



Properties of the MAC Layer in Safety Vehicular Ad-Hoc Networks

Razvan Stanica, Emmanuel Chaput, André-Luc Beylot

► To cite this version:

Razvan Stanica, Emmanuel Chaput, André-Luc Beylot. Properties of the MAC Layer in Safety Vehicular Ad-Hoc Networks. IEEE Communications Magazine, 2012, 50 (5), pp.192-200. 10.1109/MCOM.2012.6194402 . hal-03884458

HAL Id: hal-03884458

<https://hal.science/hal-03884458>

Submitted on 5 Dec 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Properties of the MAC Layer in Safety Vehicular Ad Hoc Networks

Razvan Stanica, Emmanuel Chaput and André-Luc Beylot
IRIT-ENSEEIH, University of Toulouse, France

ABSTRACT

With intervehicle communications becoming a more and more popular research topic recently, the medium access control layer of the vehicular network has also received a considerable amount of attention. However, this increased interest has not always translated into a careful analysis of the properties exhibited by the MAC protocol when used by vehicular safety applications. This article tries to fill this gap by providing a comprehensive discussion on a number of important characteristics of the link layer in vehicular communications.

INTRODUCTION

Direct vehicle-to-vehicle (V2V) communication is considered to be an important step toward a highly secure and efficient intelligent transportation system (ITS). With spectrum already reserved in the 5.9 GHz band in both the United States and Europe, and a large list of possible applications already described [1], one of the last issues before the actual emergence of a vehicular ad hoc network (VANET) appears to be the design of an adequate medium access control (MAC) protocol.

Several standardization organizations, among which IEEE and the European Telecommunications Standards Institute (ETSI), have created dedicated working groups to address this MAC layer problem. The massive commercial success and availability of products based on the IEEE 802.11 standard made this protocol the obvious candidate for channel access control in vehicular networks. In July 2010, the IEEE 802.11p Task Group published an amendment to the original standard, specifically designed to be integrated in the Wireless Access in Vehicular Environments (WAVE) architecture. ETSI also decided to include IEEE 802.11p in its ETSI ITS architecture, while still considering the use of other solutions based on time-division multiple access (TDMA).

Despite the work of the normalization bodies, the problem is that the VANET MAC layer has to deal with unique requirements and condi-

tions. The design of a protocol that can support high relative speeds, a communication range of up to 1 km, mobility, driver privacy, and variable node density while being used by applications that could have an impact on human lives is clearly not an obvious task. And if things were not complicated enough, several misconceptions regarding the vehicular MAC protocol flourished inside the VANET research community.

It all started with the acronym, VANET, very similar with the one used for mobile ad hoc networks (MANETs). This quickly led to the description of the vehicular network as “a special case of MANET,” although it soon became clear that none of the solutions previously designed in a classical MANET context could be directly applied to intervehicle communication.

This article tries to explain why some of the assumptions made regarding vehicular networks in general and the VANET MAC layer in particular are wrong. We begin with a general presentation of the medium access control layer in V2V communication and we discuss its integration in the different architectures proposed in the ITS context. This is followed by a large, but by no means exhaustive list of properties exhibited by the VANET control channel. Special attention is devoted to the two types of safety messages and to the consequences of their broadcast nature. Different metrics needed to study the performance of the MAC layer from a safety perspective are also an important topic of this section. Finally, we focus on the scalability problem of IEEE 802.11p and discuss a series of problems related to MAC layer congestion control in vehicle-to-vehicle communication.

MEDIUM ACCESS CONTROL IN VANET

The spectrum available for vehicular communication has been divided into multiple 10MHz wide channels for more robustness. In Fig. 1, we can notice that seven such channels have been allocated in the United States, while only five exist in Europe because of free spectrum scarcity. From these channels, one is known as the

control channel (CCH; Fig. 1), while the rest are called service channels (SCHs).

The particularity of the CCH is that it can be used only by applications aiming to increase road safety. On the other hand, the service channels can transport messages issued by both safety and non-safety applications (focused for example on traffic efficiency or passenger entertainment). This differentiation in channel role created an important problem, because safety and non-safety applications have different, sometimes antagonistic, requirements. Therefore the proposed MAC layer mechanisms are often optimised for one type of application, while ignoring their effect on the other one.

Although the MAC layer is divided into multiple channels, the IEEE 802.11p standard is designed to function on a single 10MHz channel. For this reason, the WAVE architecture, presented in Fig. 2, contains a second standard, IEEE 1609.4 that describes the functioning of the upper part of the MAC layer, including channel switching and per-packet channel routing.

Based on a standardisation work initiated by the Car2Car Consortium, the ETSI ITS architecture is more general, including a large number of station-internal and external interfaces. However, as it can be noticed in Fig. 3, IEEE 802.11p remains the best choice for direct inter-vehicle communication. Unlike the IEEE WAVE, the ETSI architecture does not include any MAC layer solution to manage the multiple channels and the intention seems to be to delegate this problem to the upper facilities layer, described in the following section.

A few observations need to be made regarding the term *control channel*. In its decision from October 1999, the U.S. Federal Communications Commission (FCC) defined channel 178 (Fig. 1) as a control channel, while the six others were named service channels (SCHs). From these SCHs, the FCC assigned channel 172 “exclusively for vehicle-to-vehicle safety communications for accident avoidance and mitigation, and safety of life and property applications,” and channel 184 “exclusively for high-power, longer-distance communications to be used for public safety applications involving safety of life and property, including road intersection collision mitigation.” Under these conditions, the role of the CCH was limited to announcements periodically transmitted by roadside units (RSUs) in order to advertise the applications supported on the other channels.

Meanwhile, the European regulators also decided to create a control channel and several SCHs. Nevertheless, in the ETSI architecture, the CCH has been reserved for safety V2V applications, meaning that, in the US and European allocations respectively, the same name applies to channels with different functions. Moreover, the European CCH corresponds to the WAVE channel 180, a normal service channel, which could raise some important interoperability problems. For simplicity reasons, further on in this article, the European meaning and appellation of the CCH will be used, but the totality of the observations made here can be applied to the WAVE channel 172.

U.S. spectrum allocation						
CH172	CH174	CH176	CH178	CH180	CH182	CH184
5.860	5.870	5.880	5.890	5.900	5.910	5.920
G5SC4	G5SC3	G5SC1	G5SC2	G5CC		
European spectrum allocation						

Figure 1. Spectrum allocation in USA and Europe.

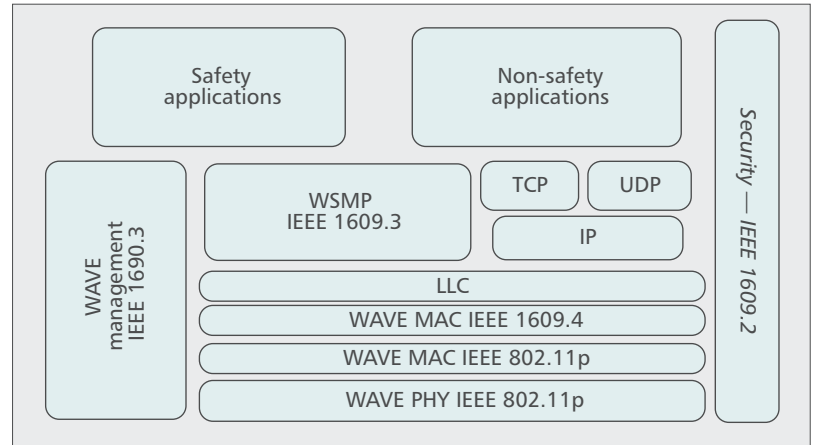


Figure 2. IEEE WAVE architecture.

THE VANET CONTROL CHANNEL

The fact that the control channel is dedicated to safety applications creates entirely new challenges for the MAC layer, challenges that do not exist either in classical MANETs or in IEEE 802.11-based WLANs. This section discusses in detail some of the most important of these characteristics. However, this list is by no means exhaustive and, for example, issues related to security or privacy are not addressed in this article.

THE ROLE OF THE FACILITIES LAYER

Before discussing VANET MAC layer properties, a short presentation of the role played by the facilities layer is needed. As described in the ETSI ITS architecture, the facilities layer covers the three upper layers of the OSI model and provides support for the different applications. The facilities layer will also be integrated in the WAVE architecture, being currently standardised in the United States by the Society of Automotive Engineers (SAE).

Non-safety applications are mostly IP-based and, therefore, they continue using the classical TCP/IP protocol stack. Nevertheless, safety applications do not use the TCP/IP architecture (see the WAVE architecture in Fig. 2). Some of the reasons for this choice come from the fact that the overhead introduced by IPv6 would be prohibitive for the short safety messages, while IPv4 would not be able to cover the geographical addressing demands of safety applications.

Moreover, while the number of proposed safety VANET applications is impressive, the information needed by all these applications is

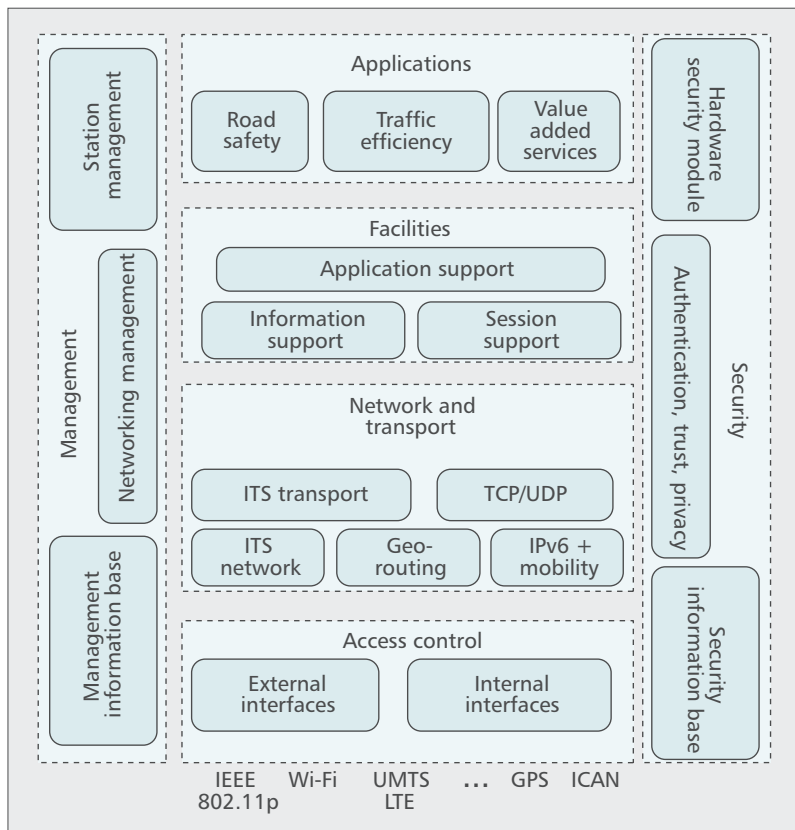


Figure 3. ETSI ITS architecture.

similar (location and speed information from the neighbouring vehicles). If each application was to acquire this information for itself, as in a classical architecture, the channel would be congested by messages containing the same information but issued by different applications.

This problem was solved elegantly in the case of V2V communication, by the introduction of an extra-layer between the applications and the transport protocol, called the *facilities* layer and shown in Fig. 3. All the information gathered from the other vehicles and from the on-board sensors is stored here and it is made accessible to all the applications, without the need of application-to-application communication.

THE BROADCAST NATURE OF THE CONTROL CHANNEL

The assumption that safety applications use unicast messages at the MAC layer is usually made when trying to directly apply for V2V communications solutions initially designed in the context of classical MANET, sensor networks or wireless mesh networks. This type of study usually considers that safety messages are only transmitted in dangerous situations, with a precise destination (equivalent to the *sink* node), and without considering any congestion problem.

However, vehicular safety applications take a proactive approach, with periodically sent beacons, also called cooperative awareness messages (CAMs) in the ETSI ITS architecture. These beacons are transmitted with the purpose of sharing information gathered by the on-board sensors (e.g., geographical location, speed, accel-

eration etc.) with the neighbouring vehicles. The role of the CAMs is therefore not to announce a danger, but to extend the driver's knowledge about the surrounding environment, with the hope that this extra-information will help enhancing road safety.

Of course, unexpected hazards can still occur and the vehicle detecting such an event should announce it to the other traffic participants. Sometimes the information does not need to be disseminated with very strict temporal requirements and it can simply be added to the next beacon. It is, for example, the case of a modification in weather conditions or in the type of road surface. Nevertheless, in other cases, the duration until the next CAM is produced is too large and the situation must be reported outside this periodic framework. Therefore, a second type of safety message has been defined for these circumstances, the Decentralized Environmental Notification (DEN).

Both CAMs and DENs contain information that is potentially interesting for all the surrounding vehicles. Even in the case of applications like pre-crash warning, where only a small number of network nodes are actually involved, the event has an influence on all the vehicles situated in the close neighbourhood. This implies that safety messages need to be transmitted using MAC layer broadcast, and the filtering and aggregation happen at the facilities layer. For example, a hard braking vehicle transmits a DEN intended for all the vehicles situated behind it, but the destination MAC uses a broadcast address and the geographical region of interest is only discovered at the higher layers. Moreover, because the control channel is entirely dedicated to safety applications, this means that the CCH is a purely broadcast channel.

The broadcast nature of the control channel has been acknowledged by the standardisation bodies, and the ETSI Technical Specification (TS) 102 637-1, focused on the functional requirements of the ITS describe the exchange of a CAM message as a 10-steps operation (Fig. 4). Steps 3 and 4 point out that this new driving assistance paradigm based on V2V communication should use broadcast messages at the MAC layer. The same TS describes the application flow for DENs, very similar to the one shown in Fig. 4, with the amendment that a supplementary filtering operation takes place at the facilities layer based on the geographical data included in the message. While broadcast in wireless networks can be achieved very simply due to the omnidirectional propagation of radio waves, this suggests that MAC layer solutions designed with unicast communication in mind are hardly transposable in the vehicular network, especially in the case of the CCH.

For example, the distributed coordination function (DCF) described in the IEEE 802.11 protocol treats differently broadcast and unicast messages. The most notable distinction comes from the fact that broadcast messages are not acknowledged because of the high collision probability between the multiple receivers. Contrarily to what happens in wired networks, wireless nodes cannot detect collisions using solely the carrier sense mechanism, and they rely on

acknowledgment (ACK) messages for this purpose. With the ACKs being unusable in the case of broadcast communication, the vehicular MAC layer has no simple solution to detect an undelivered CAM or DEN.

Moreover, the request-to-send/clear-to-send (RTS/CTS) handshake included in the DCF in order to alleviate the hidden nodes problem is also inefficient in the case of multiple receivers and therefore is not used for broadcast communication. This raises new challenges regarding the hidden nodes problem in a vehicular network where the elaborated DCF is stripped to a basic carrier sense multiple access (CSMA).

A detailed analysis of the applicability of popular IEEE 802.11 enhancements to a safety VANET is given in [2], the conclusion being that none of the discussed mechanisms can be straightforwardly adapted to meet the requirements of vehicle-to-vehicle safety communications. Although some solutions originally designed with unicast messages in mind might also be efficient in this new context, such mechanisms and protocols need to be treated with precaution and they have to be revalidated by taking into account the vehicular communication pattern.

THE LIMITED LIFETIME OF SAFETY BEACONING

Another assumption inherited from MANET research associates beaconing with signalling. In multi-hop wireless networks, beacons (usually presented under the form of *hello* packets) have the role of control messages, their presence being dictated only by the requirements of the routing protocols on topology awareness. In such a case, this in-band signalling is considered to be an overhead, a wasted portion of bandwidth that needs to be minimised in order to allow the transmission of as much applicative data as possible.

On the contrary, vehicular safety applications exchange information by the means of beaconing. While CAMs also have the goal of providing a certain knowledge about the network topology, they can no longer be treated as control messages because of their larger scope. Reducing the beaconing volume in a vehicular network means reducing the amount of available information, hence the efficiency of safety applications.

It is true that for non-safety applications working outside the CCH the VANET beacons can still be perceived as control messages. However, even in this case, the beaconing does not introduce any kind of overhead because the CAMs are sent on a different channel, the equivalent of out-of-band signalling. Non-safety applications can therefore benefit from the advantages of beaconing without having to contend with this extra-traffic.

Designing vehicular beacon-less forwarding algorithms [3] or routing protocols [4] in these conditions can be an interesting exercise, but these solutions practically neglect the purpose of a vehicular network.

Even among the research studies that acknowledge the importance of the CAM messages, the assumption that beacons are no more than simple broadcast messages is usually made.

- 1) The facilities layer constructs the CAM by collecting the necessary data from relevant facilities.
- 2) The facilities layer issues a CAM to the network and transport layer, with the required transmission parameters.
- 3) The lower layers process the CAM and construct the packets for broadcasting.
- 4) The packets are broadcasted in the ITS ad hoc network.
- 5) At receiving ITS station, the lower layer processes the received packets and extract the CAM.
- 6) The CAM is delivered to the facilities layer.
- 7) The facilities layer process the CAM and dispatches the information to the relevant facilities.
- 8) The information in CAM is delivered to the application layer.
- 9) The application layer processes the received CAM information.
- 10) The application layer provides the necessary warning or information via HMI to the driver.

Figure 4. Details of the Cooperative Awareness application message flow.

Whether we talk about analytical frameworks [5] or simulation results [6], beaconing is perceived as a periodic broadcast, with no extra-properties.

However, as we explained, CAMs contain data from on-board sensors, like vehicle location and speed. If such a message cannot be transmitted before the next beacon is produced, the information it contains is no longer valid. Transmitting an outdated CAM in these circumstances would provide neighbouring nodes with unusable data while also introducing an unnecessary delay for the next message.

Therefore, such an *expired* beacon has to be dropped in order for the CAM containing the updated information to take advantage of the next transmission opportunity.

The fact that safety beacons can expire makes them very different from regular broadcast messages. For example, the optimal value of the minimum contention window from the IEEE 802.11 back-off mechanism decreases with the increase in node density in the case of vehicular beaconing, while showing the opposite effect for pure broadcast [7].

Although the difference between beaconing and broadcast might not be that radical in other cases, the studies focusing on the performance of different VANET safety mechanisms should take into account the special characteristics of the messages transmitted on the CCH instead of seeing them from a classical broadcast perspective.

METRICS

In the context of periodic broadcast, we can imagine an IP packet being passed to the MAC layer for transmission while previous messages are still in the MAC queue(s) waiting to be served. This introduces a MAC layer delay that depends on the number of messages already in the queue and the time needed to serve such a message. The MAC layer delay can be relatively large in some cases, and this could be quite problematic in the case of safety messages that

practically have real-time requirements. Therefore, many researchers turn their attention to this metric, trying to minimize the average time a beacon spends at the MAC layer.

However, as we already discussed above, vehicular beaconing is different from regular broadcast in certain aspects, the most important being that safety beacons have a limited time duration before being dropped. Because an expired CAM is not transmitted, the MAC delay is bounded by the beacon's lifetime, and therefore any received safety message contains correct information. In these conditions, measuring the average MAC delay becomes less significant.

Applicative throughput, sometimes called *goodput*, is another metric of interest in most types of networks. This is a direct consequence of a communication model based on the TCP/IP architecture that corresponds to almost every network in our *all-IP* world. Practically every application relying on classical transport and network layers needs as much throughput as possible. This is true for video streaming, file exchange, Internet access, or sensor-collected data transmission. It was therefore natural for researchers to focus on the same metric in the case of vehicular networks.

Nevertheless, in a vehicular network, beacons are generated by the facilities layer (more precisely by the CAM and DEN management entities) based on the requirements of the applications and measuring an applicative throughput in this case is not significant. If we add to this the fact that the safety data is never fragmented as it travels through the different layers and that retransmissions are not practical, we can conclude that a more appropriate metric in the case of a vehicular network is the reception probability of a beacon. Moreover, the data sent by a vehicle is more relevant to its close neighbours (vehicles situated at less than 50–100 m from the transmitter) than to those situated farther away in the coverage area and in this case it is more meaningful to calculate the beaconing reception probability as a function of the distance from the sender [9].

However, even the beaconing reception ratio gives little information about the safety improvement brought by vehicular communications. Other metrics have recently been described with vehicular safety communications in mind, like the time duration a vehicle remains invisible to another vehicle [9], or the distance travelled by a node between two consecutive beacon receptions from a one-hop neighbor [8]. These metrics are much more interesting in a vehicular context, as they include in one single value information concerning expired beacons, radio propagation problems, and message collision, giving an idea about the improvement in driver *awareness* brought by safety applications.

DECENTRALIZED ENVIRONMENTAL NOTIFICATIONS

Although special notifications are arguably more important for the performance of safety applications than CAMs, the study of DENs has received less attention than the one of ordinary beaconing. And, with some exceptions (e.g., [6]),

these few studies focused on the multihop dissemination of safety messages.

Message forwarding and information dissemination in a certain area have also been thoroughly investigated in the context of vehicular geocast, a communication paradigm used by certain non-safety applications where a message needs to be delivered to all the stations inside a given geographical area. DENs also have to address these spatial requirements, as the information they carry must be shared with all the vehicles that might be influenced by the event. The distance that needs to be covered depends on the application, and it can go from a few hundred meters in the case of emergency braking to several kilometers in the case of a blocked road announcement. Moreover, special notifications also add temporal constraints that do not usually exist in the case of non-safety applications.

It is therefore tempting to use similar solutions for DEN and geocast forwarding [15]. However, geocast messages are the only solution to deliver the necessary non-safety data needed by vehicles found outside the coverage range of the information owner. On the other hand, safety applications can always rely on regular beacons to deliver the required data. The vehicle that originally detects the event might consider it important enough to create a special notification instead of waiting until the next beacon is produced, but the one-hop neighbors that become aware of the event do not simply forward it using a dedicated mechanism. The information is in this case delivered to the facilities layer and it is made available to the interested applications. Because multiple vehicles are now in the possession of the news, farther dissemination can be achieved by all these stations announcing the event using regular beaconing, and there is no need to increase the network load with the forwarding of a DEN.

Another problem that can be detected in the studies related to DENs is the supposition that special notifications are created uniformly over the entire network. However, choosing randomly the source vehicles comes in contradiction with the idea that special notifications announce an event detected by the onboard sensors.

Sudden brakes, ice, blocked roads, vehicles driving on the wrong lane or other situations of this type appear in a certain geographical area and they are detected by vehicles in the respective zone. It is very probable that several nodes simultaneously detect the same event, therefore the origins of the DENs cannot be considered independent.

This is particularly important in the analysis of congestion control mechanisms, because multiple high-priority messages might try to access the medium at the same time. This property of the DENs leads to another argument against the idea of a blind multi-hop dissemination of special notifications, because the same information would be uselessly forwarded in messages initiated by different sources. Instead of this, the facilities layer needs to aggregate the information received from its neighbors, and to relay a unique and clear view of the event.

MAC LAYER CONGESTION CONTROL

While conceptually the vehicular network is ready to be deployed, some practical problems still need to be investigated, including some related to the MAC layer. Probably the most important issue in this context is congestion control, especially when considering the fact that the IEEE 802.11 protocol is well known for its scalability problems. The research community acknowledged the importance of congestion control in vehicular networks, and the ETSI ITS architecture includes mechanisms for transmission power control, data rate adaptation and beaconing frequency adjustment. This section points out some less explored properties of the control channel that could have an impact on the performance of these mechanisms.

THE EXPOSED NODE-FREE NATURE OF THE CCH

The attenuation of propagating radio waves is an important phenomenon allowing spatial reuse in wireless networks. On one hand, this increases the capacity of the network but on the other hand it can lead to the occurrence of *hidden nodes*, basically stations that cannot directly communicate but whose messages can collide in a certain area of the network.

This *hidden node* problem has been thoroughly studied in wireless networks and a number of solutions have been designed, the most popular probably being the RTS/CTS handshake. Sadly, these solutions cannot be used in a broadcast environment like the CCH. Moreover, reducing the number of hidden nodes usually triggers a side effect, the exposed node problem. An exposed station sees its transmission denied by the mechanism trying to eliminate hidden nodes (or even directly by the carrier sense mechanism), although sending the message would not produce a collision.

A number of research studies focused on finding the best trade-off between hidden and exposed nodes in MANETs or wireless mesh networks. This problem changes completely in a safety VANET, again because of the broadcast nature of the CCH. An exposed terminal appears when multiple flows can coexist on a certain area, and it depends on the geographical position of the communicating nodes. By definition, the exposed node is not interested in the other messages that occupy the channel and its transmission would not create a collision at a node involved in the communication. However, in the case of a safety message, a transmission interests all the surrounding stations, including those trying to access the channel. Therefore, the concept of exposed node does not exist in this vehicular context, and the proposed solutions should consider this particularity.

THE LACK OF INTERNAL CONTENTION ON THE CONTROL CHANNEL

From the two types of vehicular safety messages, DENs contain more valuable information than CAMs. When a special event needs to be communicated to the other traffic par-

ticipants, the hypothesis is that the rest of the network is not aware of the situation and the information needs to be rapidly disseminated over a certain geographical area. It is therefore essential to grant DENs a higher priority than the simple beacons transmitted by other vehicles. This can be achieved through the use of a higher transmission power [6] or a smaller back-off time [9] for the special notifications.

As a complement to these approaches, some research studies (e.g. [10]) turned their attention to the internal contention between the various types of safety messages. Inspired by the different traffic classes defined in the IEEE 802.11e standard, the proposed solutions suggest the use of multiple queues, each with distinct access parameters. This idea, successfully used in wireless local area networks (WLANs) to meet the requirements of voice and video traffic, imposed itself in the vehicular community and both the WAVE and ETSI ITS architectures include the enhanced distributed channel access (EDCA) function, originally designed for IEEE 802.11e.

However, at a close inspection, the assumption that forms the starting point of this internal contention problem seems to be questionable. As already discussed, safety messages are not produced directly by the applications, but by the facilities layer. Also, a safety message can only be a CAM or a DEN. We already established that the arrival of a new CAM triggers the expiration of the previous one, hence there can be no internal contention between two or more CAMs. Moreover, the information included in a beacon (location, speed etc.) is also present in a special event notification. In these conditions, if a DEN is produced while a CAM is waiting at the MAC layer, the CAM is no longer needed because the data it transports can be found in the DEN and therefore it can simply be dropped from the queue. On the other hand, if a beacon is produced while a special event notification is still being treated, the relevant information can simply be updated in the DEN as there is no need to waste the bandwidth by transmitting both messages. This implies that an internal contention between a CAM and a DEN is also not realistic.

The only possibility to have two safety messages at the same time at the MAC layer is when both of them are special event notifications. Because DENs should be transmitted using a small contention window, such a situation is very implausible. Nevertheless, even if such circumstances might occasionally appear, there is no reason to assign DENs to different traffic classes and the messages can simply use the same queue using a first-in-first-out approach.

In these conditions, the only advantage of a MAC architecture based on the IEEE 802.11e traffic class differentiation is that the safety messages can be quickly assigned a series of parameters (backoff time, transmission power, modulation) by simply being transmitted to the corresponding queue [9]. The EDCA might also be useful for channel access on the SCH, where traffic differentiation is necessary.

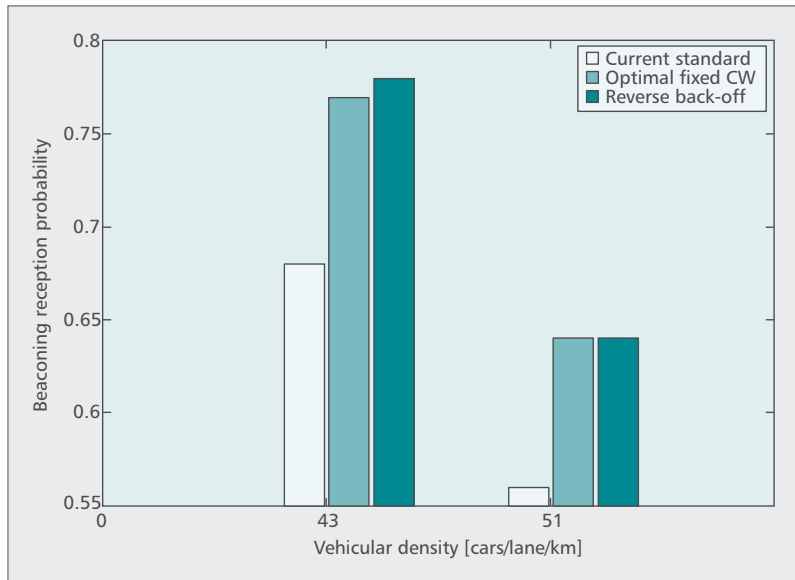


Figure 5. Beaconing reception ratio at less than 200 meters from the sender using different values for the contention window.

THE CENTRAL ROLE OF THE CONTENTION WINDOW

An essential part of the IEEE 802.11 protocol is the back-off mechanism, whose performance is highly influenced by the value of the contention window (CW). When a contending station detects the channel busy, it has to postpone its access to the medium for a number of idle slots uniformly chosen between 0 and CW.

In unicast communication CW is doubled after each failed transmission and reset to the initial value CW_{min} following a successful reception. This mechanism, known as the binary exponential backoff (BEB), is a powerful tool that allows the protocol to adapt to increased node density while also keeping the induced MAC layer delay under control. With the surge in multimedia applications, stronger delay requirements have been imposed on the link layer and the solution that has been chosen in IEEE 802.11e was to reduce the value of CW_{min} for traffic with strict delay demands like voice or video.

Vehicular safety applications also have very precise temporal requirements; therefore the temptation was to use the small contention window values from EDCA in the IEEE 802.11p amendment. However, this decision has been taken without any proper analysis in support, and several important issues can be detected with this approach.

First of all, broadcast is handled differently by the DCF. As a failed transmission cannot be detected, a message is sent only once, always using CW_{min} . This practically eliminates the only mechanism targeting the scalability problem, the BEB.

Second, the IEEE 802.11 standard was successful in a WLAN cellular environment, with an access point serving a limited number of stations. While a number of studies have demonstrated that the optimal value for CW_{min} depends on node density [12], the reduced num-

ber of contending nodes that existed in practice and the performance of the BEB mechanism have been considered sufficient in this case. However, the vehicular network is a totally different context from the original one-cell scenario. The ad hoc nature and a highly variable vehicular density can lead to situations where several hundred stations contend for channel access. In this case, a small contention window leads to a high number of collisions and to a reduced beaconing reception probability [7]. For example, Fig. 5 shows some results from the study described in [9], where an adaptive reverse back-off mechanism is proposed. The current version of the standard, with a CW value between 3 and 15 is clearly not optimal, even if only a fixed value for CW is considered, and a 10 percent improvement in beaconing reception ratio can be achieved by simply using a higher value for this parameter.

Finally, while it is true that both multimedia and vehicular safety applications have specific delay requirements, their situation is by no means identical. On one side, we have flows in need of high throughput and/or low jitter. On the other side, we have beacons transmitted periodically and we are simply interested in the reception ratio. A few milliseconds lost per transmission can result in an important throughput decrease and reduce the perceived quality of multimedia applications. On the other hand, the delay introduced for CAMs is already limited by the beaconing period. Therefore, there are no major consequences from a temporal point of view if the back-off mechanism uses a higher contention window in order to reduce the collision probability while also keeping the number of expired beacons under control [9].

PRACTICAL PROBLEMS OF DATA RATE ADAPTATION

One of the solutions proposed for MAC layer congestion control in the ETSI ITS framework is data rate control [13]. The idea behind this adaptive mechanism is that a higher data rate implies the message occupies the channel for a smaller amount of time, hence allowing more transmissions to take place.

An important compromise in this case is that the higher the data rate provided by a modulation, the higher the signal-to-interference ratio (SIR) required at the receiver in order to correctly decode the message. Simulation studies (e.g., [13]) considered this aftermath, but in a rather simplistic manner that only presumes a reduced coverage area. Using this assumption, the reception probability for geographically close vehicles is hardly affected and, in these conditions, adjusting the data rate gives similar results with transmission power control. Choosing the modulation depending on the local vehicular density appears therefore to be a very powerful tool in crowded environments.

Nevertheless, recent experimental studies present a much more disturbing image of the V2V communication channel [14]. These tests not only confirm that the vehicular channel is extremely noisy, but they also show that node density has an important impact on the degree

of interference. As more vehicles are present on the road, the number of signal reflections increases and decoding becomes more difficult. This translates in the extended presence of so-called *grey zones* around the transmitter, areas where the reception probability oscillates between 20 and 80 percent. The grey zones become larger when the local density increases or when a more demanding modulation is used. These results are very problematic for data rate control where the combination of high vehicular densities and high data rates is proposed. For example, the tests described in [14] show a beacon reception probability of 50 percent at 50 m from the sender when using a 16-QAM modulation. Moreover, this already alarming number is simply due to radio propagation errors and does not take into account the possible collisions that could appear. Therefore, while theoretically the choice between several modulations exists, field tests demonstrate that practically a data rate superior to 6 Mb/s is totally inefficient.

THE CHALLENGE OF DETECTING COLLISIONS

MAC protocols in general are designed with the idea of preventing message losses in mind. However, in some cases, such events are unavoidable and fall-back mechanisms are needed, like automatic repeat request (ARQ) or the adjustment of various MAC or PHY layer parameters. An essential property in wireless networks is that the transmitters cannot directly detect the loss and therefore they need to rely on feed-back from the receivers.

With IEEE 802.11 being among the most popular standards for wireless communications, the number of solutions focusing on alleviating the consequences of a transmission failure is impressive, but most of these proposals are based on detecting losses by the means of missing Acknowledgments. As discussed, ACKs are not used on the broadcast CCH, so timer-based mechanisms cannot be implemented.

Another important characteristic of the vehicular network is that the actions that need to be taken depend on the causes of the loss. If in WLANs a missing ACK results in a retransmission, regardless of whether the message was lost following a collision or because of bad channel conditions, in VANET the adaptive mechanisms focused on congestion control often take antagonistic approaches in the two situations. For example, a noisy channel demands an increase in transmission power, while a collision, on the contrary, can be the sign of congestion and a lower transmission power needs to be used in this case.

However, discriminating between a collision and a radio propagation problem is a complicated task, especially in a noisy environment. Some studies have shown that distinct patterns can be detected in these two cases in the evolution of the received signal strength indicator (RSSI), but this implies the offline use of powerful statistical tools and we are not currently aware of any real time solution able to detect a collision using this method.

Collisions are clearly undesired events and the vehicular MAC layer should include tech-

niques to alleviate this problem. However, these techniques must be designed beginning from the observation that collisions in a VANET are not only unwanted, but also unavoidable and undistinguishable from other types of losses (propagation errors, expired beacons).

CONCLUSION

The increased interest recently shown to ITS and vehicular communications resulted in a special attention toward VANET MAC layer issues. Sadly, this has not been doubled by a careful inspection of the properties required from the protocol controlling the channel access. While the choice of the IEEE 802.11 standard for inter-vehicle communications can be considered a practical one, the behaviour of this protocol on the purely broadcast vehicular control channel is yet to be completely understood, especially in the area of congestion control.

In this article, we give a detailed picture of the vehicular medium access control layer in the case of the VANET CCH. We present important properties of the broadcast safety messages (e.g. their limited lifetime) and the metrics relevant to this safety context. The congestion control problem on the control channel is another central point of this discussion. We hope that this article will help researchers understand the complex picture of safety V2V communications and will assist them in the design of new protocols and mechanisms for the future vehicular network.

REFERENCES

- [1] P. Papadimitratos et al., "Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation," *IEEE Commun. Mag.*, vol. 47, no. 11, pp. 84-95, Nov. 2009.
- [2] X. Chen, H. Refai, and X. Ma, "On the Enhancements to IEEE 802.11 MAC and Their Suitability for Safety-Critical Applications in VANET," *Wireless Commun. and Mobile Computing*, vol. 10, no. 9, Sept. 2010, pp. 1253-69.
- [3] D. Rossi, E. Fracchia, and M. Meo, "VANETs: Why use Beaconing at All?," *Proc. IEEE ICC '08*, Beijing, China, May 2008, pp. 2745-51.
- [4] P. Ruiz et al., "BRAVE: Beacon-less Routing Algorithm for Vehicular Environments," *Proc. IEEE InVeNET '10*, San Francisco, CA, Nov. 2010, pp. 709-14.
- [5] X. Ma, X. Chen, and H. Refai, "Unsaturated Performance of IEEE 802.11 Broadcast Service in Vehicle-to-Vehicle Networks," *Proc. IEEE VTC Fall '07*, Baltimore, MD, Oct. 2007, pp. 1957-61.
- [6] M. Torrent-Moreno et al., "Vehicle-to-Vehicle Communication: Fair Transmit Power Control for Safety-Critical Information," *IEEE Trans. Vehic. Tech.*, vol. 58, no. 7, Sept. 2009, pp. 3684-703.
- [7] R. Stanica, E. Chaput, and A.-L. Beylot, "Why VANET Beaconing is More than Simple Broadcast," *Proc. 74th IEEE VTC Fall '11*, San Francisco, CA, Sept. 2011, pp. 1-5.
- [8] Y. Tadokoro et al., "A New Approach for Evaluation of Vehicle Safety Communications with Decentralized TDMA-based MAC Protocol," *Proc. IEEE Wksp. V2VCOM '08*, Eindhoven, The Netherlands, June 2008, pp. 1-6.
- [9] R. Stanica, E. Chaput, and A.-L. Beylot, "Enhancements of IEEE 802.11p Protocol for Access Control on a VANET Control Channel," *Proc. IEEE ICC '11*, Kyoto, Japan, June 2011, pp. 1-5.
- [10] M. Barradi, A. Hafid, and J. Gallardo, "Establishing Strict Priorities in IEEE 802.11p WAVE Vehicular Networks," *Proc. IEEE GLOBECOM '10*, Miami, FL, Dec. 2010, pp. 1-6.
- [11] D. Rawat et al., "Dynamic Adaptation of Joint Transmission Power and Contention Window in VANET," *Proc. IEEE VTC Fall '09*, Anchorage, AK, Sept. 2009, pp. 1-5.

- [12] G. Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," *IEEE JSAC*, vol. 18, no. 3, Mar. 2000, pp. 535–47.
- [13] Y. Mertens, M. Wellens, and P. Mahonen, "Simulation-based Performance Evaluation of Enhanced Broadcast Schemes for IEEE 802.11-based Vehicular Networks," *Proc. IEEE VTC Spring '08*, Singapore, May 2008, pp. 3042–46.
- [14] F. Bai, D. Stancil, and H. Krishnan, "Toward Understanding Characteristics of Dedicated Short Range Communications (DSRC) from A Perspective of Vehicular Network Engineers," *Proc. ACM MOBICOM '10*, Chicago, IL, Sept. 2010, pp. 329–40.
- [15] J. Cho, S. Shin, and J. Copeland, "Fast Broadcast at the Intersection in VANET," *Proc. IEEE IVCS '11*, Las Vegas, NV, Jan. 2011, pp. 65–69.

BIOGRAPHIES

RAZVAN STANICA (Razvan.Stanica@enseeiht.fr) is a research scientist with the Network and Communications Engineering (IRT) team of the Toulouse Institute of Computer Science Research (IRIT). He obtained a Master's in engineering degree and a Ph.D. in computer science, both from the National Polytechnic Institute of Toulouse (INPT), France, in 2008 and 2011, respectively. He also obtained a Master's in engineering degree from the Polytechnic University of Bucharest, Romania, in 2008. His research interests include wireless mobile networks, with a special focus on vehicular communications and intelligent transportation systems.

EMMANUEL CHAPUT received an engineering degree in computer science from ENSEEIHT, Toulouse (France) in 1992 and a Ph.D. degree in computer networks from the Université Paul Sabatier, Toulouse in 1998. He is now assistant professor (maître de conférences) at the Telecommunication and Network Department INPT/ENSEEIHT and member of the IRT team (Network and Communication Engineering) CNRS/IRIT. His current research interests include IP over satellite networks architecture, but also vehicular communications. Within the scope of such application areas, he focuses on network architecture and resource allocation.

ANDRÉ-LUC BEYLOT received an Engineer degree from the Institut d'Informatique d'Entreprise, Evry, France, in 1989 and a Ph.D. degree in computer science from the University of Paris VI, France, in 1993. In January 2000, he received the Habilitation à Diriger des Recherches from the University of Versailles, France. From 1993 to 1995, he worked as a research engineer at the Institut National des Télécommunications, Evry, and from 1995 to 1996 at C.N.E.T. (France Telecom Research and Development), Rennes. From September 1996 to August 2000, he was an assistant professor at PriSM Laboratory, University of Versailles. Since September 2000, he has been a professor at the Telecommunication and Network Department, National Polytechnic Institute of Toulouse (INPT/ENSEEIHT). Since September 2009, he leads the IRT Team of the IRIT Laboratory. His research interests are with the performance evaluation of communication networks, especially with regard to mobile, satellite, and vehicular networks.