Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Lehrstuhl für Rechnernetze und Telematik

WS 2009-2010

Seminar Paper

MAC Protocols for VANETs
A Survey and Qualitative Analysis

Alexandru Dorin, Oprea

February 8, 2010

Advisor Prof. Dr. Christian Schindelhauer

Abstract

Vehicular Ad Hoc Networks (VANETs) are a special type of Mobile Ad Hoc Networks (MANETs). In VANETs power consumption and storage are not limited and the position of the nodes can be easily determined via GPS. But, because vehicles move very fast, the topology of the network changes rapidly and often. Thereby routing in inter-vehicular networks is a difficult task. Low latency and high reliability must be also taken into account because of active safety applications. This seminar paper is based on a article by Menouar, Filali and Lenardi [6], that presents and qualitatively compares some MANETs MAC protocols that can be used in VANETs.

Contents

1 Introduction

Mobile Ad Hoc Networks (MANETs) are a special type of ad hoc networks. As the term states, MANETs have mobile devices as nodes and are connected by wireless links. Like all ad hoc networks, MANETs are self-configuring and do not use a centralized administration. Because the network nodes are mobile it is clear that the network topology changes often over time and therefore finding routes is not such an easy task.

Vehicular Ad Hoc Networks (VANETs) are a specific instance of MANETs where the network nodes are represented by vehicles. Their main goal is to provide distributed real time communication between nearby vehicles and between vehicles and the road-side equipment. The topology of VANETs changes very fast because the nodes, represented by vehicles, move at high speeds. Despite this, the network nodes have restricted mobility: cars can move only on roads and highways. As stated by Luo and Hubaux [5], another advantage is that storage and power are not an issue, thus wider transmission ranges and longer lifetimes are possible.

VANETs have many practical applications and therefore the research in this area is evolving at an energetic pace. The most important benefits are in terms of active safety. By using inter-vehicular communications, cars can warn each other about dangerous traffic situations like an accident, an icy road, etc.

Because of the nature of wireless communications, the nodes of the network use the same radio frequencies as communication medium and therefore transmission collisions can occur. Different medium access control (MAC) protocols are known, that help avoid these problems. In their article [6], Menouar, Fethi and Lenardi do a qualitative analysis of existing MAC protocols for MANETs that can be used also for VANETs.

2 MAC protocols for MANETs

As stated before, the main problem that a MAC protocol for MANETs has to solve is to avoid transmission collisions. This is not such an easy task because the nodes are mobile and therefore it is harder to determine if the shared medium is free or not. There are also two other problems that the MAC protocols should avoid: the hidden terminal problem and the exposed terminal problem.

The hidden terminal problem occurs when two terminals (A and B) are not in range of each other and they both want to transmit data to a third terminal (C). Because they cannot see each other, terminal A and B are not aware of the others intention to send data to the terminal C. Therefore they both start sending data to terminal C and a transmission collision occurs (Figure 1).

The exposed terminal problem occurs when, trying to prevent a transmission collision, a terminal is not allowed to send data, even though it would not interfere with the ongoing transmission. In Figure 2 the terminal S1 wants to transmit data to the terminal R1, so it informs its neighbor S2 of that intention, an afterwards starts transmitting data to

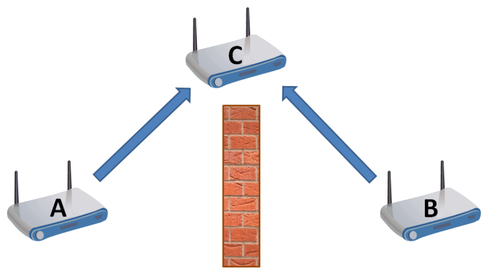

Figure 1: The hidden terminal problem.

R1. Terminal R2 is not in range of terminal S1, and also terminal R1 is not in range of terminal S2. Therefore, S2 could send data to R2 at the same time S1 sends data to R1, because no transmission collision would occur. But because S2 was informed by S1 to wait, the transmission from S2 to R2 is postponed. Thus, in order to avoid transmission collision, sometimes the wrong terminals are silenced.

Figure 2: The exposed terminal problem.

Menouar et al. [6] present a brief and chronological introduction to the MAC protocols used in MANETs. According to them, the first protocol proposed for wireless networks was ALOHA ("hello" in Hawaiian). The transmission collisions are solved in a very basic way: a node starts sending data and if a transmission collision occurs, it waits for a random period of time before retransmitting again. The throughput of the channel is severely affected by this method, being reduced at only 18.4 percent [6]. There is a enhanced version of this protocol, Slotted ALOHA (S-ALOHA), that uses time slots and doubles the maximum throughput of the system. Luo and Hubaux [5] suggest another extension called Reservation ALOHA (R-ALOHA) that has even a higher throughput than S-ALOHA, but has also potential risk of instability. All three protocols are collision recovery protocols, meaning that if a collision occurs it can be detected and the system can recover from it [1].

A step forward were the collision avoidance protocols [1] which are trying to minimize the probability of collisions, thereby attempting to avoid them. Carrier Sense Multiple Access (CSMA) protocol with the later addition of Collision Detection (CSMA/CD) is such a protocol. In this case, the nodes transmit only if they "sense" the common channel to be idle. When a collision occurs, the transmission is interrupted and another attempt is made later.

The first protocol to overcome the hidden terminal problem is Multiple Access with Collision Avoidance (MACA). This protocol uses request to send (RTS) and clear to send (CTS) packets to initiate a handshake between the sender and the receiver. Thereby the neighboring nodes are aware about an ongoing transmission and no collisions occur. To overcome the exposed terminal problem, an enhanced version of the protocol was proposed, called MACA Wireless (MACAW). This protocol initiates a second handshake by using data sending (DS) and acknowledgment (ACK) packets.

All MAC protocols presented above are so called packet based, meaning that in order for a message to be sent to a destination, it is first broken into several packages. These packages are sent separately and therefore they can each follow a different route. When they arrive at the destination, they are reassembled in the proper sequence [4]. On the other hand there are the circuit based MAC protocols, which require dedicated point-to-point connections. In this cased the message is being sent as a whole and it follows every time the same path to the destination [4]. Menouar et al. [6] present in their paper some circuit based MAC protocols that are used in MANETs. The basic idea of each protocol is the same: the medium is divided into several fixed frames, and each frame eventually into several slots. Every node that wants to send data reserves and uses a different slot. Therefore simultaneously transmissions are supported and collisions are avoided. These protocols are briefly presented in Table 1.

Category	Division Method	Example
Time Division Multiple Access (TDMA)	time	FPRP
Frequency Division Multiple Access (FDMA)	frequency	MCSMA
Code Division Multiple Access (CDMA)	code	MC MAC

Table 1: division multiple access protocols for MANETs

3 MAC Protocols for VANETs

The most important requirements for a MAC protocol for VANETs are low latency and high reliability. The bandwidth is not so important because, for active safety measures, only small messages must be sent. But these messages must be sent quickly and with very low failure rates.

VANETs have some advantages over MANETs, and a good protocol should take this into account. Vehicles have no power or storage limitations, can be easily equipped with a GPS and move only on roads. On the other hand, there is also one big disadvantage: topology changes quickly and often.

3.1 The IEEE 802.11 standard

The first protocol introduced by Menouar et al. [6] is the IEEE 802.11 standard. This standard adresses both the MAC and the physical layers of the OSI model. It can operate both in a centralized and in a decentralized mode, but only the latter is important for inter-vehicular communications. IEEE 802.11 was proposed because it is already widely accepted by the network community as a standard in wireless communications, and therefore compatible devices are more or less inexpensive.

In terms of the MAC layer, the IEEE 802.11 standard uses a CSMA protocol with Collision Avoidance (CSMA/CA). A device listens to the shared communication medium before transmitting in order to avoid collisions. There are two methods to determine if the communication channel is idle or not. The first, called physical carrier sensing, cannot overcome the hidden terminal problem and therefore is not further discussed. The second method, called virtual carrier sensing, uses a Network Allocation Vector (NAV) to determine the duration for which the communication channel will be busy. This is a very simple solution, the NAV being basically a timer which, if different than zero, indicates that the medium is occupied.

As stated by Menouar et al. [6] there are some interval spaces, called Inter-Frames Spacings (IFS), that are set between two successive transmission frames in order to manage the medium access process. These spacings are very important. For example, when a terminal senses the medium, to check if it is idle, it must do this for certain duration of time called Distributed IFS (DIFS). Later, after a data frame is received, the receiver waits for a Short IFF (SIFS) time before sending an acknowledgement. In order for the protocol to work properly, the DIFS intervals must be grater then the SIFS intervals.

Basically the IEEE 802.11 MAC protocol is a double handshake protocol (Fig. 3). After sensing the medium to be idle for a DIFS time, a vehicle sends a RTS packet that contains the duration of the whole transmission. All nodes receiving this packet set their NAV according to the transmission duration, thereby knowing how long the medium will be busy. The receiver vehicle, which also gets the RTS packet, waits for a SIFS time and then sends a CTS packet, containing again the duration of the transmission. Again, all nodes that get the CTS packet set their NAV accordingly, so they are aware of the ongoing transmission. When the sender vehicle receives the CTS, it waits also a SIFS time and then starts transmitting data. After successfully receiving the data frame, the receiver vehicle waits again for a SIFS time and then sends a ACK packet, but only to the sender. By using this method, the risk of transmission collisions is reduced and the hidden terminal problem is also solved.

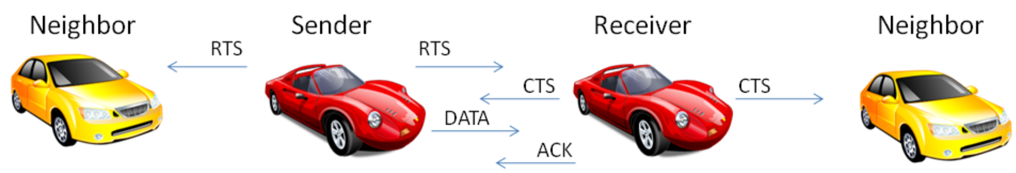

Figure 3: Packets controll exchange in IEEE 802.11.

In terms of the physical layer, the IEEE 802.11 standard offers several versions that can be applied in VANETs. The most famous ones are presented in Table 2. Menouar et al. [6] present an amendment of the 802.11 standard specially designed for VANETs: Wireless Access in Vehicular Environments (WAVE), which is referred as well as IEEE 802.11p. The main goal of this amendment is to adapt the IEEE 802.11 standard for inter-vehicular communications where reliability and low latency are extremely important. According to the official IEEE 802.11 Working Group project timelines [2], the 802.11p protocol is scheduled to be published in November 2010.

3.2 ADHOC MAC

Another MAC protocol that is proposed by Menouar et al. [6] to be used in VANETs is ADHOC MAC [3], a protocol developed by the European project CarTALK2000. Unlike the 802.11 standard, ADHOC MAC is based on a dynamic TDMA mechanism and uses

Name	Band (GHz)	Maximal throughput (Mbps)	
		in theory	in practice
802.11a	5	54	25
802.11b	2.4	11	7.5
802.11g	2.4	54	19
802.11n	2.4	600	150

Table 2: IEEE 802.11 Physical Layer for VANETs

the UMTS Terrestrial Radio Access Time Division Duplex (UTRA-TDD) as the physical layer.

ADHOC MAC uses an extension of the R-ALOHA protocol, called Reliable R-ALOHA (RR-ALOHA). Like all TDMA protocols, the medium is divided into several repeated time frames. Each frame is divided into N time slots. Each vehicle that wants to send data, has to reserve for itself one basic channel (BCH), which is one of these time slots, periodically repeated in successive frames.

To overcome the hidden terminal problem, the RR-ALOHA protocol transmits a frame information (FI) vector, which lets any terminal know the status of each slot [3]. This vector has N entries which specify the status of each of the preceding N slots, as sensed by the owner of the FI. Every vehicle transmits its FI every time frame on its BCH. For the rest of the time slots, the vehicle listens to the medium and it updates its own FI based on the FI received from its neighbors. When a new vehicle arrives the scenario is as follows: the new vehicle listens during a complete time frame before attempting to transmit on a selected slot, sending only its own FI on the selected free slot; if in the next time frame the selected slot is marked by its id in all the received FIs, than this slot becomes its BCH. This method ensures that, when a terminal gets a BCH, the slot is reserved for it in a two-hop neighborhood.

3.3 Directional Antenna-Based MAC Protocols

In ad-hoc wireless networks, the use of directional antennas instead of omni-directional antennas can offer many benefits. With directional antennas, the signal of the transmission is concentrated only on the intended receiver, thus leading to the increase of coverage range and spatial reuse. These two factors result in a greater channel capacity. Especially in VANETs, because the vehicles can move only on roads, the use of directional antennas can reduce interference and transmission collisions.

Menouar et. al [6] present only one protocol for directional antennas, called Directional MAC (D-MAC). This protocol requires that each terminal knows its position and also the positions of its neighbors. Therefore this protocol is not so easy to implement for MANETs. But this is not the case for VANETs, because nowadays almost every car has a GPS antenna.

With directional antennas the space around a terminal is usually divided in several angles. The D-MAC protocol is based on the IEEE 802.11 standard and uses a RTS/CTS/ACK handshake method. Every antenna that receives a RTS or a CTS, becomes blocked and does not interfere with the neighbors transmission. Thereby, the D-MAC protocol reduces transmission collisions and the hidden terminal problem, but does not solve the exposed terminal problem. As stated by Menouar et al. [6], even though directional antennas could dramatically improve the performance of VANETs, such systems still seem too complex and hard to manage in real implementations.

4 Qualitative comparision

Menouar et al. [6] have tried to do a qualitative comparison of the three protocols presented above. This proved to be not such an easy task because none of the three protocols have reached a stage of maturity. They are all opened to new improvements.

In case of the 802.11 standard, the hidden terminal problem is solved, but the Quality of Service (QoS) in loaded or large networks. Because low latency and high reliability are very important in VANETs, the authors conclude that 802.11 is not suitable for real-time traffic. But 802.11 has also its advantages over the ADHOC MAC protocol: it can handle better high mobility and does not need time synchronization. The 802.11p standard looks very promising, and, once published, should represent a real solution for VANETs.

The ADHOC MAC allows for reliable transmissions in a two-hop neighborhood. This protocol solves also the hidden terminal problem, offers a good QoS and real-time compatibility. Some disadvantages appear when the number of vehicles in the same communication area is greater than the number of time slots in a frame. Menouar et al. [6] do not specify which protocol is better in which environment (urban, suburban, highway, etc.) and only state that both protocols are interesting for VANETs.

As for the directional antennas based approach, Menouar et al. [6] consider that they are too complex and hard to manage in real implementation. Although this area should be further investigated in future. It offers good solutions in terms of transmission collisions, network throughput and medium reuse possibilities.

5 Conclusions

The scope of this seminar paper is to present some MAC protocols that are or can be used in VANETs. As seen in the introduction, VANETs are a special type of MANETs. They have some advantages, but also some disadvantages over MANETs. Restricted mobility, no energy/storage limitations and GPS positioning are some of the pluses of VANETs. On the other hand they suffer from high topology changes and they require smaller latency and higher reliability.

Menouar et al. [6] presented three MAC protocols that are suited for VANETs. Each of them has its advantages and disavvantages, but most important they all are being further developed trying to better adapt them for inter-vehicular communication. One issue not discussed the article is the aspect of security. It is very important that VANETs are shielded from potential attacks and that the privacy of the data is guaranteed.

We can conclude that for inter-vehicular communication there are no clear scenarios and standardized protocols, but a lot of research is done in this area, on one hand because of its market value, and on the other hand because it can help save peoples lives. Considering the huge number of vehicles and the expected benefits, VANETs are likely to become the most important realization of mobile ad hoc networks.

References

[1] Contention (telecommunications) from Wikipedia, the free encyclopedia. `http://en.wikipedia.org/wiki/Contention_(telecommunications)` [Last accessed 2010-02-06].

[2] Official IEEE 802.11 Working Group Project Timelines. `http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm` [Last accessed 2010-02-07].

[3] Flaminio Borgonovo, Antonio Capone, Matteo Cesana, and Luigi Fratta. ADHOC MAC: New MAC Architecture for Ad Hoc Networks Providing Efficient and Reliable Point-to-Point and Broadcast Services. *Wirel. Netw.*, 10(4):359–366, 2004.

[4] Lee Copeland. QuickStudy: Packet-Switched vs. Circuit-Switched Networks. http://www.computerworld.com/s/article/41904/Packet_Switched_vs._Circuit_Switched_Networks [Last accessed 2010-02-06].

[5] Jun Luo and Jean-Pierre Hubaux. A survey of inter-vehicle communication. Technical report, School of Computer and Communication Sciences, EPFL, 2004.

[6] Hamid Menouar, Fethi Filali, and Massimiliano Lenardi. A Survey and Qualitative Analysis of MAC Protocols for Vehicular Ad Hoc Networks. *IEEE Wireless Communications*, 13(5):30–35, October 2006.