is more than one intended receiver of each transmission. Therefore, even if a hidden terminal problem occurs for one receiver, it may not be a problem for others (collisions occur at some nodes but not at all of them).

In figure 2 the hidden terminal problem is depicted for the unicast case in a CSMA network containing an AP. Node TX_1 and node TX_2 are out of radio range of each other - they are hidden for one another, and therefore they cannot detect if the other one is transmitting. The AP can reach all nodes associated to it and hence it can hear both TX_1 and TX_2. The hidden terminal problem occurs when, for example node TX_1 is transmitting and node TX_2 initiates a transmission while TX_1 still transmits, since TX_2 detected no channel activity during the carrier sensing, i.e. a clear channel assessment (CCA) was obtained. The outcome of simultaneous transmissions from the two hidden terminals will be decoding problems at the only receiver, the AP (a collision). Depending on the instantaneous radio environment, the AP will be able to decode one of the two transmissions or nothing at all.

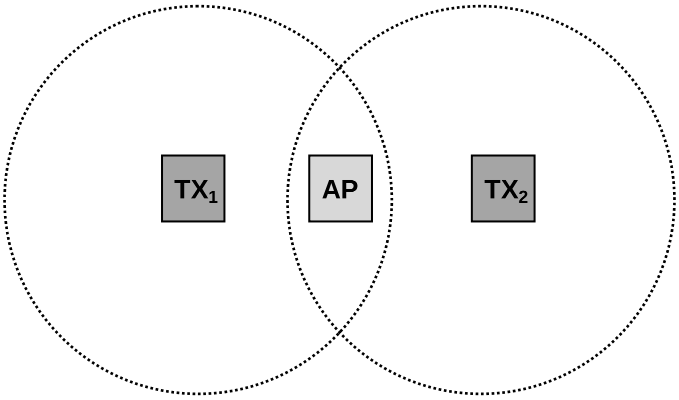


Figure 2: The hidden terminal problem in a CSMA network containing AP

The hidden terminal problem in AP-based networks can have a major effect on the performance because all communication goes through the AP and thus all concurrent transmissions result in collisions. As the nodes are semi-static, the same nodes can be exposed to the hidden terminal phenomena for long time periods. However, in an AP based CSMA network, the problem can be combatted by preceding every transmission with small control packets, request-to-send (RTS) and clear-to-send (CTS), to notify all nodes in the network about an upcoming transmission. This cannot be done in VANETs due to the broadcast nature of the data traffic, implying more than one intended receiver.

In figure 3 a hidden terminal situation in an *ad hoc* network when TX_1 and TX_2 are broadcasting, is depicted. Here, RX_1-RX_4 are likely to receive TX_1, whereas RX_8-RX_{11} are likely to receive TX_2. Therefore the outcome of a hidden terminal situation in a VANET with broadcast does not necessarily lead to major performance degradation because not all receivers will experience problems. In fact, only receivers located close to the border of the range of the transmitter are likely to experience a collision. In road traffic safety applications, the nodes located close to the transmitter are likely to be the most important receivers. Further, the next time TX_1 and TX_2 broadcast, the set RX_5-RX_7 may have changed.

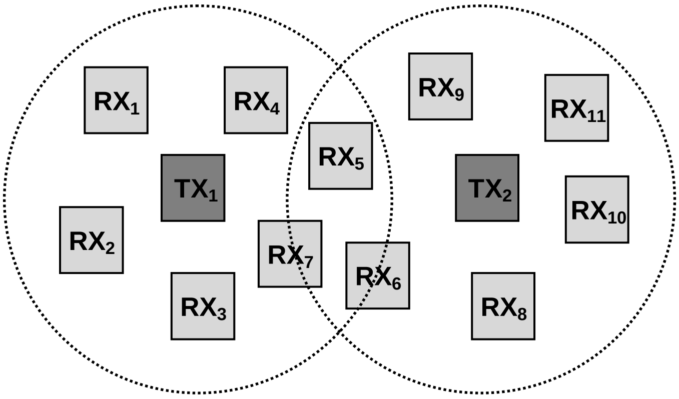


Figure 3: The hidden terminal problem in a VANET when two nodes are broadcasting

Due to the selected carrier frequency of 5,9 GHz, which in certain situations may cause severe multipath and inability to diffract around corners, the hidden terminal problem may, however, impact performance more in urban areas. While figure 3 showed a general hidden terminal situation as found in rural areas or on highways where the nodes are situated on a single road, figure 4 shows a hidden terminal situation in an urban scenario. In this type of scenario the broadcasting nodes TX_1-TX_4 could be geographically close to each other, but at the same time hidden the one to the other, due to obstructions by buildings. Note that nodes situated in intersections will be able to receive from four (or more) different streets, whereas nodes situated on a cross-street will only be able to receive upstream or downstream. Hidden terminal situations are therefore more likely to occur in the intersections.

Further analysis of the impact of hidden terminals in VANETs with broadcast communication is outlined in TR 102 861 [i.43] for two different scenarios; urban and rural. MS-Aloha is natively preventing hidden terminal situations to occur; this is further explained in clause 7.3.

NOTE: The number of collisions caused by hidden terminals depends on the number of nodes, the location of nodes, the communication environment, the transmit power level and the amount of data traffic generated by the ITS-G5 stations. The last two parameters, transmit power level and amount of data traffic, will be controlled by decentralized congestion control (DCC) [i.8] and regulated depending on the vehicle density. Therefore, the DCC algorithm will to some extent also combat the effects of hidden terminals.

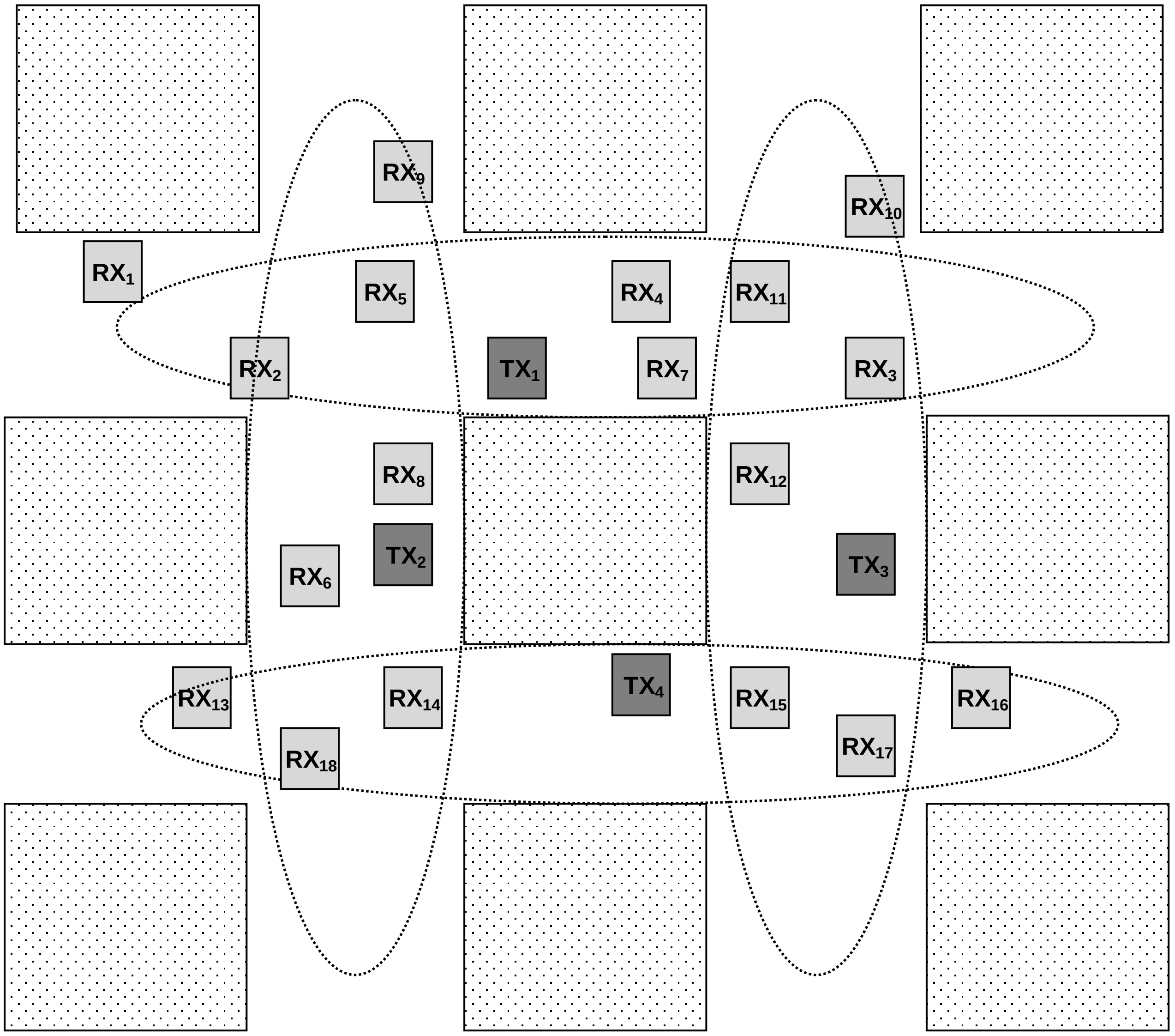


Figure 4: The hidden terminal problem in a VANET when nodes are broadcasting in an urban area

5 CSMA

5.1 Introduction

The IEEE 802.11p [i.2] is an amendment to the IEEE 802.11 [i.4] wireless local area network (WLAN) standard, which is tailored to the vehicular environment where nodes are highly mobile. The 802.11p amendment covers both MAC and PHY issues. IEEE 802.11p [i.2] uses the MAC amendment 802.11e QoS and the PHY supplement 802.11a (since 2007 both 802.11e and 802.11a are rolled up in legacy IEEE 802.11 [i.4], hence they are no longer "standalone" documents). The major differences between 802.11p and legacy 802.11 are the removal of AP functionality and simplified authorization and associating procedures, to facilitate *ad hoc* networking.

ETSI has standardized a profile of 802.11p named ITS-G5 [i.1] specially adapted to the European frequency channel allocations. At large, ITS-G5 contains recommended settings for 802.11p parameters and also requirements on decentralized congestion control (DCC) mechanisms. In clause 4.4 in [i.1] it is explicitly stated that safety-related ITS applications have concurrent requirements on delay and reliability. Further, to ensure network stability and support safety-related ITS applications mechanisms for adjustments on packet rate, transmit power control (TPC) and data rate, collectively called DCC, are developed in [i.5].

In a WLAN when an AP is present, all traffic has to traverse the AP even though TX and RX are within radio range of each other. All data traffic between TX and AP are unicast transmissions and all packets are acknowledged, i.e. an ARQ strategy is present. The AP is responsible for broadcasting e.g. beacons and traffic indication maps. An AP can manage approximately 30 to 40 associated nodes and once this quota has been filled further nodes are not granted access to the AP (blocked). The data traffic in WLAN is typically bursty in nature, i.e. much event-driven traffic is present.

802.11p only supports *ad hoc* networking but an even more loosely defined *ad hoc* topology than found in 802.11 since authentication and association procedures are removed. These procedures are not possible to accommodate in a network where the nodes are highly mobile and move in and out of radio ranges of each other. Even though there are roadside units (RSU) present in VANETs, these cannot be equated with an AP from a MAC layer perspective since this would imply granting access to the network through authentication and association. The separation between an RSU and a mobile ITS station is only made at higher layers.

5.2 Channel access procedure and parameters

In the MAC method CSMA of 802.11, each node initiates a transmission by listening to the channel, i.e. performs a carrier sense operation, during a predetermined listening or sensing period called the arbitration interframe space (AIFS), T_{AIFS}. If the sensing is successful, i.e. no channel activity is detected, the node transmits directly. If the channel is occupied or becomes occupied during the sensing period, the node has to perform a backoff procedure, i.e. the node has to defer its access 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*, T_{slot}, derived from the PHY layer in use (i.e. in 802.11p T_{slot} =13 μs), and set this as the backoff value, (*iii*) decrease the backoff value by one T_{slot} for every T_{slot} the channel is sensed as free, (*iv*) upon reaching a backoff value of 0, transmit directly. Thus, after a busy channel becomes clear, all nodes have to listen a T_{AIFS} before decrementation of the backoff value can resume.

In unicast transmissions every packet is acknowledged (ACK). In other words, the receiver transmits a receipt upon successful reception. The backoff procedure is then also invoked when an ACK is missing. During high network utilization periods ACKs can be lost due to simultaneous transmissions caused by hidden nodes or wireless channel impairments such as fading. For every attempt to transmit a specific packet (where the ACK from the receiver is repeatedly missing), the node doubles the *CW*, resulting in a greater spread of simultaneous transmission attempts during high utilization periods. CSMA is therefore reliable in unicast mode since packets are retransmitted until a successful ACK is received. However, the reliability comes at the expense of a random delay which is not upper bounded. Therefore, CSMA works best for non-real-time, event-triggered data traffic where high utilization periods are followed by low utilization periods and collisions have time to be resolved, i.e. the network can recover.

In a broadcast communication scenario, one-to-many, ACKs cannot be used. This implies that the backoff procedure is only invoked once: if the channel becomes busy during the initial sensing period, T_{AIFS}. Therefore, the feature with doubling the *CW* during high utilization periods is never used.

In figure 5 the channel access procedure for CSMA is depicted considering CAM to be transmitted, i.e. broadcast communication.

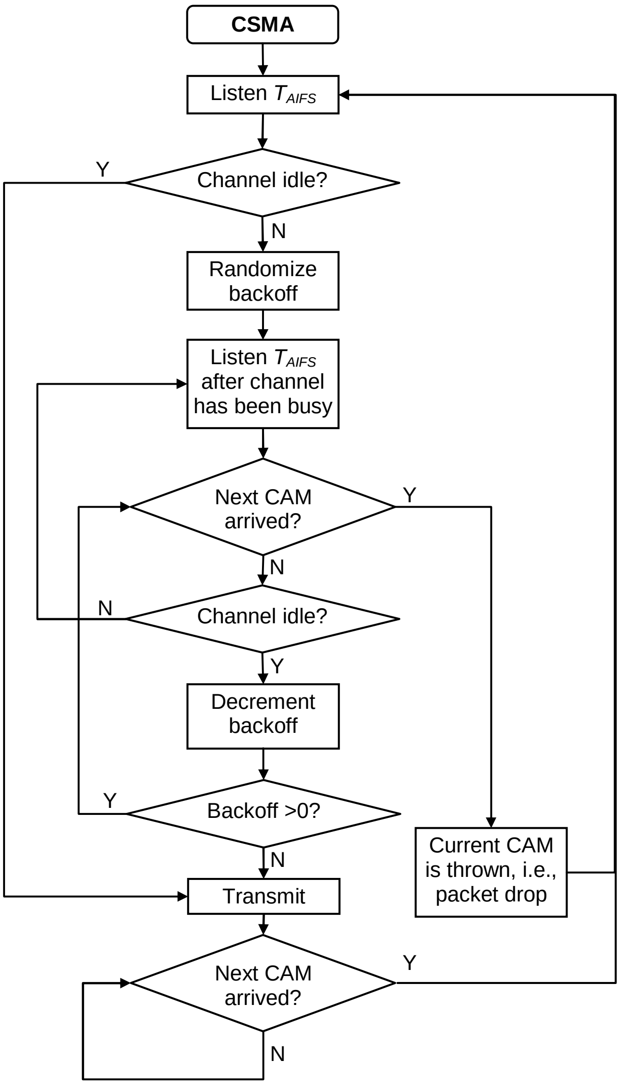


Figure 5: The channel access procedure of CSMA when CAMs are broadcasted

IEEE 802.11p [i.2] supports QoS by dividing the data traffic into four different queues called access categories. The highest priority queue has the shortest T_{AIFS} and the smallest initial *CW*. In table 1, the different queues with associated T_{AIFS} and *CW* are tabulated as for the four different ACs of 802.11p; voice (*AC_VO*), video (*AC_VI*), best effort (*AC_BE*), and background (*AC_BK*), where *AC_VO* has the highest priority and *AC_BK* the lowest priority.

Table 1: The priority queues found in 802.11p and its associated values

AC	T_{AIFS} [µs]	CW_{min}	CW_{max}	Initial backoff values to randomly select from [µs]
AC_VO	58	3	7	{0, 13, 26, 39}
AC_VI	71	7	15	{0, 13, 26, 39, 52, 65, 78, 91}
AC_BE	110	15	1 023	{0, 13, 26, 39, 52, 65, 78, 91, 104, 117, 130, 143, 156, 169, 182, 195}
AC_BK	149	15	1 023	{0, 13, 26, 39, 52, 65, 78, 91, 104, 117, 130, 143, 156, 169, 182, 195}

5.3 Simultaneous transmissions

Simultaneous transmissions within radio range occur either due to *(i)* nodes reaching a backoff value of zero at the same time or *(ii)* that carrier sensing is performed approximately at the same time. The former is the most abundant source of simultaneous transmissions. As can be seen in table 1, the number of values available to randomly select from when the backoff procedure is invoked is few for the highest priority, which increases the probability that several nodes select the same backoff value during high utilization periods. This in turn will lead to a higher probability of concurrent transmissions. The probability of sensing the channel at the same time increases with the number of nodes in the VANET as well as the number of transmission attempts. If, for example, two nodes discover the same event, they are likely to try to access the channel to transmit a DENM at the same time.

5.4 Summary

Road traffic safety applications have requirements on delay, reliability and fairness. In CSMA the fulfilment of these requirements are dependent on the number of vehicles within radio range and the amount of data traffic presented to the network, i.e. the scalability of the MAC method. With few nodes in the system the requirements are easily met (this applies to every MAC method). When the network load increases in CSMA; the channel access delay increases, the reliability decreases and the probability for unfairness increases. Due to the randomness of the channel access procedure in CSMA the channel access delay is not upper bounded implying that CSMA is not a predictable MAC method.

The road traffic safety applications running over VANETs differ from most of the applications present in WLAN. Many ITS applications are by nature broadcast and this heavily affects the 802.11 strategies for recovering from collisions and high utilization periods. In a broadcast scenario no ACKs are present and therefore the backoff procedure is only invoked once during the initial carrier sensing of the wireless channel. The favourable feature of increasing the *CW* is therefore disabled in broadcast mode and fewer backoff values are available. This results in more simultaneous transmissions attempts within radio range by CSMA nodes during high utilization periods since nodes are allowed to transmit directly when the backoff value reaches zero. Especially, if the highest priority data traffic is considered because then there is only four different backoff values to select from. Due to this the reliability is heavily affected for CSMA. Further, when the number of nodes increases some nodes will experience considerably longer channel access delays than other nodes in the VANET implying fairness problems. Therefore, the DCC methods developed in [i.8] are important to protect at least some of the transmissions in overloaded situations. However, to find the right parameter settings for the transmit power control (TPC) and the packet rate is still an open issue in order not to deteriorate road traffic safety application performance.

CSMA requires no synchronization among nodes, supports arbitrary packet lengths, and has a low average delay when the number of nodes in the network is sufficiently low (~30 nodes to 40 nodes). CSMA works excellent when employed in WLAN since the AP can handle a certain amount of nodes and when the AP reaches the limit it blocks further nodes and thereby the already associated nodes are protected from excessive channel access delays and unfairness.

6 Motivations for time slotted MAC approaches

There are pros and cons for all MAC methods and they are tailored to the network topology and the data traffic it is supposed to support. Many commercially available networks, e.g. Wi-Fi, 2G/3G, were designed for a centralized network topology where applications are mainly using unicast communication, one-to-one, and a feedback channel exist due to the point-to-point connection. Broadcast transmissions exist but are made by the AP or BS. In VANETs running road traffic safety applications it is the other way around, i.e. broadcast is the main transmission mode by all nodes. Broadcast communication together with the decentralized topology changes everything and on top of that the nodes are mobile. Throughput, which has been an important performance measure for unicast transmissions and is defined for centralized networks, is hard to define for a VANET covering for example a whole highway. Performance measures have to be defined from the sending and the receiving node's perspectives, e.g. perceived channel access delay and packet reception probability. The data traffic models found in VANETs are also different from for example Wi-Fi/2G/3G. The foundation for safety applications is the transmitted periodic position message (CAM) having an update rate of 1 Hz to 10 Hz. In the introduction of road traffic safety these will be the predominant data traffic present before full deployment of all suggested road traffic safety applications triggering hazard warnings (DENM) reach full penetration. The point is that the continuous time-triggered data traffic model with broadcast has not been a predominant model in commercial networks before. In Wi-Fi/2G/3G nodes show up, e.g. people makes a phone call or web browsing, and after a while they will disappear, e.g. people hang up or stopped web browsing. The event-driven model of these centralized networks (which is of course periodic while, e.g. phone call is ongoing) is well investigated and the network capacity is known due to the centralized topology.

CSMA is a well-known MAC method, which does not need synchronization and supports arbitrary packet sizes. It has shown to reach almost optimal capacity under the assumption of adaptive transfer rate [i.53]. The results found in [i.53] are very interesting but still considers one sender-receiver pair with one interferer present, i.e. unicast transmissions with ACK feedback. The feedback allows the sender to increase the transfer rate when the channel condition is good at the receiver with increased throughput and decreased interference as a result. In VANETs the sender does not know the channel condition of each and every receiver therefore the transfer rate is set in advance and it is a compromise between desirable decoding distance and channel occupancy. When the number of nodes increases within radio range in the VANET with broadcasted CAMs/DENMs many simultaneous transmissions will take place and packet drops at TX will occur with decreased packet reception probability and excessive channel access delays as a result. This performance degradation will jeopardize road traffic safety applications requiring upper bounded channel access delay and high reliability concurrently as outlined in clause 4.2. Therefore, the work conducted on decentralized congestion control (DCC) and transmit power control (TPC) in [i.8] is extremely important in order to combat the scalability issue of CSMA. However, the current proposal in [i.8] is to only load the control channel with 25 % of data traffic to guarantee that the DENM could be supported in the event of a hazard. This is a waste of resources since bandwidth is a costly, naturally limited resource.

Self-organizing time slotted MAC approaches such as STDMA and MS-Aloha can utilize the control channel to 100 % and above if necessary through careful scheduling of transmissions. They are designed to guarantee an upper bounded channel access delay regardless of the number of nodes within range. When all slots are occupied they allow concurrent transmissions in time slots through careful scheduling aiming at protecting the closest neighbours of the transmitter from interference. A time slotted MAC approach is obviously very suitable for time-triggered CAMs, but also for event-driven DENMs as events in VANETs are likely to affect more than one node simultaneously. STDMA is already in commercial use in a collision avoidance system for ships, which foundation is built on position messages, e.g. CAMs. MS-Aloha is specifically designed for VANETs with broadcast communication. Since both STDMA and MS-Aloha can handle overloaded situations, i.e. more requested resources than actually available, their channel access delay is upper bounded, i.e. they are predictable. Further, the reliability is maintained for the closest neighbours in overloaded situations. Due to the guaranteed channel access all nodes have equal opportunity to access the channel and therefore both algorithms are inherently fair. However, they do need synchronization and typically only support fixed packet sizes. The investigation of time slotted MAC approaches for VANETs is motivated by the fact that they can fulfil all the necessary requirements set up by road traffic safety applications as discussed in clause 4.2. STDMA is detailed in clause 7.2 and MS-Aloha in clause 7.3.

7 Time slotted MAC approaches

7.1 Introduction

In time slotted MAC approaches, the available time is divided into time slots and further grouped into frames, figure 6. The time slots are of fixed length and hence so are the frames. A fixed transfer rate is usually provided by the physical layer in a time slotted MAC system and therefore, one message typically fits into one time slot. If a node has a longer message to send than is allowed in the time slot, this is solved by allocating one or more consecutive slots. The slotted Aloha (S-Aloha) protocol, presented already in 1975 [i.10], can be seen as the starting point for time slotted MAC approaches. Several different slotted approaches have been proposed and refined throughout the years - all still based on the time slot concept. They are given a name containing either time division or Aloha, but the time slotted approach is still the same, as will be shown below.

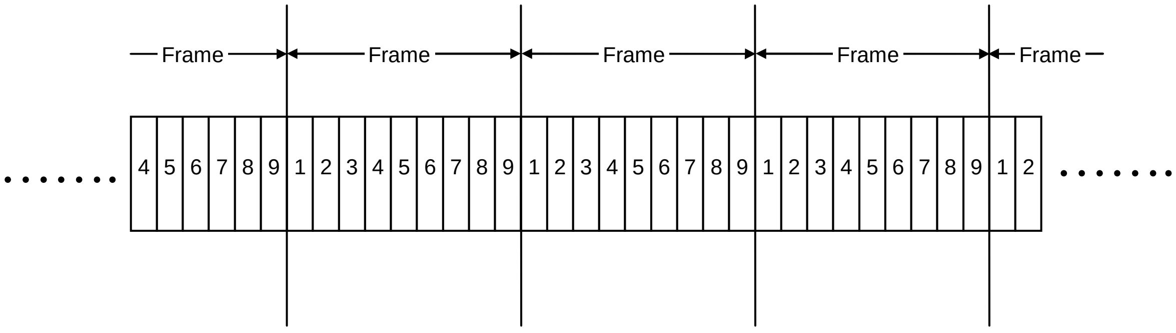


Figure 6: Example of a framing structure in time slotted MAC, slots are grouped into frames

During the past, time slotted MAC approaches have been used in centralized networks [i.9]. The central controller maintains the network synchronized and also performs admission control, i.e. when there are no more available time slots, no more nodes are granted access to the network. The central controller can, in other words, block further nodes to join the network and access the shared wireless communication channel. This blocking can be present in both centralized as well as *ad hoc* networks, utilizing a time slotted approach. In most network settings, the blocking does not necessarily lead to major problems for the end user, more than a substantial delay until network resources are released and available again. However, blocking cannot be allowed in VANETs supporting road traffic safety applications. There are time slotted MAC protocols that can handle overloaded situations, i.e. they are not blocking. Two examples of non-blocking time slotted MAC schemes are STDMA, discussed in clause 7.2 and MS-Aloha detailed in clause 7.3. The non-blocking feature implies good scalability properties.

In most non-blocking time slotted approaches a random access channel is used for slot allocation. One part of the frame is then used exclusively for slot allocation and it is not possible to allocate slots for transmission in this part. Instead slot allocations is made using, e.g. CSMA as in figure 7. Contrary to most other non-blocking time slotted approaches, STDMA and MS-Aloha do not rely on a random access channel for slot allocation. Instead nodes listen to the frame and determine the current slot allocation, based on what is perceived as free and occupied slots in the frame.

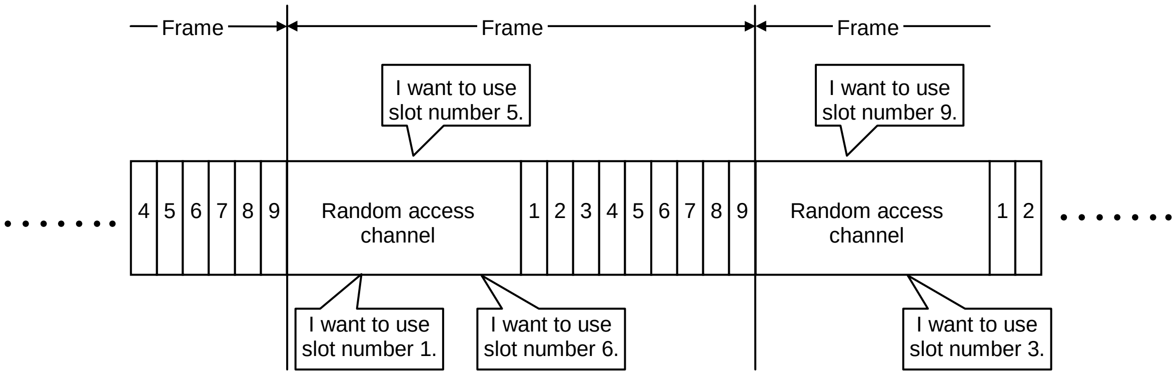

Frame
Frame
Frame
I want to use slot number 5.
I want to use slot number 9.
4 5 6 7 8 9
Random access channel
1 2 3 4 5 6 7 8 9
Random access channel
1 2
I want to use slot number 1.
I want to use slot number 6.
I want to use slot number 3.

Figure 7: Example of a framing structure in time slotted MAC scheme using a random access channel for slot allocations

The time slotted approaches need more or less protocol overhead, depending on the degree of coordination and flexibility which they are aimed at. In the case of a centralized network topology, the controller determines the slot allocation based on requests, and disseminates this information to everybody, usually in the beginning of the frame, i.e. which slot belongs to which node. In VANETs, this protocol overhead is distributed equally over all nodes in the network. By protocol overhead is here meant the data that has to be transmitted in order to keep the MAC algorithm running and self-organizing. It does not account for ordinary protocol overhead such as header information containing addresses, forward error correction etc., which is required by all protocols. Concerning the protocol overhead involved in STDMA (clause 7.2.4.2) and MS-Aloha (clauses 7.3.3.2 and 7.3.6), they have two different approaches resulting in slightly different overhead, while CSMA does not need any overhead, or extra bytes in the protocol to function.

Time slotted MAC approaches require synchronization among nodes to function. In a centralized network, this is provided by the AP or BS, but it is distributed in decentralized networks such as VANETs. This issue is widely explored in clause 8.

7.2 STDMA

7.2.1 Introduction

STDMA [i.11] is a time slotted self-organizing MAC method, that always grants channel access for all packets before a predetermined time, regardless of the number of competing nodes. Therefore, STDMA is scalable without violating fairness and channel access delay. The channel access delay is upper bounded, implying that STDMA is predictable and it is perfectly suited for real-time communication applications such as road traffic safety. Since all nodes have equal opportunity to access the channel the algorithm is fair despite the number of nodes. Through careful scheduling of transmissions in space during high network utilization periods the reliability is maintained for the closest receivers of a transmitter (which ought to be the most interesting nodes to reach). STDMA, using parameter settings that have been adapted to the vehicular environment, is shown to perform remarkably well in a highway scenario [i.44], [i.45], [i.46] and [i.47]. The price paid for the better performance of STDMA is the required network synchronization through a global navigation satellite system, e.g. GPS.

7.2.1.1 The AIS system

STDMA is already in commercial use in the automatic identification system (AIS) for the shipping industry with focus on surveillance applications, such as collision avoidance among ships using the VHF mobile maritime band. The AIS system is standardized in ITU-R Recommendation M.1371-1 [i.9] and its use is mandatory for all ships larger than 300 gross ton and all passenger vessels regardless of size. The ships are required to carry a transponder that regularly transmits position messages using STDMA as channel access method. The first release of this standard was in 1998 and the fourth revision was ratified in April 2010, which includes new features accommodating the leisure boat industry. Previous surveillance applications for ships have been based on ground infrastructure in the harbours and along the coastline with radar support. Radar has shortcomings such as the inability to see behind large obstacles or incorrect radar images due to bad weather situations. By adding data communication, more solid information can be obtained about other ships in the vicinity and thereby accidents can be avoided. The update rate of the position messages in AIS depends on the speed of the ship. The AIS system is very similar to what is currently under development for the vehicular environment, where vehicles are going to transmit position messages, i.e. CAM, to update the LDM facility in order to support road traffic safety applications.

In STDMA, time is divided into frames and further into time slots. In AIS the frame length is 1 minute and the number of slots in each frame 2 250. The transfer rate is 9,6 kbit/s and one time slot is 26,6 ms. Two different frequency channels are used for transmissions with a bandwidth of 25 kHz each and centre frequencies of 161,975 MHz and 162,025 MHz respectively. The transponder uses both channels for transmissions and is capable of receiving on both channels at the same time, i.e. one transmitter and two receivers are required. UTC synchronization between nodes is required and is carried out using a GNSS such as GPS. A node signals in every transmission if it has direct UTC or indirect UTC. The latter is used if a node does not have a working GPS due to poor signal quality or faulty receiver. If that is the case, the node synchronizes to other nodes that signal that they have direct UTC capabilities. The AIS standard ITU-R Recommendation M.1371-1 [i.9] describes in detail the synchronization in different scenarios and also fall back solutions.

At start-up the node decides upon a report rate, i.e. how many position messages that should be transmitted in each frame. The AIS standard has certain predetermined report rates depending on the speed of the ship. Anchored ships send one message every 3 minutes, whereas ships having a speed of 0 knots to 14 knots report every 10 seconds, 6 messages per frame, and for higher speeds up to every 2 seconds, 30 messages per frame.

There are two different transponders in AIS - Class A and Class B. The mandatory part of AIS for the large ships and passenger vessels use Class A transponders where STDMA is utilized as channel access method. Class B transponders are intended for the leisure boat industry and is not mandatory. Class B transponders instead use a carrier sense TDMA (CSTDMA) scheme for channel access, which implies that channel access is not predictable. Consequently, the AIS system has introduced CSMA nodes into an already existing STDMA system.

In AIS, also base stations that are situated, for example, at harbour entrances are used. These are connected to a back-office system so that authorities can follow ships in the harbour environment. The AIS base stations also transmit information about the harbour to the approaching ship.

Håkan Lans holds a patent on STDMA [i.10], which expires in July 2012. The patent has been re-examined in the US cancelling all claims on March 30, 2011.

7.2.1.2 Position reports

In the AIS system there are 27 types of messages. The most frequently used message type is the position reports transmitted regularly by each ship. The report rate is determined by the speed of the ship and it can be as seldom as every 3 minutes (anchored ship) or as often as every 2 seconds (speed > 23 knots or changing course with a speed > 14 knots). The total message length in the AIS system is 256 bits, which fits into one time slot using a transfer rate of 9,6 kbit/s. In figure 8, the generic message structure in AIS is depicted containing 248 bits. The missing 8 bits are used for TX ramp up in the beginning of the packet transmission. The message identification (MSG ID) field determines the content in the data field. The user identification number (User ID) is unique to the vessel in question and obtained by the authorities of the country in which the ship is registered. The communication state field contains necessary information about the slot currently carrying a position report. The frame check sequence (FCS) is a 16-bit cyclic redundancy check (CRC). The buffer of 24 bits contains 4 bits for bit stuffing, distance delay of 12 bits, repeater delay of 2 bits and synchronization jitter of 6 bits. The duration of one bit in AIS given a transfer rate of 9,6 kbit/s is 104 µs. Therefore, the distance delay will be approximately 212 nautical miles and the purpose with the delay is to provide protection for propagation distances of at least 100 nautical miles, which is equivalent to 185 km. The synchronization jitter allows for ±3 bits or ±312 µs difference between source and destination.

24	8	6	30	113	19	16	8	24	= 248 bits
Preamble	Start flag	MSG ID	User ID	Data	Communication state	FCS	End flag	Buffer	

Figure 8: The generic message structure in the AIS

In table 2 the different parts of the data field in the position reports are tabulated.

Table 2: The different parameters in the data field of a position message

Parameter	Number of bits	Description
Repeat indicator	2	There are repeaters available in AIS and this parameter indicates how many times a message has been repeated.
Navigational status	4	Reports the status of the ship such as at anchor, aground, fishing, under way sailing, under way using engine etc.
Rate of turn	8	Reports the rate at which the ship turns.
Speed over ground	10	Speed over ground.
Position accuracy	1	If set to 1 if the position accuracy is ≤ 10 m. Otherwise it is 0.
Longitude	28	Reports the longitude of the ship.
Latitude	27	Reports the latitude of the ship.
Course over ground	12	Course over ground.
True heading	9	The heading of the ship in degrees.
Time stamp	6	UTC time when the position report was generated.
Special maneuver indicator	2	Used for inland waterways.
Spare	3	Not used.
RAIM-flag	1	Receiver autonomous integrity monitoring (RAIM) flag is associated to the GNSS receiver used and provides information about the position accuracy information provided by the GNSS.

In table 3 the different parts of the communication state field is tabulated.

Table 3: The different parameters in the communication state of a position message

<table>
<tr><th>Parameter</th><th>Number of bits</th><th colspan="2">Description</th></tr>
<tr><td>Sync state</td><td>2</td><td colspan="2">This parameter reports in which synchronization state the node is in, which are four different; UTC direct, UTC indirect, synchronized to a base station or synchronized to another mobile node.</td></tr>
<tr><td>Slot time-out</td><td>3</td><td colspan="2">The number of times this particular slot will be used until a new slot is selected and 0 means that it is the last time and 1 to 7 the number of remaining frames until slot change.</td></tr>
<tr><td rowspan="6">Submessage</td><td rowspan="6">14</td><td colspan="2">The submessage parameter contains different information depending on the slot time-out value.</td></tr>
<tr><td>Slot time-out</td><td>Content of submessage</td></tr>
<tr><td>0</td><td>Contains the slot offset to the new allocated slot in the next frame.</td></tr>
<tr><td>1</td><td>Contains the UTC hour and minute if it is available.</td></tr>
<tr><td>2, 4, 6</td><td>Contains the slot number.</td></tr>
<tr><td>3, 4, 7</td><td>Contains the number of other stations this node is receiving currently.</td></tr>
</table>

7.2.1.3 Overhead to run the STDMA algorithm

The bits that are present in the position message that are directly tied to maintaining the STDMA algorithm is the bits contained in the communication state field in figure 8, which are 19 in number. Except for these bits, the algorithm will, in situations when the network becomes overloaded, also require the positions of each and every node within radio range. The positions are used by each node locally to schedule simultaneous transmissions in space when the network load increases. This intentional slot reuse is described in detail in clause 7.2.6. The part of the position report required to schedule transmissions in space is the longitude and latitude data, found in the data field in figure 8, which are 28 and 27 bits respectively. The other parameters contained in the data field of the position report in table 3 are not necessary for the STDMA algorithm in particular, but instead they can be used by applications on higher layers. In total STDMA needs 74 bits to function or 10 bytes (if adding 6 spare bits).

It should be noted that STDMA nodes only transmit information about how many nodes they currently receive information from, in the submessage of the communication state field. No other information regarding, e.g. which nodes or what kind of information that can be received is transmitted. This is often the case with other self-organizing time-slotted MAC schemes, that nodes transmit their status of the frame allocation to all other nodes. This is to prevent unintentional slot reuse by hidden terminals as described, for MS-Aloha, in clause 7.3.

7.2.2 Parameters

By assuming the same physical layer as in IEEE 802.11p [i.2] and the same frequency band of 5,9 GHz, the timing constants involved in AIS needs to be updated to fit the vehicular environment. A more suitable frame duration could be 1 second and a transfer rate of 6 Mbit/s, which is the default rate selected by ETSI for CAMs. Depending on the default transfer rate and packet lengths, the number of slots in a frame will be determined. This number is determined in advance. It will not be possible to change the slot duration in a system under operation. However, the physical layer of 802.11p offers several transfer rates and hence different packet lengths could be supported within the same slot size by using these.

There are eight different STDMA parameters used for running the algorithm internally; report rate (RR), nominal increment (NI), selection interval (SI), nominal start slot (NSS), nominal slot (NS), nominal transmission slot (NTS), minimum time-out (TMO_MIN), and maximum time-out (TMO_MAX). In table 4 explanations to the different parameters are given.

Table 4: The different parameters associated with STDMA

Name	Abbreviation	State	Description
Report rate	RR	Fixed	The RR is the desired number of position messages that is to be sent during one frame.
Nominal increment	NI	Fixed	The NI is the number of slots that will elapse on average between two consecutive position reports. It is derived by using the following equation: NI = 2 250 / RR, where the total number of slots in the frame is 2 250.
Selection interval	SI	Fixed	SI is the subset of slots that the node is allowed to choose from during each NI. SI is 20 % of NI and thereby SI is also given in number of slots.
Nominal start slot	NSS	Fixed	This slot determines where the very first slot of the internal frame and the SI is placed around NSS, letting NSS be the center slot.
Nominal slot	NS	Fixed	This slot is placed NI slots away from NSS and is the center slot of the next SI.
Nominal transmission slot	NTS	Dynamic	NTS is the slot chosen for transmission within SI. Each NTS is likely to be different in every SI.
Slot time-out maximum	TMO_MAX	Fixed	The maximum number of times a specific NTS can be used for transmission. In the AIS standard this has a value of 8, implying that a specific NTS can only be used for up to 8 frames.
Slot time-out minimum	TMO_MIN	Fixed	The minimum number of times a specific NTS can be used for transmission. In the AIS standard this has a value of 3, implying that a specific NTS can be used for at least 3 frames.

In figure 9 the frame structure of STDMA with the different parameters is depicted. The RR determines the NI and the SI. If RR, for example is 10 messages per frame, there will be 10 NI and 10 SI in each frame. The NI will be 225 slots and each SI will contain 23 slots that the node is eligible to select from for transmission. There is always one NSS, whereas the number of NS is equal to RR - 1. The NTS are the actual transmission slots, which are found within each SI, and each NTS has an integer, *n*, drawn from the uniform distribution [TMO_MIN, TMO_MAX], attached to it. This *n* determines for how many consecutive frames this particular NTS will be used for transmission. When the NTS has been used during *n* frames, a new NTS is selected within the SI and a new random number is attached to it. A node is not allowed to use the same NTS directly - it is always forced to change NTS whenever the *n* value reaches zero, to cope with network topology changes. The position of one NTS within one SI is uncorrelated with the position of the NTS of the following SI. In the example in figure 9, there are three position messages to be transmitted during one frame, implying three NI and three SI in each frame. There is one NSS and two NS. Although the position of the NSS is near the end of the global STDMA frame, it is actually the start of the local frame for this example node. All STDMA nodes use the same numbering of slots, starting with slot 0 when the global STDMA frame starts, but, each node has its own local frame start, which is where the NSS is placed. Hence, nodes are slot synchronized and not frame synchronized. The placement of NSS is described in clause 7.2.3. Further, in figure 9, the attached integer, *n*, determining the number of times a particular NTS is kept is also pointed out as the frame advances. In every transmission, the node signals for how many times more this particular slot is going to be used.

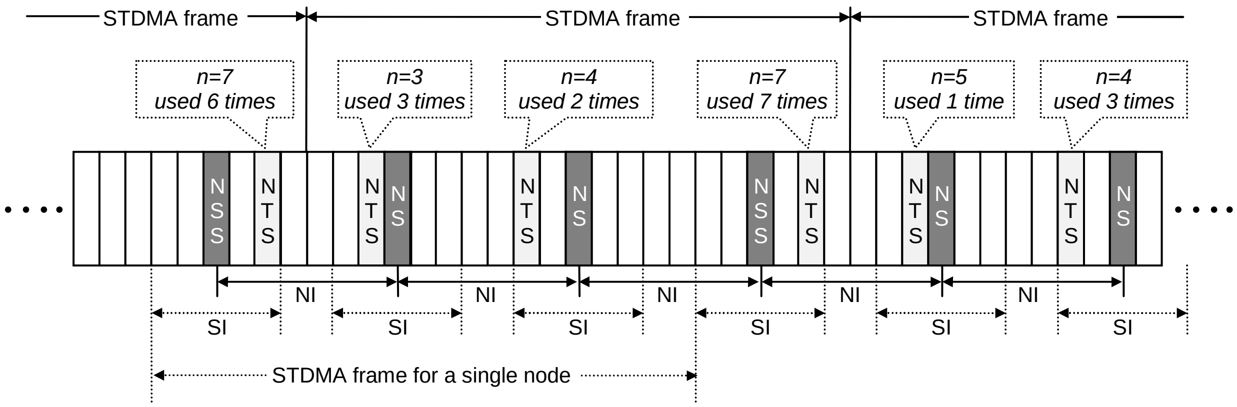


Figure 9: The global STDMA frame and the STDMA frame as used by one node with the different parameters described in table 2

7.2.3 Channel access procedure

When the node is turned on it follows four different phases: *initialization*, *network entry*, *first frame*, and *continuous* operation.

7.2.3.1 Initialization

During the *initialization* the node listens to the channel activity for one frame to determine the current slot allocation. During this time, the node builds its own frame map to reflect the occupied slots and it also collects information about the status (e.g. position, speed, and heading) of the current members of the network. The STDMA frame in the AIS system starts every UTC minute and the slots are numbered from 0 to 2 249. The local frame start for a node does not necessarily coincide with the STDMA frame start. Instead the first slot the node listened to will be the local frame start for that node. In the example in figure 10, the node starts its local frame with slot number 6.

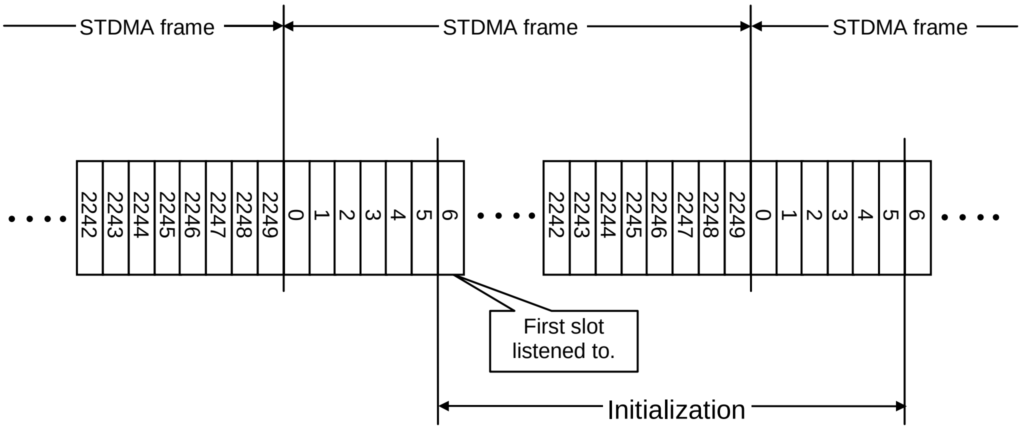


Figure 10: The STDMA frame and the initialization phase which does not necessarily coincide with the STDMA frame

7.2.3.2 Network entry

The *network entry* phase follows the *initialization*. In this phase the node introduces itself to the network for the first time. The *network entry* phase only lasts for a minor part of the frame: from the last slot in the *initialization* phase until the first transmission slot has been selected, i.e. the first NTS. When the last slot in the *initialization* phase is reached, the node randomly selects a slot located between the last slot and NI slots away and assigns this slot to be the NSS. In figure 11, this procedure is depicted and SI is placed with NSS in the middle. After the *initialization* phase the node is aware about the slot allocation in the whole frame and consequently which slots that are occupied in its current SI. The node now randomly selects a slot that the node perceives as being free among the slots in its SI. Note that the node is only allowed to choose a slot for transmission within its SI. If there are no free slots within SI, the node will use an occupied slot for its transmission, which belongs to the node situated furthest away from itself geographically. Recall that each node knows the position of every other node in the network due to the exchange of position messages.

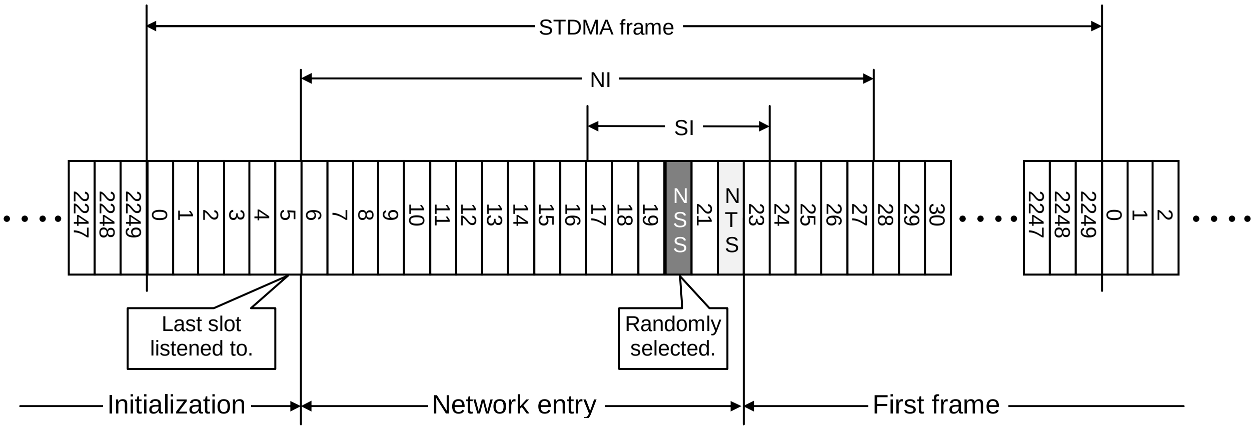


Figure 11: The STDMA frame and the initialization phase which does not necessarily coincide with the STDMA frame

7.2.3.3 First frame

During the first frame the node continues to allocate slots, i.e. NTS, and attach random integers, *n*, to every NTS. One NI is added to the NSS and this new slot in the centre of the next SI is called NS. Note that the actual transmission does not necessarily take place in NSS or NS - they are merely used to position each SI evenly in the frame. Instead, a new transmission slot is randomly selected within this new SI among the candidate slots (the slots within SI that are perceived to be free by this node) and is denoted NTS. When a transmission is performed in a selected NTS, the offset to the next upcoming NTS is also included in the transmission made in the current NTS, i.e. prior to transmission of current NTS the next NTS is selected to be able to include the offset to the next NTS in the current NTS. This is done to avoid concurrent transmissions by nodes temporarily being hidden from one another due of fading or shadowing. This is a feature to cope with the natural impairments of the wireless channel.

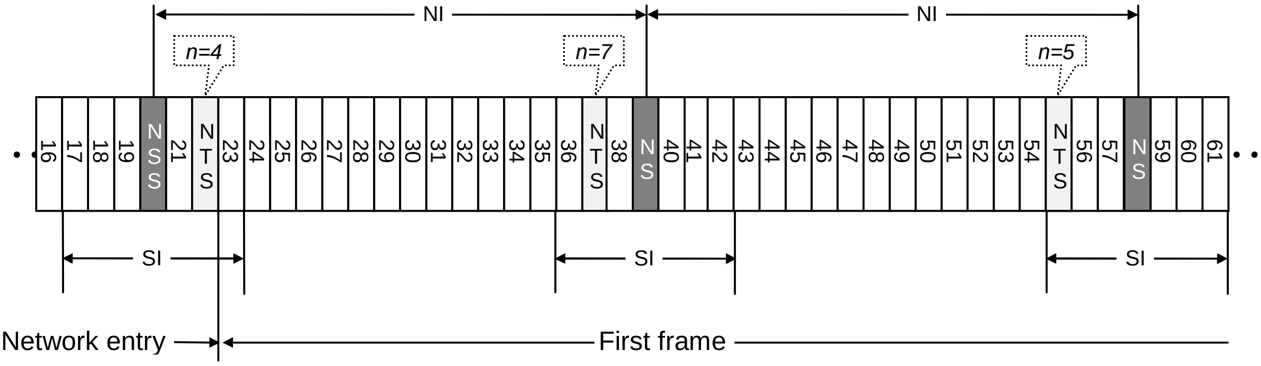


Figure 12: The STDMA frame and the initialization phase which does not necessarily coincide with the STDMA frame

7.2.3.4 Continuous operation

When the node reaches its NSS again (one frame has elapsed) and it has allocated all NTS determined by the RR during the *first frame* phase the node enters *continuous operation*, figure 13. Now the node is introduced to the network and the rest of the nodes, being in radio range of this node, are aware about upcoming transmissions. The NSS, and all NS and SI now remain constant during the continuous operation. Instead new NTS are selected regularly. In figure 13 it is also pointed out that the random number attached to each NTS has been decremented as a new frame advances. When the number of times one NTS is allowed to be used has reach zero, the node select a new slot within the same SI among the slots that are currently perceived as free. A node is not allowed to use the same NTS again by just attaching a new random number to it. It is forced to select a new NTS and attach a new random number to it from the uniform distribution [TMO_MIN, TMO_MAX]. This is done to avoid using of the same slot of nodes within radio range that selected their slots when there were out of range of each other. This is a feature to cope with network topology changes.

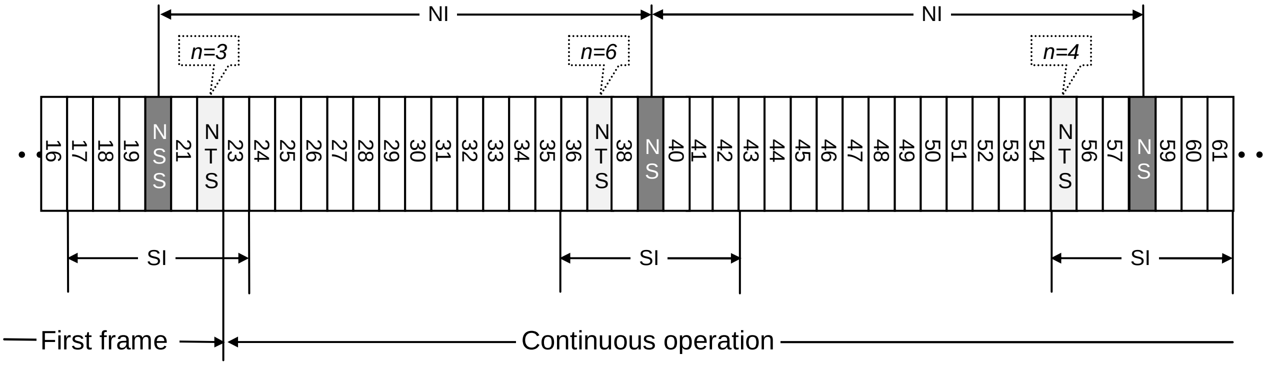


Figure 13: The node reaches its NSS and enters the continuous operation

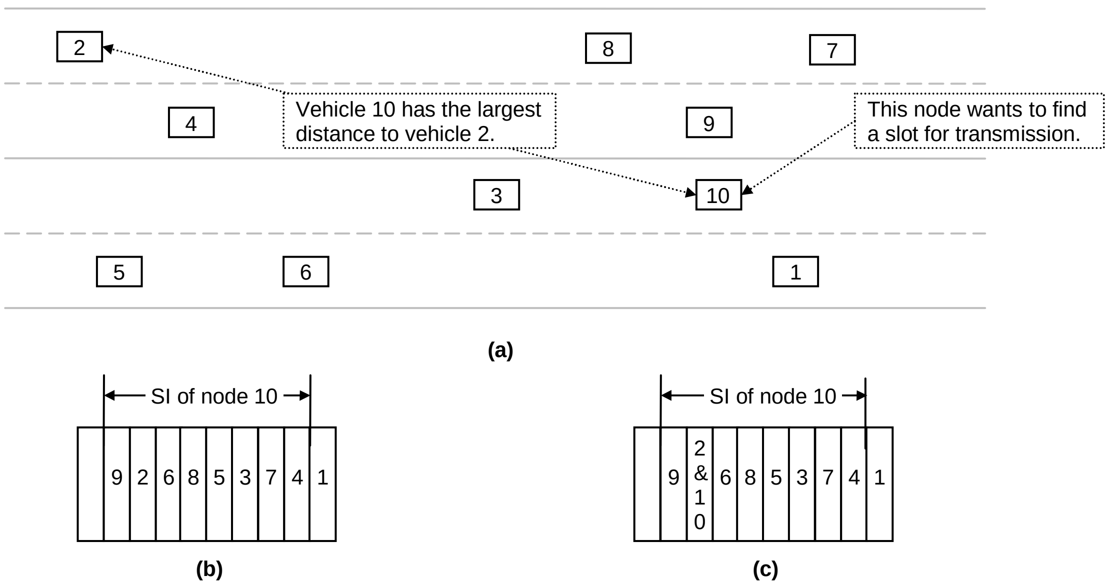
The node is allowed to change its report rate during continuous operation. The change of report rate could for example occur when a node increases or decreases its speed. New NI and SI are then determined together with new positions of NSS and NS, respectively. However, the node is already present in the system and can therefore just utilize slot offsets for announcing new upcoming transmissions.

7.2.3.5 Summary

The node divides the STDMA frame into a number of equal groups of slots called NI. NI is the number of slots elapsing on average between two consecutive transmissions. The number of NIs in the frame is the same as the RR. To every NI is one SI, i.e. a group of slots that the node is eligible to select from for transmission. The SI is 20 % of the number of slots contained in NI. The slot selected for transmission within the SI is called NTS and to the selected NTS a random integer is attached (time-out value). When *n* reaches zero, it has used the NTS for the predetermined number of times and it selects a new NTS and attach a new random number to it. The slots outside the SI of a particular node are not used for communication by that node. In the middle of each SI an NS is situated. The first NS in the frame for one particular node is called the NSS and is said to be the "frame start" for this node. Due to this, there are as many possible "frame starts" for individual nodes as it is slots in the frame. The NSS plays a role when the node is in its start-up phases since it is used for keeping track of the different phases. However, when the node enters continuous operation its significance diminishes, i.e. it becomes a NS in practice. All nodes in the system have their own NS placement and since it is a repeatable pattern, nodes have NI possible ways to place its NS (provided that they have the same RR). All nodes have their own perception of the slot allocation in the frame. However, nodes close to each other will have similar slot allocation maps since they receive the same transmissions. During continuous operation the node sees the STDMA frame as a ring buffer, where relative offset are used when there is a NTS change due to the time-out value reaching zero.

7.2.4 Simultaneous transmissions

When there are more requested resources than available time slots, i.e. all slots within an SI are occupied, the node selects a slot for transmission already allocated by another node. The selection of which slot to use for transmission is done based on the positions of other nodes. As the information of positions is included in every transmission, all nodes are aware of the positions of all other nodes within range. A node selects a NTS that is occupied by the node situated furthest away from itself. In figure 14, a situation of this intentional slot reuse is depicted. Figure 14 (a) shows 10 vehicles situated on a road, all within radio range of each other. Vehicle number 10 wants to select a slot for transmission from the slots in its SI. However, it finds its SI fully occupied with vehicles 2 to 9, figure 14 (b). Vehicle 10 then chooses to transmit at the same time as vehicle 2 by using its slot, since this vehicle is furthest away from vehicle 10 among all the vehicles that has allocated slots in the SI of vehicle 10, figure 14 (c). Note that there is an empty slot available, but it cannot be selected as it is not part of the SI of vehicle 10. This feature of allowing nodes to select a slot even though the whole SI is fully booked enables STDMA to handle overloaded situations. In other words, the algorithm is scalable and predictable since a channel access is always guaranteed.


2
8
7
Vehicle 10 has the largest distance to vehicle 2.
4
9
This node wants to find a slot for transmission.
3
10
5
6
1
(a)
SI of node 10
9 2 6 8 5 3 7 4 1
(b)
SI of node 10
9 2&10 6 8 5 3 7 4 1
(c)

(a) A road with 10 vehicles, where vehicle 10 is searching for a new transmission slot;
(b) no slot available in the SI of vehicle 10; and
(c) vehicle 10 selects to transmit at the same time as vehicle 2.

Figure 14

We denote this feature of selecting a transmission slot that is already occupied as *pinching* of the slot. In the AIS system, there are three restrictions when pinching a slot:

- A node is not allowed to use a slot allocated by a base station if the ship is closer than 120 nautical miles to the base station.
- If the position information of the node using a slot for some reason is not present (i.e. the slot is occupied but no position information is available), this slot is not eligible to be selected for transmission. The lack of position information could be due to a faulty GNSS receiver or decoding failure.
- A node searching for a suitable transmission slot is not allowed to pinch a slot occupied by the same node twice during a frame.

An example of the last restriction is found in figure 15. Here vehicle 10 has 3 SI (SI$_1$, SI$_2$, and SI$_3$) in each frame. All slots in all SIs are occupied with other transmissions. In SI$_2$ the slot of vehicle 2 was not available to use since this was pinched already in SI$_1$. In SI$_3$ neither the slots of vehicle 2 nor vehicle 5 are allowed to be used by vehicle 10 due to earlier pinching actions.

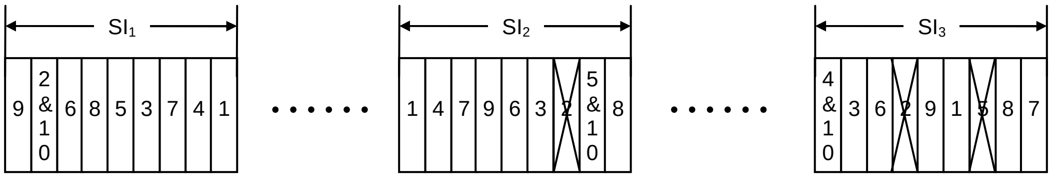


Figure 15: Shows how the slot allocation is performed when all slots within the SI are occupied and the same node's slot is not permissible to use in consecutive SIs in the same frame

These simultaneous transmissions or intentional slot reuse, although scheduled to be as far as part in space as possible, will decrease the reception probability for nodes situated in between the concurrent transmitters. However, due to frame capture not all nodes will experience collision at their receivers. For the example in figure 15, nodes 1, 7 and 9 are likely to receive the transmission from node 10, whereas nodes 4 and 5 are likely to receive the transmission from node 2. The simultaneous transmissions will decrease the effective communication range for every transmitter. However, in dangerous situations it is the closest nodes that are the most interesting to reach and those are protected due to the scheduling in space. In other words, the effective "cell" size of each concurrent usage of the same slot will decrease due to interference.

There also exists some unintentional slot reuse in STDMA, implying that nodes select the same slot for transmission without being aware of that the slot is actually occupied by someone else. A prerequisite for unintentional slot reuse is that two nodes have partially or totally overlapping SI. The unintentional slot reuse is mainly due to two reasons: (*i*) two nodes selected the same slot for transmission before they were within radio range of each other and (*ii*) two nodes close to each other with the same perception of free and allocated slots in their SIs chooses the same free slot for transmission.

The effects of intentional and unintentional simultaneous transmissions will be evaluated further in TR 102 861 [i.43].

7.2.5 Summary

Recall that the road traffic safety applications requirements on the MAC protocol are; delay, reliability, and fairness. Since every node in an STDMA network is always granted channel access, the channel access delay is upper bound and the algorithm is fair because all nodes have equal opportunity to access the channel. The reliability is affected when simultaneous transmissions take place, but due to careful scheduling in space the closest receivers are protected.

The *ad hoc* topology enforces the following requirements on the MAC protocol; self-organization, reactiveness, mitigation of hidden terminal situations, and scalability. STDMA is designed to self-organize and it regularly forces nodes to change slots to cope with the rapid network topology changes in the VANET. Further, STDMA is designed to handle overloaded situations implying that simultaneous transmissions will be allowed in slots when there are no free slots available. The selection of simultaneous transmission slots is optimized based on the maximum distance between two nodes within radio range. In other words, a node that is forced to select an occupied slot will transmit at the same time as another node situated furthest away from itself. The outcome in overloaded situations is that the effective "cell radius" around a transmitter will decrease, implying that the number of nodes that are reached at larger distances will decrease. The closest nodes, which are likely to be the most interesting to reach in a road traffic safety scenario, are in this way protected and a high packet reception probability can be maintained for these nodes. In [i.49] it is shown that in a situation with a network load of 400 % STDMA is still working properly and nodes receive packets. STDMA is thus proven to be scalable.

The technique for mitigation of hidden terminals in STDMA consists of the transmission of the offset for the next slot, i.e. each node signals its intention to use an upcoming slot well in advance. Note however, that it was shown in [i.50] in a highway scenario with a fading channel model that the hidden terminal situations do not contribute to a major performance degradation when looking at the packet reception probability.

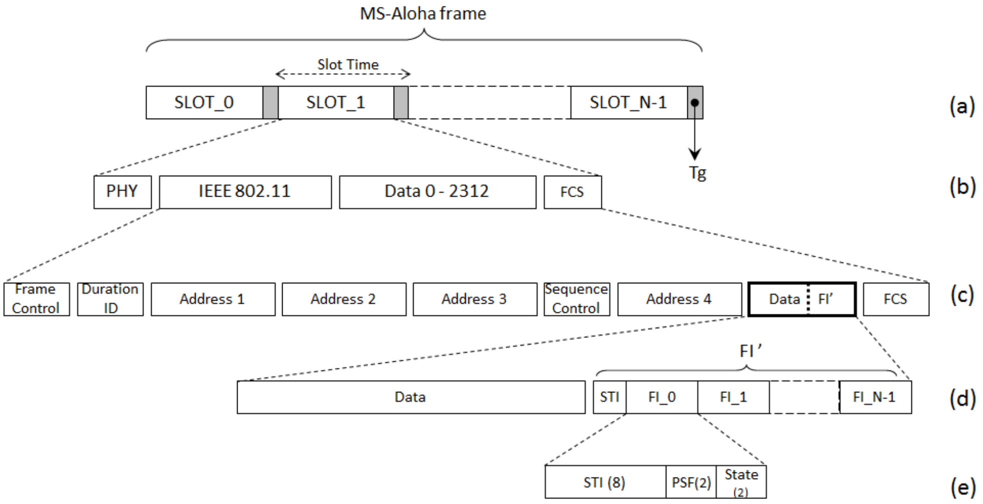
7.3 MS-Aloha

7.3.1 Introduction

MS-Aloha is a slotted MAC protocol, specifically designed for VANET: it addresses the issues of *scalability* (i.e. effective slot reuse and non-blocking behaviour) and *reliability* (connection-oriented paradigm and prevention of hidden terminals and unintentional slot re-use) by distinctive mechanisms which are built thanks to the knowledge of physical layer parameters (received power). It also manages priority (by pre-emption) to increase *flexibility*. It has been defined [i.32] and demonstrated (by simulations) to work under mobility and in very congested urban scenarios [i.33] and [i.34] with outstanding results. In this introduction all the main features of the protocol are shortly mentioned and in the clauses 7.3.2 and 7.3.3 they will be discussed separately. In clause 7.3.4 the settable parameters of MS-Aloha are shortly recalled.

Finally clause 7.3.5 summarizes the available protocol features and emphasizes the main characteristics and advantages of the proposed protocol for VANET communications and applications.

In MS-Aloha, all the nodes are supposed to share a common synchronization source (*e.g.* GPS or Galileo receiver) and a common periodic frame structure (figure 16(a)), divided into slots which represent the distinct resources that can be allocated. In order to counteract propagation delays, a guard-time *Tg*) is also added (figure 16(a)).



(a) MS-Aloha frame structure: Slots 0...N-1 with Guard Times Tg;
(b) 802.11p-compliant L1-L2 frame within each slot;
(c) L2 fields, 802.11p-compliant: FI' embedded in Data subfield;
(d) the FI' field and its FI subfields FI_i (as many as the number of slots): STI identifier embedded in FI';
(e) information contained in each FI_i subfield (state, priority, STI). For reasons of space the fields shown (in particular FI) are not in scale.

Figure 16: MS-Aloha frame structure

All the nodes append to the packet an exhaustive description of how each slot is perceived (*free*, *busy*, *collision*). This information is contained in the Frame Information (*FI*) structure - (figure 16 (b)). In its default configuration, the *FI* has as many 12-bits subfields as the number of slots in the frame; each subfield contains a short identifier of the node who has been allotted the slot (*STI*), the priority of the connection and the state (*free*, *busy*, *collision*). The FI is meant to propagate network information over three hops, preventing unintentional slot re-use and improving SINR and reception rate. In [i.35] a method to prevent *STI* exhaustion also in VANET context was proposed, giving it a temporary *label* meaning, and continuously swapping it. More details in clause 7.3.3.2.

In fact, a node *A* infers the state of each slot both by direct sensing and by the correlation among the received *FI*s and, based on them generates its own *FI*: thus the information contained in the received *FI*s is somehow aggregated and forwarded by *A*. Altogether the *FI*s provide a *redundant* and *diversified* information on the slots' state and intrinsically prevent hidden terminals, thanks to the aggregation mechanism. The *FI* trailer can be appended to all MS-Aloha's frames or only on a subset of them.

7.3.2 Channel access procedure

MS-Aloha is based on the following, simple, basic mechanisms:

- Absolute synchronization exists.
- Each node appends to all its frames a trailer (Frame Information (*FI*) - (figure 16) where it describes how each slot is perceived (*free*, *busy*, *collision*). The *FI* has as many subfields as the number of slots in the frame; each of them contains the state of the slot (*free*, *busy*, *collision*), a short identifier of the node who has been allotted the slot (*STI*), and the priority of the connection.
- A node *A* infers the state of each slot both by direct sensing and by the correlation among the received *FI*s and, based on them generates its own *FI*. In MS-Aloha each node is supposed to aggregate in its *FI* all the *FI*s received: if node *A* receives a *FI* announcing slot *J* engaged by *X*, than *A* forwards it. If it receives two *FI* announcing the reservation by different nodes (say *Y* and *Z*) of the same slot *J*, *A* announces a collision in *J*.

- A node tries to reserve a slot by simply picking a free one, based on its direct channel sensing and on the *FI*s received. The same mechanism is applied if it already owns a resource and wants to continue its transmission in the next frame. Consequently, reservations are confirmed at each transmission. This helps manage mobility in a completely distributed way, without any central decision.
- The reservation state of a slot is not forwarded more than two-hop far from the transmitter, in order to enable slot re-use.

The implementation of these features requires the resolution of some practical problems, which are discussed in clauses 7.3.2.1 and 7.3.2.3. Additional mechanisms are available to improve protocol performance and prevent protocol blocking. They are discussed in clause 7.3.3.

In MS-Aloha, a node reserves a slot based on its direct and indirect channel perception and reservations are confirmed at each transmission. This helps to manage mobility in a completely distributed way, without any central decision. Collisions may occur in the initial contention phase, but, thanks to the continuous forwarding of channel allocation, they can be effectively detected and resolved. This redundancy not only prevents hidden terminal but also counteracts the effects of fading on signalling.

Reversely the signalling can hinder slot re-use. The 2-hop Spatial Multiplexing (*2-SM*) is mechanism introduced in [i.32] to facilitate slot re-use. This algorithm assures that the information on channel state (FI) is not forwarded more than two-hop far from the transmitting node (and used more than three-hop far), avoiding early resource exhaustion. 2-SM mechanism allows also the introduction of the concept of slot re-use correlated with power and radio-range. Based on this idea, MS-Aloha was further extended [i.34] to force slot re-use acting on the area where a slot is announced *busy*. A logical threshold (*Thr*) at MAC layer is adopted for this purpose: only frames received with a power higher than *Thr* are considered for the MAC analysis on *FI*. On the contrary, packets with lower power may be received by upper layer (depending on SINR as usual), but do not contribute to the *FI* of the node (as if they were not received). In this way, the minimum distance where a slot is kept busy is decreased, causing also a reduction in the minimum possible distance where the same slot can be re-used. This solution slightly modifies the *2-SM* approach into 2-hop Spatial Multiplexing with Thresholds (*2-SMt*), falling in the domain of a cross-layer PHY-MAC mechanisms (MAC decisions are based on physical layer parameters).

The mechanism of *2-SMt* gives the opportunity to solve the problem of MS-Aloha blockage: in fact if *Thr* is increased, the minimum distance for slot re-use lowers. However the solution may be said to be only conceptual, because it leaves two open issues: *(i)* how high *Thr* should be; *(ii)* based on what settings or performance metric should *2-SMt* be activated. For filling this gap the algorithm of *2-SMt* was further generalized by some additional mechanisms which led to the definition of *dynamical 2-SMt* (*2-SMtd*).

In 2-SMtd the usage of thresholds is made dynamical and distributed so that each node should separately - independently of the others - set its *Thr*, based just on its perception of the channel. Secondly the idea of fixed thresholds can generalized to a *continuum*: not just an only setting exists for *Thr* but, rather, the opportunity to move it up and down in fixed steps (say, for instance 3 dB). Finally a straightforward rule to master decisions on thresholds is proposed: since each node keeps trace of the congestion state of the channel by the number of free (and engaged) slots, this number can drive the variations of the thresholds. Also *2SMtd* has been validated by simulations.

2-SM, 2-SMt and 2-SMtd fall in the area of slot re-use and simultaneous transmissions: they are then extensively discussed in clause 7.3.3.

7.3.2.1 Memory refresh

FI are exchanged by nodes to share their view of the channel. A problem hence arises about the persistence of the *FI* information within nodes and in the network. Excessive persistence should be counteracted so to cope with the topology and load changes, mainly due to mobility. In fact, in VANETs, a MAC protocol needs to promptly react to several network conditions in order to avoid resource waste and insubstantial channel allocations.

A common and dangerous situation could occur, for example, when the information of the slot allocation is not refreshed by the owner. Consequently, once a slot *j* had been assigned to a node *A*, and this information had been announced all over the domain (e.g. more than 2-hop far from the transmitting node), even if *A* gave up transmitting, the slot state would be frozen and the slot would be continuously announced as busy. In this case, the slot *j* would be unusable around the network, causing a possible blocking state for the channel.

For these reasons, in MS-Aloha each node periodically refreshes its memory (on slot allocations). Concerning the possible setting of the refresh time, it should be greater than the frame time; otherwise the information would not have enough time to be certainly announced 2-hop far. Vice-versa, if the refresh time were higher than frame-time, it would increase the latency and lead, however, to "fake" undesired collisions.

In MS-Aloha each node flushes the information on slot *j* when the frame has reached again the position *j* (the information on slot allocation expires after a frame-time). This memory refresh-time has been demonstrated [i.31] to be long enough to avoid propagating insubstantial information while getting an actual knowledge of wireless channel state.

7.3.2.2 Solutions against protocol overheads

The only additional overhead introduced by MS-Aloha is in the *FI* trailer which is appended to each transmission, in order to describe the state of the channel.

In principle, the *FI*, can be regarded as a PLCP function, since it adds medium-dependent information to the frame. From a practical point of view, the *FI* it can be appended to the data being transmitted, so to enforce backward compatibility to CSMA/CA. The *FI*, which includes as many FI_j sub-fields as the number of slots, each describes how the slot is perceived by using the following 12 bits:

- *STI* (source temporary identifier) - 8 bit: a short identifier of the node *L*, the node which has been deduced as the owner of slot *j* (by the transmitting node *M* which builds the *FI*). The identifier is ***STI* is used only by the signalling mechanisms of MS-Aloha, in order to identify**. The *STI* is empty if the slot is unused.

- *PSF* (priority status field) - 2 bit: field indicating the priority of data transmitted in the slot. It is used for pre-emption mechanisms.

- *STATE*: a 2-bit long field indicating *j*th-slot state.

Consequently, each *FI* is 12 X *N*-bit long (*N* is the number of slot in a MS-Aloha period). This means that the overall FI_j is limited, otherwise a dangerous overhead may be introduced, given the effect of multiplication by *N*.

In more detail:

- It has already demonstrated [i.31] that, if FI_j is 12-bit long, then the overhead introduced is acceptable and lower than CSMA/CA's one (due to statistical waiting time).

- The overhead introduced is sufficient to make MS-Aloha fully deterministic, unlike the other slotted MAC: *(i)* it manages spatial multiplexing at more than two hops, *(ii)* minimizes interference by unintentional slot re-use by hidden terminals, *(iii)* can achieve *ideal* packet reception rate. Notably, without this overhead, no protocol can guarantee an ideal performance even in proximity of the transmitter).

However this holds if the protocol can manage node identification by a short identifier; this is the case of a 8-bit *STI*. Notably, the 8 bits of *STI* only allow 256 nodes to be distinguished, which can appear to be limiting in an urban context. Anyway, it is not a problem if two nodes choose the same *STI*, unless they attempt attempt to access the same slot. In fact, *STI* is meant only to determine collisions by the *FI* analysis. If the same *STI* is used by different nodes but in distinct slots, the identification can still be ensured by the couple "slot number + *STI*". Consequently, the only ambiguous case happens for the statistically not-negligible event of two nodes randomly selecting the same *STI* and free slot. In that case the *STI* would not permit to highlight the collision.

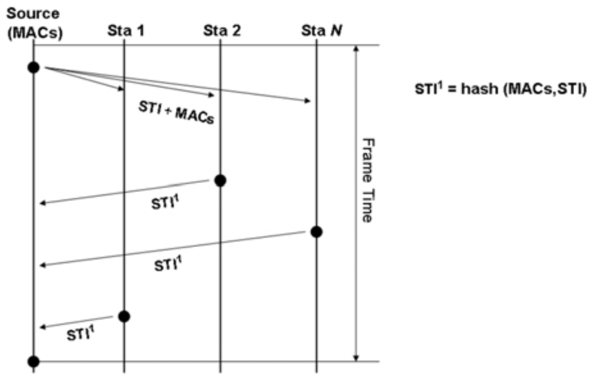


Figure 17: The label swapping approach for the scalability of STI space

This threat was finally solved [i.31] by introducing a *STI* swapping mechanism (depicted in figure 17), specifically aimed at resolving the remaining logical conflicts among the *STI*s. The "label swapping" algorithm is based on the following rules:

- The unused information of the source MAC address is used to resolve different nodes. Notably, a MAC address - for instance the MAC of node *A* using a given slot *j* - spans only one hop. At the second hop, in fact, only the information summarised by *FI* is broadcasted (this contains A's *STI*, not its MAC addresses).

- Every time a node receives a frame directly from node *A*, it computes a new *STI'*A, based on some hashing between *STI*A and *MAC*A. All the nodes compute the same *STI'*A.

- The other nodes, which are two-hop far from the node *A*, just receive *STI'*A and, can use it in their *FI*s. They even do not know about *STI*A, therefore, no ambiguities occurs.

- *STI* assumes a "temporary duration" and *STIs* are swapped at each *(i)* transmission by A and *(ii)* acknowledgment(s) by the others. Consequently, also *STI* are refreshed accordingly to the memory refresh.

In practice, even if two nodes, *A* and *B*, choose the same *STI*A = *STI*B, the nodes receiving such information (say node *C*, *D* and *E*) will not just propagate the *STI*s in their *FI*s, but will generate new 8-bit *STI* label, based on a hashing of the STI and of the MAC source (respectively *STI'*A, *STI'*B). *C*, *D* and *E* will compute the same *STI'*A, *STI'*B because they have also received *A*'s and *B*'s MACs.

There is still a non-null probability that also the *STI'*s cannot resolve the stations (also *STI'A* = *STI'B*); however the process is further carried on in the same way: when transmitting in next period, *A* it will generate and use a new *STI''*A, and so on. This would sooner or later solve this quite unlikely event.

The chosen memory refresh time (clause 7.3.3.1) prevents any potential additional issues, as the is flushed memory after an MS-Aloha period: this synchronizes the label swapping process, as well.

Another possible way, to further counteract the already limited overhead caused by the *FI*, is to adopt mechanisms avoiding the continuous *FI* transmissions. For instance the *FI* could be alternatively sent or not by a node on a period base. This, for instance, has been proposed for DTDMA (clause 7.4) [i.40] and could be adopted, as well, by MS-Aloha. However the approach should be apparently discouraged for the following reasons: *(i)* the overhead has already been demonstrated to be acceptable - and even negligible considering the typical times involved by CSMA [i.34]; *(ii)* by sending *FI*s in each slot, the reaction-time achieved is no longer than a period; consequently, even in case of collisions, the network can promptly re-organize itself. In a wider perspective, aiming at *determinism*: the reaction-time should not be weakened.

7.3.3 Simultaneous transmissions

A slotted protocol needs to reuse slots in order to prevent resource exhaustion and channel blocking. In fact, if a slot could be used only once throughout the network, then the bandwidth would be blocked as soon as the number of nodes exceeds the number of slots in the frame structure: this situation really contrasts the hypothesis on the number of nodes in a VANET which, in principle, are not predictable.

On the other hand, slot re-use should be carefully managed so to limit interferences. In fact, if a slot is not re-used far enough, it results in strong interferences and poor reception rates.MS-Aloha manages slot re-used based on received power. Thanks to the information included in its *FI* trailers simultaneous transmissions in MS-Aloha satisfy the following:

- No simultaneous transmissions by hidden terminal (clause 7.3.3.1).

- No unintentional slot re-use (clause 7.3.3.1).

- Slot re-use at 4 hop distance (clause 7.3.3.2) to limit interference.

- Slot re-use based on received power, on a dynamical way based on congestion, so to shrink the width of each hop (clauses 7.3.3.3 to 7.3.3.4).

7.3.3.1 Prevention of hidden terminals and unintentional slot re-use

All the nodes append to the packet an exhaustive description of how each slot is perceived (*free*, *busy*, *collision*). This information is contained in the Frame Information (*FI*) structure - (figure 16). The *FI* has as many subfields as the number of slots in the frame; each subfield contains a short identifier of the node who has been allotted the slot (*STI*), the priority of the connection and the state (*free*, *busy, collision*).

Conceptually a node *A* infers the state of each slot both by direct sensing and by the correlation among the received *FI*s and, based on them, generates its own *FI*: thus the information contained in the received *FI*s is somehow aggregated and forwarded by *A*. Altogether the *FI*s provide a *redundant* and *diversified* information on the slots' state and intrinsically prevent hidden terminals, thanks to the aggregation mechanism.

This intrinsically solves the three possible cases of unintentional slot re-use by multiple nodes in the same radio range:

- Two nodes *A* and *B* are not in each other's radio range but are in the same *C*'s radio range (*hidden terminal* scenario).

- Two nodes *A* and *B* are not in each other's radio range originally but, due to mobility, they get closer enough to interfere.

- Two nodes *A* and *B* simultaneously start to transmit and select the same slot. The probability of this event is in direct ratio to the number of nodes and in inverse proportion to the number of free slots (hence critical with congestion).

All these cases cannot be managed only by channel sensing. In fact a third node *C* either receives from one of the two (or more) nodes unintentionally using the same slot, or, what is more likely, by neither one (due to disruptive interferences). Hence the *collision* cannot be detected simply by channel sensing.

Depending on the probability of occurrence of hidden terminals (as discussed in TR 102 861 [i.43]), unintentional slot re-use may become so relevant to affect the reception rate, certainly in urban scenarios. All in all, the ideal reception rate can be achieved only with two-hop coordination of slot re-use.

MS-Aloha has been designed and demonstrated to prevent all these cases. In fact, given the case of two nodes *A* and *B* unintentionally using the same slot:

- If all the other nodes can receive only by one (say *A*), then *B* will discover the collision by the *FI* received.

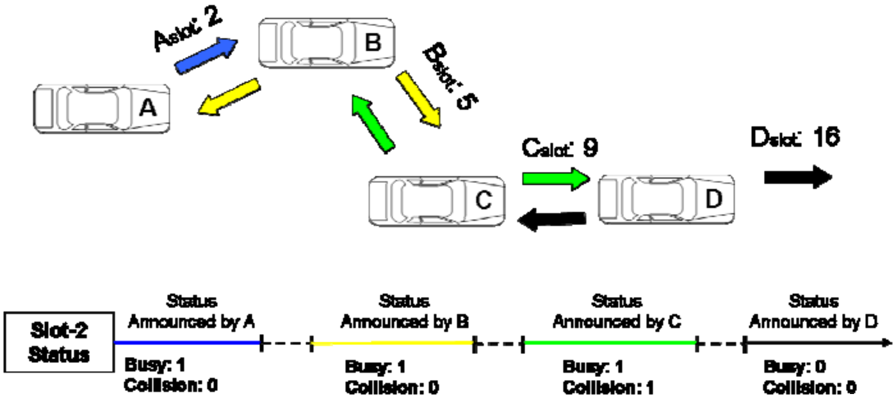
- If some nodes (say *LA*) receive from *A* and other ones (say *MB*) from *B*, the multiple *FI*s exchanged between *LA* and *MB* nodes permits to discover (and announce) the conflict.

The mechanism has been widely validated by simulations and also in urban scenarios [i.35], [i.36], where the event can create dynamic situations which can be particularly harmful (sudden appearance of nodes and fast changing topologies).

7.3.3.2 Slot reuse at four-hop distance

In MS-Aloha, each slot can be associated to more nodes, according to a minimum-interference rule: this intrinsically embodies the idea of spatial multiplexing. MS-Aloha permits slot reuse (and prevents slot exhaustion) by limiting the area where a slot is announced engaged. The main idea is that the *FI* information will be propagated through a limited number of hops. Without such feature, even with the period refresh mentioned before, some information on slot allocations can still be excessively forwarded over multiple hops. For example, in case of a daisy-chain topology where consecutive nodes have reserved consecutive slots, the information can be forwarded hop-by-hop several times, before the end of the frame, forcing the persistence of "old" information. In this way a slot will be announced busy too far from where it is actually used, hindering its re-use and potentially causing nodes' blocking.

Conversely, the implemented solution keeps a slot engaged only two-hop-far from the node using it.



NOTE: Node *A* transmits; node *B* directly receives from *A*, node *C* indirectly knows about *A* (it announces two-hop state, or '11'); node *D* indirectly knows about *A*: it does not use *A*'s slot but announces it 'free' (00).

Figure 18: The mechanism of two-hop announcement of slot allotment

To keep trace of the number of hops, MS-Aloha defines an additional state (inside *FI)*. Hence possible states will be free, busy, collision and 2-hop. In practice when a new FI is received and the state 2-hop is recognized, it means that the third hop has been reached. The receiving node is then required to consider the slot engaged but to propagate the information of "free" slot. To avoid runaway propagation, also the number of hops covered by the information on collision is upper-bounded. So, when a node notifies a collision which it cannot detect directly, it does not forward the information but considers that slot engaged: the node is supposed to be two-hop far from the colliding node.

This mechanism is called 2-hop Spatial Multiplexing [i.32] and is demonstrated in the example of figure 18.

7.3.3.3 Mechanisms for forced slot re-use

MS-Aloha was further extended to force slot re-use [i.34] acting on the area where a slot is announced busy. This feature is aimed at providing MS-Aloha with a tool to force slot re-use with a higher rate. For this purpose, a logical threshold (*Thr*) at MAC layer is added: only messages received with a power higher than *Thr* are considered for the MAC analysis on *FI*. On the contrary, packets with lower power may be received by upper layer (depending on SNR as usual), but do not contribute to the *FI* of the node (as if they were not received).

In this way, the minimum distance where a slot is kept busy is decreased, causing also a reduction in the minimum and maximum possible distance where the same slot can be reused. So, it is possible to control and monitor the width of the area where a feedback is taken into account. Because of the highly mobile channel with strong fading in VANETs, no fixed relation between the distance and the power threshold *Thr* can be given. Nevertheless, this relation can be described in terms of time-variant channel statistics. Hence the statement on minimum and maximum distances can hold.

This mechanism modifies the 2-Hop Spatial Multiplexing (2SM) into 2-Hop Spatial Multiplexing with Thresholds (2SMt), falling in the domain of cross-layer PHY-MAC mechanisms: now, MAC decisions are based on physical layer parameters. Moreover, it is important to highlight that 2-SMt does not act on transmitting power, but only on the receiving side.

The cross-layer thresholds are likely to increase interferences (MAC collisions) among nodes using the same slots. In fact, this feature brings a lower PDR (Packet Delivery Ratio) at the higher distance, depending on the transmitted power, but performances in the neighbourhood of the transmission (the main zone of interest) do not change.

Results about this algorithm are discussed in [i.34] and [i.37].

7.3.3.4 Dynamic mechanisms for the forced slot re-use

The mechanism of 2-SMt counteracts protocol blockage by slot exhaustion: if the threshold *Thr* is increased, the minimum distance for slot re-use lowers. However the proposed solution has some open issues like *(i)* how high *Thr* should be and *(ii)* when/how it should it be activated.

In order to cover this gap, the MS-Aloha's algorithm of 2-SMt has been added a dynamical behaviour, leading to a new definition called dynamical 2-SMt (2-SMtd) [i.37].

Here, the dynamical threshold is managed in a distributed way and each node separately, independently of the others, sets its *Thr*, based just on its own perception of the channel. This is possible only by an uninterrupted sharing of channel allocation between nodes. In fact, since each node keeps trace of the congestion state of the channel by the number of free slots (information within the *FI* structure), this number is used by the algorithm to drive the variations of the *Thr*, moving it up and down in fixed steps (for example 3 dB).

More in detail, each node updates three internal variables: *(i)* the current level of the threshold *Thr*; *(ii)* the time T2-SM elapsed from the last variation of *Thr*, and *(iii)* the percentage of free slots *F%*. Whenever the number *F%* is lower than F_1 (*near-exhaustion condition*) or higher than F_2 (*unloaded condition*) the threshold is respectively increased or decreased of Δ= 3 dB. More details on the proposed algorithm can be found in [i.37].

After testing the 2-SMtd in a large number of scenarios, involving very different network conditions, it has been confirmed to be stable and able to ensure a remarkable reactivity.

7.3.3.5 Pre-emption

In slotted protocols, slot exhaustion leads to protocol blocking, with harmful consequences for VANET safety applications. Traditional CSMA/CA approaches avoid this phenomenon with priority mechanisms (e.g. EDCA for 802.11p). Instead, in slotted connection-oriented approaches there are two possible, complementary, solutions to this problem:

- An improved resource re-use (see clauses 7.3.3.3 and 7.3.3.4). Despite fundamental, slot re-use alone cannot be sufficient. In fact, as demonstrated in [i.37], if slot re-use goes to extremes, it can have detrimental effects on the reception performance, even at short distances. In fact a too massive slot reuse causes stronger interference from closer nodes using the same slot.

- Introduction of mechanisms to manage prioritize among reserved flows.

While priority algorithms are well known and have been standardized for CSMA/CA-based protocols (e.g. IEEE 802.11e), in literature few solutions are available for slotted and connection-oriented MAC protocols. MS-Aloha has been the first slotted MAC for VANET with native support of priority (pre-emption) transmissions.

In order to enable pre-emption decisions, each node has to know the priority of existing connections. For this purpose each *FIj* subfield contains not only the indication of the slot state and of the node using it (if it is engaged) but also a priority indication in the Priority State Field (PSF) - figure 16 (e). Being 2-bit long, PSF admits 4 possible states, in decreasing order of priority: [00, 01, 10, 11].

The algorithm works as follows. When a node *A* needs to transmit high priority data, it analyses the channel for a whole frame period in order to know the channel allocation and chooses an available free slot. If all the slots are engaged, *A* scans the *FI*s looking for slots with lower priority. Then, *A* selects one of these slots (say *J*) and causes a collision on it, keeping the slot for the following frame. By the on-going acknowledgements between vehicles, the node *B* previously transmitting in *J* is notified that a high priority flows has pre-empted the slot, then *B* leaves the resource and waits for a new free slot. In this way, the high priority message is able to always gain the access to the channel. Summing up, this approach guarantees priority for critical transmissions also in congested scenarios.

The PSF classes can be used in different way, a possible solution could be:

- PSF = [00] - Emergency. This is for emergency vehicles only. Even if all the slots are engaged, an emergency channel can be set-up by emergency vehicles rejecting any other lower-priority connections.

- PSF = [01] - Safety. This is for ordinary safety communications by vehicles. Each node may be supposed to have a safety connection set-up while active. Each node can occupy only one slot with safety priority.

- PSF = [10] - Auxiliary and PSF = [11] - Entertainment. The last two configurations are meant to enforce statistical multiplexing. Connection-oriented approach may cause some stiffness in resource re-use. However this does not happen if any low-priority connections (auxiliary and/or entertainment) can dynamically reserve free slots and, reversely, higher priority connections can force them to leave. Each node can be assigned more than one slot only in the entertainment class of priority.

Notably, pre-emption does not require either modifications to the existing protocol or additional communication overheads (e.g. handshake).

7.3.4 Parameters

So far, several functions and mechanisms have been introduced for MS-Aloha. Each of them has been accompanied by the introduction of parameters.

In principle MS-Aloha can guarantee a nice scalability, completely preventing blocking. In fact, simulations, set in realistic urban scenarios (both obstructed and unobstructed Manhattan grids and involving fading), have shown [i.37] that MS-Aloha can work also with large number of nodes (up to 900 in less than 1 km^2). However the protocol's performances can be optimal or sub-optimal, depending on the protocol settings.

It is then important to be aware of the possible settable parameters. They are here shortly recalled:

1) Transfer rate, Slot length and *Tg* duration.

2) *STI* and *FI* length (also as consequence of the number of slots *N*).

3) Decision on the transmission of the *FI* only in some periods. In fact, the *FI* could be alternatively sent or not by a node on a period base (clause 7.3.2.2).

The parameters listed in items 1 to 3 are mutually linked and require a joint setting. Obviously they should be set so to best suit the median frame length and packet transmission rate. This introduces also the application rate.

1) Application rates and pre-emption configuration depending on the carried services.

2) Configuration of 2-SMtd (including both the thresholds involved by the algorithm and their increments). This includes the definition of parameters such as: *FI%*, F_1, F_2 and the algorithm for the variation of *Thr*. Notably, the variation can be set in a diversified way, so to penalize differently the information coming from different hops (e.g FI_J related to a first or a second hop).

All these aspects are analysed in more detail in TR 102 861 [i.43], based on results coming from simulations.

7.3.5 Summary

The mechanisms provided by the MS-Aloha solution have already been discussed in clauses 7.3.1 to 7.3.4. In the present clause the available features will be wrapped-up, emphasizing MS-Aloha's main differences and consequent advantages, in the arena of slotted MACs for VANETs. In fact, while MS-Aloha has all the advantages typical of synchronous MACs (as mentioned in clause 6 and 7.1) it has also several benefits coming from its being specifically designed for VANETs. Basically MS-Aloha is designed to manage scalability, mobility patterns, and propagation typical of VANETs. The following list highlights such features by points.

- *Hidden terminal*. MS-Aloha completely prevents hidden terminals and unintentional slot re-use (which could affect SINR and reception rate, hence reception *determinism*). All the three cases described in clause 7.3.2 are successfully solved by MS-Aloha. For the sake of completeness, the same approach is used also by another slotted MAC for VANETs (DTDMA, see clause 7.4), but without solutions for slot re-use. Techniques based on time-outs, instead, just limit the duration of unintentional slot re-uses but increases the number of slot reservations event over time.

- *Reactivity*. Given the continuous frame-by-frame reservations (or confirmation of the reservations) and check on the acknowledgments by MS-Aloha, any possible problem in the protocol state (*e.g.* collisions, sudden appearance of nodes, effect of topology changes due to mobility) can be resolved within one-period. Conversely, solutions based on time-outs require multiple periods. MS-Aloha's solution is simple and straightforward to be implemented in hardware: it requires only to apply logical operators to the FI received (AND on the Busy fields and EXOR on the respective STIs).

- *Scalability and slot re-use*. If a slot could be used only once throughout the network, then the channel access would be blocked as soon as the number of nodes exceeds the number of slots. Conversely, by introducing the idea of reusing slots, the concept of spatial multiplexing is subtended as well. In fact, given a connection-oriented approach, each slot can be associated to more nodes and the nodes simultaneously using the same slot need to satisfy a minimum-interference rule which intrinsically embodies the idea of spatial multiplexing. Several approaches can be adopted to decide on slot re-use: in MS-Aloha slot re-use is based on received power (by the features called 2SM, 2SMt, 2SMtd and respectively described in clauses 7.3.3.3, 7.3.4.1 and 7.3.4.2). The power-based approach has three main benefits with respect to position-based ones: *(i)* it is more robust, because it works when the position cannot be computed from GNSS signal; *(ii)* it does not imply additional traffic to be exchanged among vehicles and, supposing that such traffic is sent in any case and is negligible, it works regardless such notifications about position are received or not; *(iii)* it permits to make decisions based on the information spanning three hops. Last but not least, *(iv)* in a urban scenario, as demonstrated in [i.41], two nodes (say *A* and *B*) may be close but *A* could receive from *B* a power lower than from a third node *C* which is farther but in line-of-sight. This means that slot re-use based on position may not be effective. Conversely a re-use policy based on received power is fairer and simpler.

- *Scalability and pre-emption*. A slotted MAC which is able to force slot re-use can guarantee scalability and prevent protocol blocking. However slot re-use alone cannot be sufficient. In fact, as demonstrated in [i.37], if slot re-use goes to extremes, it can have detrimental effects on the reception performance, event at short distances. In fact a too massive slot reuse causes stronger interference from closer nodes using the same slot. Thus, only with pre-emption, additional flows can be housed. In fact *(i)* pre-emption further increases scalability and exploits all the available bandwidth; *(ii)* despite this, the feature does not worsen the performance of emergency communications. MS-Aloha is the only slotted protocol for VANETs managing also pre-emption.

- *Decentralised Mitigation Techniques*. The mechanisms of 2-SM, 2-SMt and 2-SMtd involve an interference mitigation technique. In fact, the interference is mitigated by slot re-use which is *(i)* based on the received power (*i.e.* on the level of interference) at more than two hops and is *(ii)* progressive, in that it does not penalize a specific slot but causes a smooth (*progressive*) increase in interference at all the slots; additionally *(iii)* the mechanism is decentralised and apply only where/when it is required.

- *Acknowledgement*. In MS-Aloha, by the analysis of *FI*, a station *A* using slot *J* can infer which nodes have received its packet in the previous frames: *A* has simply to check what nodes are announcing *A* in position *J* of their *FI*s. In other words MS-Aloha has, for free, ACKs available for any transmissions (regardless of their being broadcast or unicast). Additionally, being the ACKs sent in piggyback, they do not waste transmission resources. This feature may lead strong benefits to VANETs services, as discussed, for instance in [i.48].

- *Limited overhead*. The overhead involved by MS-Aloha is *(i)* limited, fixed and often negligible in terms of medium efficiency (see clause 7.3.3.2). By converse, the information carried in the overhead *(ii)* permits to coordinate transmissions (and multiplex over space) at two-hop (not one-hop!) distance, leading to all the benefits mentioned in this list - including a minimum interference and an almost ideal reception rate (otherwise not achievable). *(iii)* The aspect of numerical overhead (computed only on frames) is somehow simplistic for VANETs involving large number of nodes and broadcast transmissions. In fact, if the coordination is not effective enough, it results in poor receptions and unintentional slot re-use, which constitute an even deeper waste of resources. In other words: if the numerical overhead is low but fewer nodes receive packets, the gain is not worth; this means also that, in VANETs, the time efficiency cannot be evaluated on a per-node base and cannot be kept separate from space-efficiency. As discussed in [i.34] more significant metrics for the evaluation of VANETs' overheads should be the reception rate and is the ratio between the inter-packet- time of consecutive received packets and the time required for the transmission of the payload. In these metric MS-Aloha is unequalled. *(iv)* Finally, it may be worth mentioning that, as mentioned in RR-Aloha and ADHOC MAC [i.51], two predecessors of MS-Aloha, the MAC can work (with some worsening in the reactivity) also if *FI*s are not sent in all the frames (for instance on alternate periods or even less, considering the three-hop coordination).

- *Backward compatibility* and *coexistence with CSMA/CA*. *(i)* MS-Aloha is backward compatible with IEEE 802.11p [i.2] at PHY-PLCP layer: it may use the same formats and physical modulations. *(ii)* In addition, given the feature of pre-emption, MS-Aloha can enforce coexistence with CSMA/CA in a way transparent to CSMA/CA stations. The mechanism will be better explained in clause 9.1, however its rationale is to leverage pre-emption to prevent CSMA/CA from breaking MS-Aloha's reservations without blocking high-priority flows on MS-Aloha. More in details if an MS-Aloha station intends to transmit in slot *J* and slot *J-1* is free, it can reserve slot *J-1* with low-priority; in this way, transmission in slot *J* cannot be disturbed by in-progress transmissions by CSMA/CA, while MS-Aloha stations can easily reserve *J* with a higher priority. This mechanism is still being studied and may represent a key feature for seamless migration from a pure CSMA/CA VANETs to a hybrid CSMA/CA-MS-Aloha one. *(iii)* Nonetheless, also in a pure MS-Aloha network, the feature allows nodes to step back to CSMA/CA, in case of missing synchronization (clause 8.4), and to coexist in the same network. This may be a last resort solution, which is unlikely to happen but important to have.

- *Determinism.* In MS-Aloha nodes are always guaranteed channel access by slot reservation. This makes channel access deterministic (non-blocking) and fair. Moreover delay is fixed and reception is almost ideal, at least in the proximity of the transmitter, where the reception is more critical for safety.

7.4 Other time slotted approaches

This clause will shortly outline other time slotted MAC approaches that has been proposed for VANETs.

Many time slotted MAC approaches proposed for VANETs are based on slotted Aloha (S-Aloha) [i.54]. The S-Aloha is an enhancement of the Aloha protocol presented in 1973 [i.55], which simply sends whenever there is something to send and if no ACK is received, a retransmission is made after a random backoff. In S-Aloha [i.54], the available time is divided into slots constituting a frame. A node randomly chooses a slot to transmit in whenever it has something to send. The throughput efficiency of S-Aloha is considerable higher than pure Aloha, but synchronization between nodes is needed to avoid overlapping transmissions. To further improve the throughput of S-Aloha, the reservation S-Aloha (R-Aloha) protocol was proposed in 1981 [i.56]. In R-Aloha nodes listen to the channel to determine which slots are occupied. When a node wants to send, it chooses a slot that was perceived as free in the previous frame. The node then keeps the same slot as long as it has something to send. Due to this the R-Aloha scheme does not take node mobility into account. Aloha [i.55], S-Aloha [i.54] and R-Aloha [i.56], are all examples of protocols where every data packet needs to be acknowledged by the intended receiver. This implies that they cannot easily be adapted to a broadcast scenario as there is no other means to avoid or determine if concurrent transmissions have occurred.

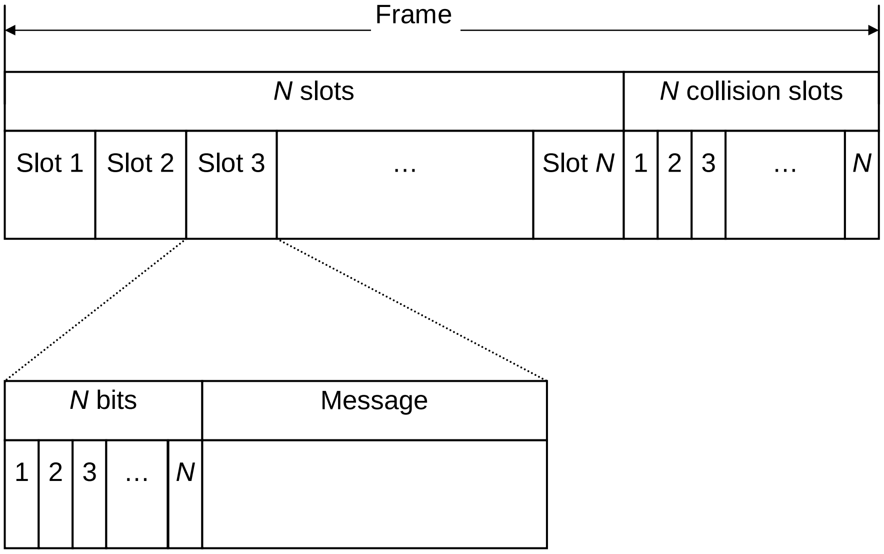


Figure 19: The slot allocation scheme in CSAP

In 1988 the first MAC protocol specifically addressing broadcast in VANETs was proposed, namely the concurrent slot assignment protocol (CSAP) [i.57]. In CSAP the frame is divided into two sub-frames; one part containing the slots for actual data transmission whereas the other part is used for signaling if collisions are experienced by receivers, i.e. the collision slot, figure19. When a receiver recognizes a collision in a specific slot in the ordinary data frame part, it will transmit a high frequency signal in the corresponding collision slot to notify the concurrent transmitters. Together with the data, each transmitter also send side information consisting of a simple slot allocation scheme, where free and occupied slots as experienced by this particular transmitter are marked with zeros and ones, respectively, figure 19. When a node realizes that it has accessed a specific slot concurrently with another node, it changes to a new one. The work on CSAP was extended in 1991 by Zhu *et al.* [i.58] through the MAC scheme termed decentral channel access protocol (DCAP), which supports higher node mobility than CSAP. The procedure of changing slots when collisions occur is enhanced in DCAP by including another protocol called integrated service management protocol. The extra bits containing the collision information found in the end of the CSAP frame are removed and instead a handover request based on lost connections to formerly adjacent nodes (which still should been in radio range of each other according to their movement pattern) is issued. However, since the collision detection mechanism in both CSAP and in DCAP relies on a third party (there is a probability that two nodes have chosen the same slot, while no other nodes are within range of these two concurrently transmitting nodes - and thus no one can communicate the collision information), every transmission is performed only with a certain probability, *p*, and deferred with 1- *p* in order to minimize concurrent transmissions.

The reliable R-Aloha (RR-Aloha) proposed by Borgonovo *et al.* [i.59] in 2002 is almost identical to the DCAP proposal. In RR-Aloha the node sends side information in each slot containing the slot allocation chart as perceived by this particular node. Further, the ADHOC-MAC [i.60] is based on RR-Aloha with some additional features such as bandwidth allocation for point-to-point communication together with multicast support. In RR-Aloha and ADHOC-MAC the frame length is fixed. In adaptive ADHOC (A-ADHOC) [i.61] the authors extend previous work and propose to use a variable frame length to reduce the setup time and use the channel resources more efficiently. This implies that with few nodes there is a short frame length and fewer slots, i.e. more frames per second, and when the number of nodes increases, the frame length will be extended to accommodate more nodes. In RR-Aloha one bit is used in the slot allocation chart to denote whether a slot is free or occupied. However, the only time a slot is regarded as occupied is when a node has successfully received a packet in that particular slot. Hence, a slot is said to be free if there has been a collision, i.e. a negative ACK is interpreted as free by concurrent transmitting nodes when they receive the slot allocation charts from other nodes. In RR-Aloha+ [i.62] the RR-Aloha proposal was enhanced by introducing one more bit in the slot allocation chart transmitted by every node. This new bit is used for signaling the occurrence of a collision, i.e. nodes sending at the same time causing collisions somewhere in the network. During the performance evaluation of RR-Aloha+ it was discovered that the information about the slot allocation was propagating too far, such that it blocked transmissions that could have taken place, i.e. the exposed node problem. Therefore, the RR-Aloha+ protocol does not use slot charts that are more than one frame old, in order to maintain updated information. In addition, in RR-Aloha+ there are problems with scalability when there are more nodes than slots in the system.

Although slots are cleverly coordinated with slot allocation charts in all the extensions of RR-Aloha described above, the number of nodes in the network is limited to the number of slots in the frame. When a node wants to join a network in which all slots are occupied, it has to wait until a slot is released, either because a node disappears (moves away) or stops transmitting. Since no guarantees can be made about channel access delays when many nodes want to access the channel concurrently the channel access delay is not upper-bounded and therefore unsuitable for road traffic safety applications as described in clause 4.2. The protocols are therefore not scalable in terms of the number of supported nodes. Also in the decentralized TDMA (D-TDMA) approach suggested in [i.38] and [i.39], nodes send side information containing the slot allocation chart. However, even if this scheme is denoted TDMA, it is almost identical to the DCAP and ADHOC-MAC proposals, and, hence, it is not possible to have more nodes than available slots. Improvements in terms of increased payload in D-TDMA were made in [i.40], but the randomness for a large number of nodes, larger than the number of slots, remains.

Günter *et al.* [i.63] propose a clustering scheme where a cluster head is elected and within each cluster a TDMA scheme is applied. One part of the TDMA frame within each cluster is never allocated by the cluster members. Instead these slots are used by newly arriving nodes to announce their presence and to request transmission opportunities. When two clusters come within radio range of each other, the clusters are regrouped. This scheme is based on a single frequency channel and to decrease the interference between clusters, a superframe between the clusters is proposed. Nine ordinary cluster frames are grouped into a single superframe and only one ninth of the available time is allocated to a cluster. This scheme is not predictable due to randomness involved when electing a cluster head. However, once a cluster head has been selected access is granted according to TDMA, which is predictable, but since there is a chance that newly arrived nodes fail to announce their presence the channel access delay cannot be upper-bounded.

In space division multiple access (SDMA), the communication channel is accessed based on the current location of the vehicle [i.64], [i.65], [i.66] and [i.67]. Location estimation is provided either through GNSS or a magnetic positioning system [i.64]. However, the position information is also propagated in the network, and thus all vehicles broadcast their position information. Dead reckoning is also suggested as a counter measure for GPS errors [i.67]. The idea with SDMA is to divide all roads into different sectors and within each sector another MAC method, e.g. TDMA can be applied. In [i.67] each sector is five meters and has a one-to-one mapping to a specific TDMA time slot. However, in an SDMA scenario there could be many unused slots due to sparse vehicle traffic or high relative speeds. The proposal from [i.67] is then to increase the channel utilization by allowing vehicles to use time slots from other sectors, i.e. all time slots up to the sector containing the next vehicle in front.

8 Time synchronization

8.1 Introduction

The issue of time synchronization can be split into two arguments: what the sources of synchronization should be and what precisions the chosen synchronization method could guarantee. Both the topics are covered in the following clauses.

Moreover, a synchronous solution is also liable to miss synchronization, while nodes should still be able to communicate: hence, a fallback solution should be provided to face also such events. They constitute the last topic covered in this clause.

The AIS system described in clause 7.2.1.1 relies on GPS synchronization but ships do not suffer from losing the GPS signal in urban canyons. The fallback solution in the absence of GPS signal is to synchronize to other ships having direct GPS signal. For more information on the GPS synchronization in the AIS system see clause 3.1.1 in [i.9].

8.2 Motivation for GNSS synchronization

The first, main distinction, which is made, concerns what kind of synchronization: *absolute* (derived b y a common absolute source) or *non-absolute* (e.g. local).

Some syllogisms can highlight how synchronization cannot be distributed by a VANET, hence provided by an external, common source. First it is worth reminding that synchronous VANETSs do not only need *frequency*-synchronization, but also *time/phase*-synchronization. In fact, since all the stations have to transmit on the same shared medium, all the stations have to share exactly the same time in order to coordinate transmissions.

Additionally the synchronization has to be *tight* as in pure Sonet/SDH fixed networks where the prerequisite of the multiplexing hierarchy is a synchronization spanning over the entire network and so precise to limit the occurrence of positive or negative justifications. In SDH/Sonet the justification is the mechanism to adjust the number of bits multiplexed from different links onto a same link in order to compensate for limited clock precision and/or clock drifts.

In tight synchronization, the problem can be split into: the definition of required synchronization precision - which is covered by the state of the art and, in particular, by ITU-T Recommendations [i.12]; the construction of a tree topology aimed at making frequency and phase distribution controlled. In ITU-T Recommendations G.811, 812, and 813, different clock precisions are defined, including clock hold-on capabilities over time and over multiple hops. The recommendations cover also the specifications of regeneration required at each hop of the clock distribution tree.

Concerning the latter point, the problem of distributing synchronization across multiple hops is a complex task which ITU-T Recommendation G.81x [i.12] standard solves by opening the rings in the network topology and building a tree whose root is the master clock; the clock is then distributed (and recovered) hop-by-hop by network links, with intermediate regeneration steps. Also back-up clock trees are foreseen. The approach of G.81x is robust, well-known and has been long-tested, however it may be hardly adapt to VANETs, where high terminal mobility makes the problem tougher.

The reasons are manifold. First of all, it is not possible to build a stable clock tree under strong mobility: if the synchronization of node *A* depends on signal received by node *B* and they move, the tree fails. On the other hand, the prompt construction of a new clock-tree would involve the knowledge of the exact position of all the nodes and also the propagation phenomena among them (to account also for urban obstructions potentially affecting the topology of the tree). Altogether these lead to the conclusion that a stable clock tree is not compatible with slotted MAC for VANETs.

Moreover, in absence of a clock tree, only puzzling information can be collected in the phase domain. The reason is depicted in figure 20 and has been already discussed in [i.23]: suppose that node *A* hooks up a clock phase (the time) and that it is distributed hop-by-hop to nodes *B*, *C*, *D* and back to *A*. Considering propagation delays, at each hop the time is delayed by Δ. So when the phase comes back to *A* it is 4Δ -late. If each hop is 100 m-wide, 3 hops can cause a delay - hence a phase uncertainty - of about 1 μs. With larger spans the uncertainty further worsens.

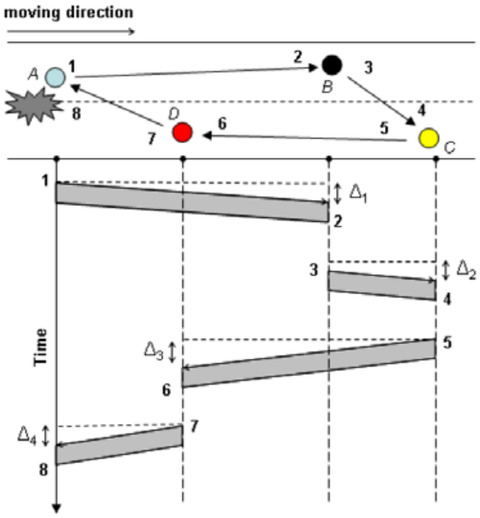


Figure 20: Uncertain clock delays and clock loops in a vehicular topology

It may be objected that in literature some solutions are available to synchronize nodes without using an absolute time reference. The most known ones are Timing-Synch Protocol (TPSN) [i.13] (which is an evolution of the Network Time Protocol (NTP) [i.14]) or Flooding Time Synchronization Protocol (FTSP) [i.15](using broadcast communications and MAC layer time-stamping). Other solutions, as Reference Broadcast Synchronization (RBS) [i.16], solve synchronization *locally*, dividing the network into interconnected single-hop clusters. None of them is however suitable for slotted VANET MACs, because they either require clock-trees or have a limited scalability (due to the required clustering).

Actually it is worth mentioning also some fully distributed synchronization solutions, not requiring an underlying clock-tree: among them the Average TimeSync Protocol (ATS) [i.17] which exploits a consensus algorithm to achieve a time reference agreement by averaging local time information.

ATS compensates clock skew and offset at each node to synchronize them with a virtual time reference that depends on the local clock skews and offsets. This represents a solution of *leaderless* synchronization in multi-hop wireless access networks. However ATS does not suite slotted VANETs either, for the following reasons: *(i)* it is proven only under the hypothesis of negligible propagation time, hence leads to a synchronization precision which is lower than the neglected propagation delay; *(ii)* it does not account for hidden terminals and sudden appearance of a new node.

All in all currently absolute synchronization constitutes the only solution suitable for synchronous VANETs: hence it is here supposed to be provided by Global Navigation Satellite Systems (GNSS).

8.3 From the accuracy of GNSS synchronization to the required Guard-Times

The accuracy of the synchronization is a parameter which is carefully evaluated in order to define an adequate Guard-Time (*Tg*) between consecutive slots. *Tg* will also counteract propagation delays, which will be evaluated as well in this clause.

The reason for a Guard-Time is then twofold: *(i)* even if all the stations in a slotted VANET were perfectly and absolutely synchronized, they would require a Guard-Time to compensate propagation delays; at light-speed *c* a delay Δ = 1 μs corresponds to about 300 m; then a Δ in [3, 4] μs should be sufficient for the intended range of 1 km, under the hypothesis of ideal synchronization.

Conversely, *(ii)* the initial hypothesis of ideal synchronization should be carefully evaluated. In fact, only under stationary condition the precision of the synchronization is high: assuming the position known, all the information received from GNSS satellites can be exploited to compute time. With a known position, the receiver does not have to calculate a positional fix to update the clock (1PPS) phase. In turn a rapid and accurate control of the phase error is facilitated and the difference between the real GPS time and the equipment tick is less than 25 ns. Even under strong mobility (as 1 440 km/h), time receivers like ITS GPS receiver module in mode 3-5 [i.18] and Frequency Generator Datum ET6000 [i.19] are stated to reach a precision *P* of 100 ns and 250 ns respectively. Altogether the Universal Time Coordinate (UTC) can be received by two stations with a mutual difference which is less than twice *P*, hence certainly $P < 1$ µs, even with a less precise GNSS receiver.

(iii) The third possible cause of lack of precision is probably the most critical and is clock hold-on in case of absence of GNSS signal: there are many possible failure modes that have been well documented elsewhere [i.25], but the most likely cause of failure is probably RF interference and jamming. This topic is tricklish and can be started by a best-case analysis.

The case of GPS synchronization includes the topic of Global Positioning System Disciplined Oscillator (GPSDO) [i.21], [i.22], [i.23] and [i.24], whose function is to receive signals from the GNSS satellites, and to use the information contained in these signals to control the frequency of a local quartz or rubidium oscillator. In GPSDOs the GPS signals are used to lock an oscillator adjusting both phase and frequency and, as a result, a GPSDO will outperform a standalone oscillator of the same type, even in free-run (after the a GNSS failure). A simple GPSDO can be built by using a phase detector to measure the difference between the 1 PPS signal from the GNSS receiver and the signal from the VCO. The VCO is typically a 10 MHz oscillator, so its signal is divided to a lower frequency (often all the way down to 1 PPS) prior to this phase comparison.

In fact, when the GPS signal is unavailable, a GPSDO continues to oscillate but in a stable frequency since the local oscillator is steered with a controller retaining the knowledge of its past performance. There is no exact answer as to how long GPSDOs can continue to meet the requirements in free-run; however an experiment can be mentioned for sake of exemplification. A holdover experiment was conducted at the NIST laboratories in Boulder, Colorado in October 2006 [i.26]: antennas from four GPSDOs were removed after a continuous running for weeks or months (when the GPSDOs could be supposed to be well locked).

The frequency accuracy and the offset of each device, after one week of holdover, are shown in table 5. Interestingly the quartz-GPSDO *D* with steering algorithm outperforms a rubidium-GPSDO *C* without it.

Table 5: Holdover performance of four GPSDOs as from the experiments mentioned in [i.16]

GPSDO Device	Type	Frequency Accuracy after 1 week hold-on	Time Offset after 1 week hold-on
A	Rubidium	80×10^{-12}	42 µs
B	Rubidium	3×10^{-12}	< 3 µs
C	Rubidium	1×10^{-12}	637 µs
D	Quartz	300×10^{-12}	82 µs

If 80 µs in one week is the offset for precisely locked GPSDOs, the question is about how much it may drop when the receiver is moving and has not been locked for months. This introduces the *(iv)* worst-case analysis which refers to the free-run of oscillators without any steering by GNSS. In this case [i.20] the solutions span from stabilized crystal oscillator (OCXO), temperature-controlled crystal oscillator (TXCO) and high performance OCXO (HPOCXO).
A TXCO is an oscillator that uses a quartz crystal to establish its frequency and is designed with temperature compensation features that minimize frequency drift over varied temperature ranges. Even avoiding the very expensive HPOCXO, an accuracy spanning in ±0,1 ppm - ±2,5 ppm can be achieved.

If $Tg = 50$ µs and 5 µs are supposed to counteract the previously mentioned time of flight and GPS accuracy under mobility, a residual time of (50 - 5) / 2 µs = 22,5 µs can be left for hold-on compensation between two opposite time-displacements (this the reason for the division by 2). With an accuracy of ±0,1 ppm this corresponds to about 4 minutes hold-on. Under the hypothesis of locked GPSDO, the hold-on time lasts periods which are magnitude longer.

Additionally *(v)* some recent solutions have been proposed to improve GNSS synchronization [i.27], [i.28] and to make it more stable by merging non-GNSS information [i.29] and [i.30]. Such methods, under another perspective, make GNSS reception more reliable and the needs for hold-on less frequent.

Altogether it seems that a sustainable (hence accurate) synchronization (and Guard-Time) can be fulfilled, with an only main issue: the costs required for a mass-deployment of the synchronization solution.

8.4 Fallback solution in absence of GNSS

Two classes of fallback solutions may be useful for synchronous MAC: *(i)* solutions aimed at holding-on synchronization in case of missing GNSS signal; *(ii)* solutions aimed at facilitating the automatic switching to CSMA/CA when synchronization is not available anymore.

The former class falls in the area of enhanced GNSS and will not be discussed here: part of the available techniques have already been mentioned in the previous clauses.

Concerning the second class, the include MAC mechanisms and are aimed to optimize protocol interworking and will be mentioned in clause 9.

9 Migration and coexistence in road traffic scenarios

9.1 Introduction

The first generation of VANETs supporting road traffic safety applications will use IEEE 802.11p with CSMA as MAC method. As described in clause 4.5, CSMA will encounter problems as the number of ITS equipped vehicles increases. It will have scalability problems with performance degradation as a result in terms of decreased reliability and excessive delays. There are two ways to handle this issue with the scalability either through DCC methods or exchange the MAC layer. The former has been developed within [i.7] and the current proposal is to only utilize the control channel to 25 % to facilitate DENMs in a dangerous road traffic situation when using CSMA. By changing to a time slotted MAC layer the utilization could be 100 % and above in overloaded situations. However, it should be noted that the time slotted MAC approaches could also benefit from the DCC methods developed in [i.7] with slightly different parameter setting than suggested for CSMA.

The life of a vehicle could be as high as 20 years. This is a too long period for introducing cooperative ITS, a critical mass of vehicles much be reached earlier than 20 years after the first market introduction. To speed up the number of ITS equipped vehicles there will probably be some kind of "after installation" on older vehicles. The long lifetime of a vehicle makes the migration path towards a new technology cumbersome. However, if the market introduction will not succeed with current chosen technology due to flaws there will probably not be cooperative ITS equipped vehicles in foreseeable future. During current standardization work there should be possibilities to upgrade road traffic safety applications. The closer to the hardware the more difficult it becomes to change technology except that it is possible to update software such as end user applications. The applications influence important parameters such as packet size. By only having this single option the change to a time slotted MAC layer would become easier.

9.2 Backward compatibility

Backward compatibility with IEEE 802.11p [i.2] can be discussed in terms of *(i)* protocol formats and *(ii)* MAC algorithms:

1) Concerning the first aspect, both STDMA and MS-Aloha have a strong backward compatibility to CSMA/CA in terms of formats. In fact, in both the cases, the same PHY and PLCP of IEEE 802.11p [i.2] can be used. This is expected to simplify the migration path from asynchronous to synchronous MACs and to benefits from the existing HW radio frontend blocks, inside the IEEE 802.11p [i.2] ASIC implementation. Additionally this feature makes possible the coexistence of different MACs, working in the same PHY and implemented in the same circuitry.

2) A different problem, instead, is that of the operational backward compatibility, defined as the possibility, for a synchronous node, to step back to a CSMA/CA mode. As discussed in clause 8, despite unlikely, this can be useful as a last resort, when synchronization cannot be recovered (for instance due to a HW problem on the synchronization block of the node). In this case a node should be able to detect its state (for instance by checking the synchronization of the received frames) and to switch to CSMA/CA MAC. Then the problem is moved into the area of coexistence, which is discussed in clause 9.4.

9.3 Coexistence with CSMA

The issue of coexistence between synchronous (STDMA/MS-Aloha) and asynchronous (CSMA/CA) MACs is quantitatively discussed in TR 102 861 [i.43]. Here the possible solutions are only introduced from a conceptual point of view. At the current stage the following cases have been envisioned.

- *Forced Coexistence*. This is a trivial coexistence: some stations run the synchronous protocol, other one CSMA/CA. They do not add mechanisms: hence synchronous solutions are just . Asynchronous transmissions are threats for reservations by the slotted protocols. The study will analyse if and at what extent (percentage of node following either MAC) this mode may work.

- *Time-Based Coexistence*. According to this approach, a time-based periodic structure (of period *t*) can be defined so that in a first period *a* stations can follow , for instance asynchronous MAC; in a second period *b* stations have to transmit following synchronous rules. Obviously *a* + *b* = t. Depending on the penetration of synchronous stations, the *a/b* ratio could be changed. This idea is far from being new and could be easily accepted by community. In fact, *(i)* a similar approach has already been standardized by IEEE 802.11 [i.4] for HCCA Coordination Function. Additionally *(ii)* time switching in VANETs, also for the asynchronous MAC IEEE 802.11p [i.2], has already been accepted for CCH/SCH switching in the USA std IEEE 1609.4 [i.42].

- *Transparent Coexistence*. This coexistence, currently, applies only to synchronous MAC with pre-emption. The rationale of transparent coexistence is to adopt some mechanisms so that slotted, connection-oriented, protocols can reserve their protocol in such a way that: *(i)* CSMA/CA can work without any changes to its algorithms - just by plain sensing; *(ii)* CSMA/CA transmission cannot break slot reservations; *(iii)* the scalability of synchronous protocol is not affected.

  In practice the method is completely managed by MS-Aloha stations by pre-emption and exploiting the maximum frame length (say *B* in bytes, *TB* in time domain and *SB* in terms of equivalent number of slots).

  For example, if a station *X* has to transmit in slot *J*, then it has to check the *SB* slots preceding *J*. If they are not all engaged, then *X* reserves with low-priority connections (and fake traffic) the free ones. As a result, the other MS-Aloha stations are only weakly affected, thanks to pre-emption mechanism, while CSMA/CA is expected to be managed (against disruptive transmissions): thanks to carrier sensing it will not transmit traffic potentially affecting MS-Aloha reservations.

  The viability of the transparent coexistence will be discussed in TR 102 861 [i.43].

10 Executive summary

Road traffic safety applications have requirements on *delay*, *reliability*, and *fairness*. The ability of the MAC method used in a VANET to meet these requirements is affected by how many nodes that currently is within radio range of each other. In VANETs the number of participating nodes cannot be restricted. Therefore, the one feature of the *ad hoc* topology that affects performance most is the scalability of the MAC method. Further, the MAC method has to be decentralized and allow nodes to self-organize, which is an inherent requirement from the *ad hoc* topology. The maximum delay should be upper bounded implying that the maximum time from channel access request to actual channel access is known beforehand, i.e. the MAC method is predictable. The reliability should be as high as possible given the current status of the wireless channel, especially for the closest neighbours to a transmitter. Finally, when considering the same data traffic class, all nodes in a VANET should have equal probability of channel access during each period of time, regardless of the number of nodes, i.e. the MAC method has to be fair.

CSMA as MAC method allows any number of nodes in the system - but it does not allow any number of transmissions. When the number of transmissions increases in a CSMA system, some nodes experience long or even excessive channel access delay, reliability is affected due to unintended, simultaneous, unsynchronized transmissions and certain nodes experience unfairness in the channel access procedure during certain periods of time. The majority of road traffic safety applications employ broadcast transmission, which may reduce reliability in general since acknowledgements are out of question. In addition, due to the broadcast mode, the backoff procedure of CSMA will only be invoked once and the exponential growth of the contention window, which aims at spreading simultaneous transmission attempts, is not possible. Therefore, CSMA has to be controlled e.g. through DCC strategies together with TPC to avoid collapsing during heavy utilization periods. The approach of restricting the data traffic may, in the long run, deteriorate performance of road traffic safety applications.

As a potential remedy to these problems, two time slotted MAC approaches have been presented in the present document - STDMA and MS-Aloha. Although these algorithms have slightly different approaches for e.g. slot selection and slot re-use, they can fulfil the requirements set up by road traffic safety applications. STDMA and MS-Aloha can cope with overloaded situations since they coordinate transmissions in time and space thereby supporting a higher channel load while maintaining a higher packet reception probability for the closest receivers compared to CSMA. They have a predictable channel access delay and are inherently fair since no nodes are prohibited to transmit during certain heavily loaded time periods, regardless of the number of nodes in the system. Table 6 summarizes the different requirements and to what extent these are fulfilled for each of the three MAC methods.

Table 6: An overview of the road traffic safety applications' requirements and the MAC methods ability to fulfil those

	Light network load			**Heavy network load**		
	STDMA	**MS-Aloha**	**CSMA**	**STDMA**	**MS-Aloha**	**CSMA**
Delay	Predictable	Predictable	Random	Predictable	Predictable	Random
Reliability	High	High	High	High	High	Low
Probability of fairness	High	High	High	High	High	Low

The disadvantage of time slotted MAC approaches as compared to CSMA is that they need synchronization, which preferably is done via a GNSS such as GPS. The GNSS signal might be obstructed for long time periods in for example urban canyons. However, by using a precise oscillator, for instance a GPSDO locked in phase and frequency, a sufficient capability of running without external synchronization is expected. Hence, nodes could still stay synchronized enough and hold-on also in absence of GNSS signal. Further, nodes that do not have access to a direct GNSS signal can synchronize to stations having GPS reception. In the worst case a time slotted MAC approach can fallback to become a CSMA system.

In summary self-organizing time slotted MAC approaches specifically aimed for *ad hoc* networking have all the prerequisites to perform better than CSMA due to the scheduled transmissions which are coordinated not only in time but also in space, thanks to slot assignment and slot reuse mechanisms. In TR 102 861 [i.43] quantitative results are provided to further substantiate these qualitative statements.

Annex A: Bibliography

H. Hartenstein and K. Labertaux: "VANET: Vehicular Applications and Inter-Networking Technologies", Wiley 2010.

R.Scopigno and H.A. Cozzetti, "GNSS synchronization in VANETs", in Proc. of the 3rd IEEE Int. Conf. on New Technologies, Mobility and Security, Kairo, Egypt, Dec. 2009.

H.A. Cozzetti, R. Scopigno and L. Lo Presti, "Tight coupling benefits of GNSS with VANETs", in IEEE Aerospace and Electronic Systems Magazine, vol. 26, issue 4, 2011.

History

Document history		
V1.1.1	December 2011	Publication