17

MAC PROTOCOLS FOR VANET

MOHAMMAD S. ALMALAG, MICHELE C. WEIGLE, AND
STEPHAN OLARIU

ABSTRACT

Two major goals of vehicular ad hoc networks (VANETs) are to improve road safety and to increase transportation efficiency. In order to achieve these goals, a reliable and efficient medium access control (MAC) protocol is required. MAC protocols for VANETs must balance the delivery success rate, delay, throughput, bandwidth utilization, fairness and overhead of the transmitted packets. In this chapter we provide an overview of the characteristics of VANETs that must be considered in developing MAC protocols appropriate for VANETs. We also provide an overview of the current MAC standards for VANETs, in particular IEEE 802.11p and WAVE. We outline several proposed MAC protocols for VANETs and describe how they differ from the standard. Finally, we propose a cluster-based MAC protocol that uses TDMA to reduce collisions and provide fairness among vehicles.

17.1 INTRODUCTION

Vehicular ad hoc networks (VANETs) are an important component of Intelligent Transportation Systems (ITS). VANETs enable the exchange of messages between vehicles and between vehicles and infrastructure. Such communications aim to increase safety on the road and provide comfort to drivers and passengers.

Mobile Ad Hoc Networking: Cutting Edge Directions, Second Edition. Edited by Stefano Basagni, Marco Conti, Silvia Giordano, and Ivan Stojmenovic.

Several ongoing research projects supported by car manufacturers, governments, and academia are establishing standards for VANETs, obtaining frequency spectrum allocations, implementing protocols and applications, and running field trials. However, the widespread deployment of such technology poses several technical issues, concerning architecture, routing, mobility, channel modeling, security, performance, and applications definitions.

The specific characteristics of VANETs make their quantitative and qualitative analysis particularly critical, especially when designing medium access control (MAC) layer protocols. Even though VANETs are considered to be a class of mobile ad hoc networks (MANETs), they have a number of specific characteristics that make many solutions for general MANETs unsuitable for VANETs [1]. Some of the VANET characteristics that influence the design of an ideal MAC protocol are:

- Number of Nodes. The node density of a VANET may vary. It can be small as in rural areas or large as during rush hour in a large city. It is important to have a MAC protocol that can deal with both cases. The main challenge in rural areas is network disconnection, while scalability is the main challenge in high-density areas.
- High Node Mobility. Nodes in a VANET can move at very high speeds (160 km/h), which might lead to frequent disconnection among nodes. If one node is moving at a very high speed (140 km/h) and connected to a node that is moving at a very low speed (30 km/h), the lifetime of the link will be short.
- Predictable Network Topology. The movement of nodes in a VANET is somewhat predictable because node movement is constrained by the road topology.
- Frequently Changing Network Topology. Due to high node mobility, the network topology in a VANET changes very frequently. It is important to have a MAC protocol that can adapt to frequent changes in the topology in a seamless way.
- Availability of Location Information. Location information can be provided by having a Global Positioning System (GPS) receiver on board. Having such information for communications not only can reduce delivery latency of message dissemination but can increase system throughput.
- Infrastructure Support. Unlike most MANETs, VANETs can take advantage of infrastructure on the roads. This could enhance the performance of VANET MAC protocols.
- No Power Limitation. Unlike MANET nodes, nodes in VANET have no energy limit. They depend on a good power supply (e.g., vehicle battery). This allows nodes to have better computation resources.

Besides the characteristics of VANETs, MAC protocol design should consider different types of messages in VANETs and their dissemination requirements. There are three types of messages: periodic messages, event-driven messages, and informational messages. These three types of messages have different priorities but must share the same bandwidth. Periodic messages are generated to inform nearby vehicles about the vehicle's current status—for example, speed, position, and direction [2]. Because information in periodic messages is important to all vehicles surrounding the sender, these messages need to be broadcasted frequently. Because of this, periodic messages may cause the broadcast storm problem, leading to contention, packet collisions, and inefficient use of the wireless channel [3]. Event-driven messages are emergency messages sent to other vehicles based on unsafe situations that have been detected. This type of message has a very high priority. There are several applications in VANETs that use this type of message—for example, Collision Avoidance Systems (CCA) [4]. The challenge with this type of message is that the sender needs to make sure that all vehicles intended to benefit from these messages receive them correctly and quickly [5]. Informational messages are non-safety application messages. They help in making driving more convenient and comfortable. An example of this type of message is one facilitating Internet access to the vehicles [6]. Unlike the other types of messages, this type does not require high priority, but may require a high transmission rate.

As the number of nodes in VANET increases, the number of all type of messages that need to be transmitted will increase. In this case, VANET may be experiencing contention, which occurs when one node wants to transmit while another node is already sending. IEEE 802.11 handles this through a backoff mechanism. When a frame arrives for transmission, the node checks the status of the channel. If the channel is idle and remains idle for the length of a certain amount of time (DIFS period), the frame can be transmitted. If the channel is busy, or becomes busy during the DIFS period, backoff occurs. The node picks a random value between 0 and CW_{min} as the backoff timer value (BT). If the channel becomes idle and remains idle for a DIFS, the BT can start being decremented. For each additional slot time that the channel remains idle, the BT is decremented. When BT reaches 0, the frame can be transmitted. If, at any time during backoff, the channel becomes busy, countdown is paused until the channel is idle for a DIFS. A node that picks a lower BT will have its countdown complete sooner and be able to access the channel sooner. Contention does not necessarily result in lost data, but it does result in delayed data. This can be problematic for VANETs, where much data are time-sensitive.

Another problem in VANETs is that most transmissions are broadcast. Broadcast wireless transmissions do not use MAC-layer acknowledgments (ACKs). ACKs are normally sent by a receiver for each frame successfully received. When a node fails to receive an ACK in a certain amount of time, it doubles its CW_{min}, which increases the amount of time it will likely have to wait before sending the retransmission. Since broadcast has no ACKs and therefore no retransmissions, CW_{min} is never adjusted. Because of this, all nodes will have the same CW_{min}, which increases the probability that two nodes will pick the same BT value. IEEE 802.11 includes a mechanism (RTS/CTS) to prevent collisions for unicast transmissions, but unfortunately most VANET transmissions are beacons sent via broadcast and cannot use RTS/CTS.

17.2 MAC METRICS

Considering the challenges in VANETs, MAC protocols should be evaluated considering several metrics:

- Throughput. This is the average number of successfully received bytes per second. This metric is based on one-hop broadcast communications.
- Reliability. The reliability in a VANET is measured as the probability of receiving a periodic message from a given vehicle within each transmission cycle.
- Channel Access Time. It is the time between application passing message to the MAC layer and the frame leaving the vehicle.
- Fairness. The fairness is measured by maximizing the equality of sharing the channels among vehicles.
- Overhead. In designing a MAC protocol for VANETs, control messages may need to be exchanged between vehicles for channel reservations. The amount of overhead added should be considered.
- Quality of Service. It is important to achieve a certain level of quality of service (QoS) to support multimedia communication in VANET. A MAC protocol for VANET should allow vehicles to send and receive non-safety messages without any impact on the reliability of sending and receiving safety messages even if the traffic density is high.

17.3 IEEE STANDARDS FOR MAC PROTOCOLS FOR VANETs

In the United States, the Federal Communication Commission (FCC) has allocated 75 MHz of spectrum at 5.9 GHz for Dedicated Short-Range Communications (DSRC) [7], which provides high-speed communication between the vehicles and roadside units (RSUs). DSRC is divided into seven channels, each 10 MHz wide, as shown in Figure 17.1. Channel 178 is the control channel (CCH), which is used for beacon messages, event-driven emergency messages, and service advertisements. The remaining six service channels (SCHs) support non-safety applications provided by RSUs.

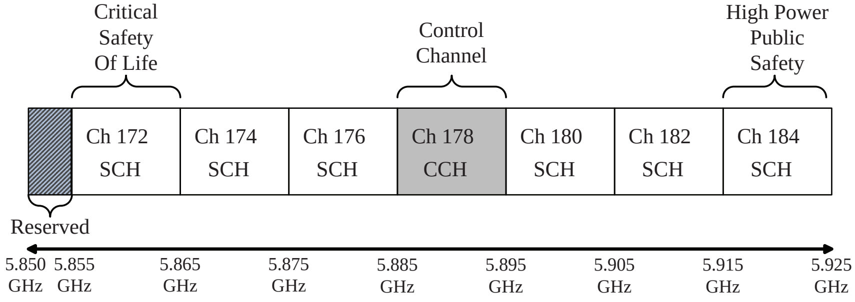

Figure 17.1 US DSRC spectrum allocation.

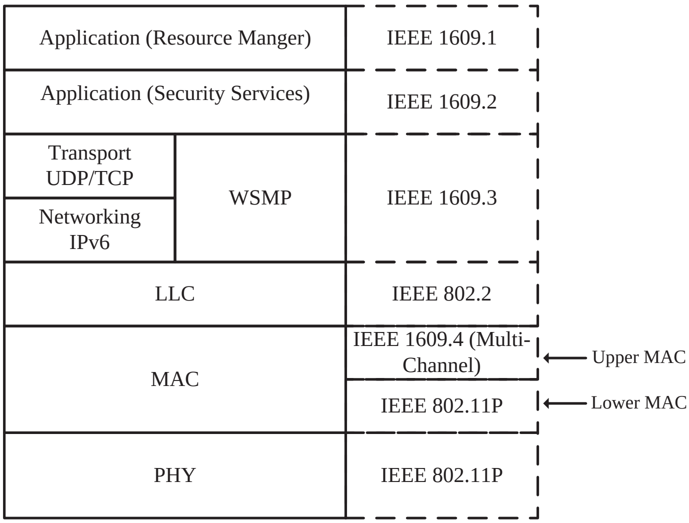

Figure 17.2 The WAVE Protocol stack.

The IEEE has completed the 1609 family of standards for the Wireless Access in Vehicular Environments (WAVE) standard [8] for vehicular communications. In remainder of this section, we explain the WAVE standard as well as the challenges and issues of WAVE MAC.

17.3.1 The IEEE 1609 WAVE Standards

IEEE 1609 WAVE is family of standards for vehicular communication encompassing vehicle-to-vehicle as well as vehicle-to-infrastructure communications [8]. WAVE specifies the following standards, as shown in Figure 17.2:

- IEEE 1609.1 specifies the services and interfaces of the WAVE Resource Manager application, [9].
- IEEE 1609.2 defines secure message formats and processing [10].
- IEEE 1609.3 presents transport and network layer protocols, including addressing and routing, in support of secure WAVE data exchange [11].
- IEEE 1609.4 specifies MAC and PHY layers, which are based on IEEE 802.11. This is the main focus of this chapter.

17.3.2 The IEEE 1609.4 Standard

In WAVE, the IEEE 1609.4 trial standard [12] operates on top of the IEEE 802.11p in the MAC layer. IEEE 1609.4 focuses mainly on dealing with multichannel operations of DSRC radio, as shown in Figure 17.3. There is a sync interval (SI) that consists of a

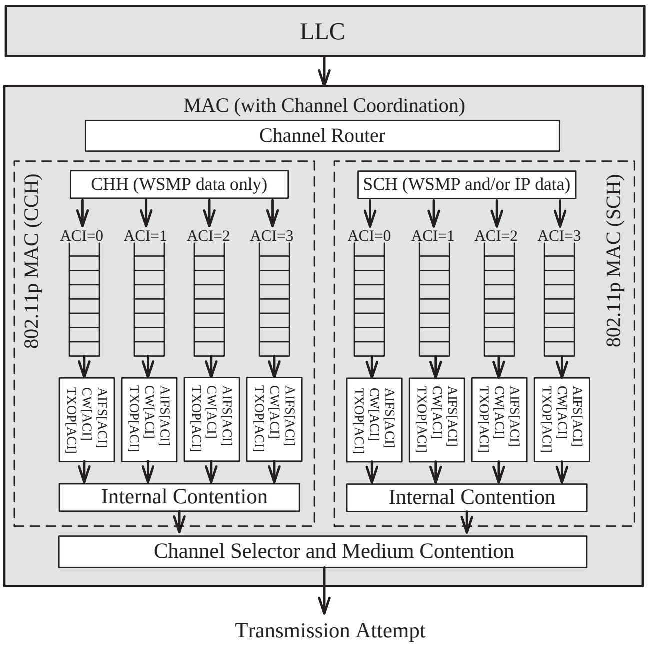

Figure 17.3 Reference architecture of the MAC channel coordination. (Based on Figure 4 of IEEE Trail-Use Standard for Wireless Access in Vehicular Environments (WAVE)-Multi-channel Operation.

CCH interval (CCHI) and a SCH interval (SCHI), each separated by a guard interval, as shown in Figure 17.4. All radio devices are assumed to be synchronized using a Global Positioning System (GPS). During the CCHI, all radios must be tuned to the CCH to broadcast updates and listen for messages from neighbors and RSUs. During the SCHI, vehicles may tune to the SCH of their choice, depending on the services offered.

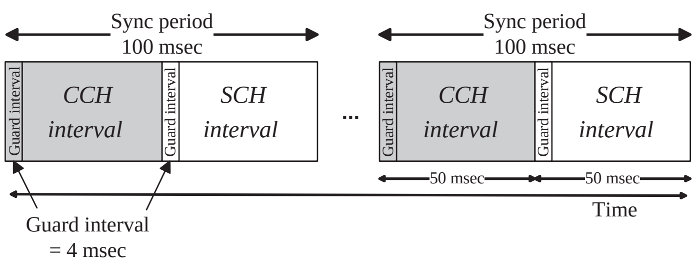

Figure 17.4 Division of time into CCH intervals and SCH intervals, IEEE 1609.4 standard (based on reference 12).

The standard defines the length of the SI as 100 ms, based on the desire of having 10 safety messages sent per second. It also defines a guard interval (GI) at the start of each CCHI and SCHI. The purpose of the GI is to account for the channel switching. Currently, the value of the GI is 4–6 ms, which is the time overhead for a radio to be tuned to and made available in another channel.

17.3.3 The IEEE 802.11p Standard

The IEEE 802.11p [13] standard is the foundation of the IEEE 1609 WAVE family of standards. It defines the physical and the medium access control layers. The WAVE stack uses IEEE-802.11p, which is based on CSMA/CA as defined in IEEE 802.11 as the MAC protocol; it includes the QoS amendments of IEEE-802.11e. Recently, IEEE has completed work on the 802.11p local area network standard that employs IEEE 802.11e Enhanced Distributed Channel Access (EDCA). Figure 17.3 gives an overview of the EDCA architecture and the type of channels that are supported, CCH and SCHs. For the IEEE 802.11p, different Arbitration Inter-Frame Space (AIFS) and Contention Window (CW) values are chosen for different application categories (ACs). There are four available data traffic categories with different priorities: background traffic (BK), best effort traffic (BE), voice traffic (VO), and video traffic (VI). Each data traffic category has its own queue; there are four different queues for each channel. Table 17.1 shows the parameter settings for different application categories in IEEE 802.11p.

Based on the nature of VANET, IEEE 802.11p has to have different MAC operations than IEEE 802.11. Here is a brief description of some of the changes at IEEE 802.11 MAC [14]:

- *WAVE Mode*. Since safety communications in VANETs demand fast data exchange, IEEE 802.11 MAC operations are too time-consuming. Scanning channels for the beacon of a Basic Service Set (BSS) and performing multiple handshakes to establish the communications is not affordable. Therefore, in the WAVE mode, vehicles are in the same channel and the same BSSID in order to communicate without any additional overhead.
- *WAVE BSS*. The WAVE standard defines a new BSS type, WAVE BSS (WBSS). When a vehicle/RSU wants to form a WBSS, it transmits an on-demand beacon. This beacon is of a specific format and used to advertise a WAVE BSS.

Table 17.1 IEEE 802.11p Parameter Settings for Different Applications Categories

AC	CW_{min}	CW_{max}	AIFSN
VI	3	7	2
VO	3	7	3
BE	7	225	6
BK	15	1023	9

The process taken to join the WBSS or not is done by the upper layers. Also, the WAVE advertisement includes all the information needed by the receiver to configure itself into a member of the WBSS. The way WBSS works leads to low setup overhead by discarding all association and authentication processes.

17.3.4 Challenges and Issues of WAVE MAC

As currently envisioned, WAVE allows for the communications of safety and non-safety applications through a single DSRC radio. Unfortunately, it has been shown that DSRC cannot support both safety and non-safety applications with high reliability at high traffic densities. Either safety applications or non-safety applications must be compromised. To maintain the 100-ms requirement of safety applications and ensure reliability, the CCHI must be lengthened and the SCHI shortened. Wang and Hassan [15] studied this scenario, requiring 90% and 95% reliability for CCH messages with different traffic densities. Their results indicate that as traffic density increases, ensuring CCH reliability requires compromising SCH throughput. At high densities, to avoid compromising non-safety applications, the SI would need to be lengthened. This would result in fewer beacon messages sent per second, compromising safety.

17.4 ALTERNATE MAC PROTOCOLS FOR VANET

The issues of MAC protocols for WAVE, as described above, led researchers in developing new MAC protocols for VANETs. In general, MAC protocols can be classified into three different categories: channel partitioning, random access, and taking turns [16]. In this section we survey some of the most recent research efforts on MAC protocols for VANET. We will discuss the MAC protocols based on the categorization above.

17.4.1 Channel Partitioning

Channel partitioning MAC protocols are based on sharing the channel efficiently at high uniform load. In MAC layer, channel partitioning is done using the following methods: Time-Division Multiple Access (TDMA), Frequency-Division Multiple Access (FDMA), and Code-Division Multiple Access (CDMA). In this section we will discuss some of the MAC protocols for VANET designed using TDMA.

In VANETs, TDMA is used to enable multiple nodes to transmit on the same frequency channel. It divides the signal into different time frames. Each time frame is divided into several timeslots, where each node is assigned to a timeslot to transmit [17]. The length of the timeslot may vary, based on the needs of the node assigned to it. The nodes will transmit in rapid succession, each using its own timeslot.

The main advantages of protocols developed under this category are reducing interference between nodes and providing fairness. However, they add allocation complexity and suffer from inefficient channel utilization at low loads.

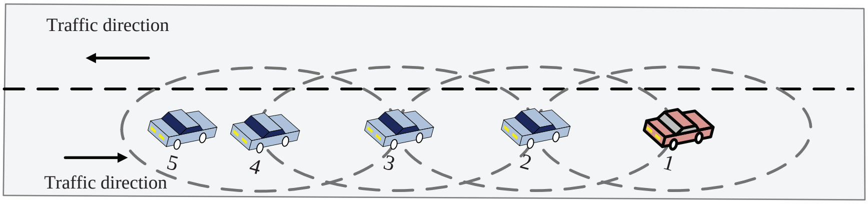

Figure 17.5 Highway scenario where the first vehicle needs to disseminate and emergency message.

17.4.1.1 Vehicular Self-Organized MAC (VeSOMAC). Yu and Biswas [18] proposed Vehicular Self-Organized MAC (VeSOMAC), a MAC protocol for intervehicular wireless networking using DSRC. They designed a self-configuring TDMA slot reservation protocol capable of intervehicle message delivery with short and deterministic delay bounds. To achieve the shortest delay, vehicles determine their TDMA timeslot based on their location and movement on the road. Also, the TDMA slot assignment is designed to be in the same sequential order with respect to the vehicles' physical location.

As shown in Figure 17.5, if vehicle 1 detects an emergency event that needs to be disseminated to other vehicles behind it, the message will go from vehicle 1 to vehicle 5 through vehicles 2–4, assuming that each vehicle is in range of only one vehicle ahead and one vehicle behind. Also there is an assumption that as soon as the message is transmitted, it can be sent by the next vehicle without processing or propagation delay. If the TDMA slot assignment is not based on the physical location of the vehicle in the platoon 1-2-3-4-5, it may take more than one TDMA frame for the emergency message to reach vehicle 5. For example, we show an alternate assignment of 4-3-2-1-5 as shown in Figure 17.6, vehicle 1 is assigned to a timeslot that is after the timeslot assigned to vehicle 2. That means vehicle 2 will finish sending to its neighbors using its timeslot before it hears the message from vehicle 1 in time frame 1. The same case applies when vehicle 2 tries to send to vehicle 3. We notice that in order for the message to be delivered from vehicle 1 to vehicle 5, four time frames are needed. Using the VeSOMAC protocol will minimize delivering the message from vehicle 1 to vehicle 5 to only one time frame by using vehicle location for the timeslot assignment, as shown in Figure 17.7.

To solve the direct and hidden terminal collisions in VANET, VeSOMAC needs to satisfy timing constraints where no two one-hop or two-hop neighbors' slots can

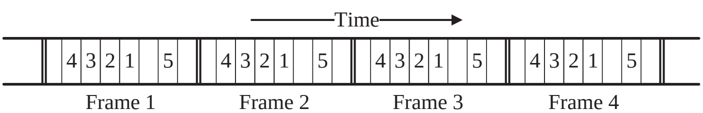

Figure 17.6 TDMA slot assignment without using VeSOMAC, regular TDMA (based on reference 18).

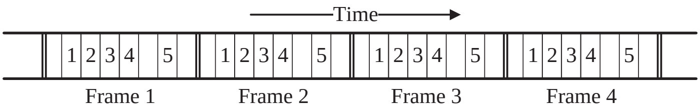

Figure 17.7 TDMA slot assignment with VeSOMAC (based on reference 18).

overlap. It also uses an in-band header bitmap to exchange slot allocation information among vehicles. To achieve faster message delivery, VeSOMAC uses an ordering constraint where the vehicle ahead will be assigned to an earlier timeslot than the vehicle behind it in the platoon.

In this protocol, the process of assigning timeslots is done without using infrastructure or virtual schedulers such as a leader vehicle. However, the assumption of forwarding messages without processing time or propagation delay is unrealistic. It shows that if the message needs to be delivered from the tail to the head of the platoon, it will need a time frame for each hop. So far, VeSOMAC does not explain the communication between vehicles and RSUs.

17.4.1.2 Multichannel MAC Protocol for Vehicular Ad Hoc Networks (VeMAC). Omar et al. [19] proposed a multichannel MAC protocol for VANETs, called VeMAC, to reduce interference between vehicles and reduce transmission collisions caused by vehicle mobility. VeMAC is based on a TDMA scheme for intervehicle communication. Vehicles in both directions and RSUs are assigned to timeslots in the same TDMA time frame. Also, VeMAC is designed based on having one control channel and multiple service channels in the network (as with DSRC/WAVE).

VeMAC assumes that there are two transceivers on each vehicle and that all vehicles are time-synchronized using GPS. The first transceiver is assigned to the control channel, while the second transceiver is assigned to the service channels. Vehicles will use the control channel to transmit two types of messages: high-priority messages (such as safety messages) and control messages for slot assignment. Since VeMAC considers vehicles in opposite directions, vehicles are said to be traveling in either the right (R) or left (L) direction. With the information provided by GPS, vehicles can determine their direction; if a vehicle is moving from west to east (north to south), it is in the right direction (R) and opposite vehicles are in the left direction (L), as shown in Figure 17.8. The time frame in VeMAC is divided into three different slots sets, L, R, and F, as shown in Figure 17.9. Vehicles in the right direction (R) will be assigned to timeslots in the time frame from the R slot set, vehicles in the left direction (L) will be assigned to timeslots from the L slot set, while RSUs will use slots in the F slot set.

In VeMAC, each vehicle is guaranteed to access the control channel once per frame. Also, vehicles have equal opportunities to announce for services provided on the service channels. To avoid the hidden terminal problem, each vehicle in VeMAC includes in the header of each packet transmitted on the CCH the following information: the timeslots used by the vehicle on the SCH, the timeslot used by each neighboring vehicle on the CCH, the timeslots used by each neighboring vehicle on the SCH, and

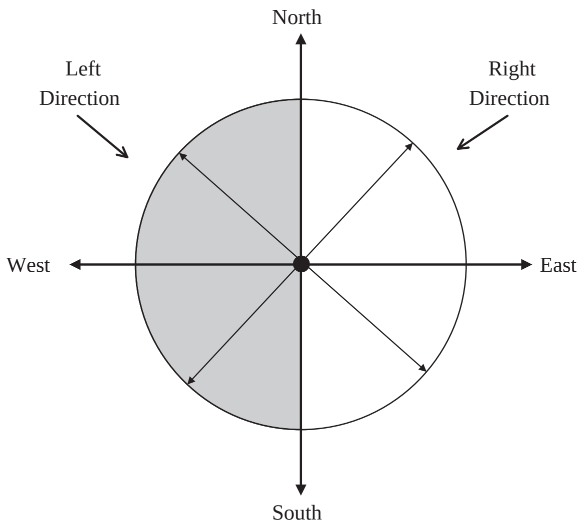

Figure 17.8 Vehicles directions in VeMAC. Vehicles in the dark area are considered to be in the left direction, while others are in the right direction.

the position and the current direction of the vehicle. By using this information, each vehicle can determine the set of timeslots used by other vehicles within its two-hop range, which will help in avoiding the hidden terminal problem.

17.4.1.3 TDMA Slot Reservation in Cluster-Based VANETs. We propose a new dynamic TDMA slot assignment technique for cluster-based VANETs. In this technique, the collision-free intra-cluster communications are managed by the clusterhead using TDMA. As a result, we encounter three important problems. These problems are cluster formation, cluster maintenance, and slot assignment. In this work we propose three algorithms to solve the addressed problems. Since the main focus of this chapter is MAC protocols in VANET, we will explain the slot assignment algorithm. The cluster formation algorithm is explained in reference 20.

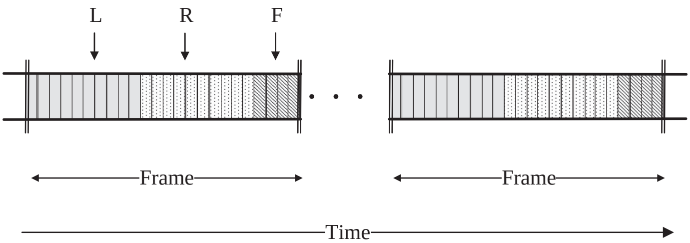

Figure 17.9 TDMA time frame in VeMAC shows L, R, and F sets (based on reference 19).

The presentation of our technique involves several aspects of intra- and inter-cluster communication. In turn, each of these communication regimes is partitioned into cases depending on whether or not the cluster is single-hop. The clustering technique we are using is clusterhead-based, where the consensus is dictated by the clusterhead (CH). We also assume that all vehicles are equipped with GPS to ensure that vehicles have synchronized clocks.

To explain our technique, we assume an N-vehicle cluster. The transmission time is partitioned into consecutive, nonoverlapping logical TDMA frames. We assume the existence of k slotted SCHs numbered from 0 through $k-1$. In each SCH, the logical TDMA frames are aligned—that is, begin and end at the same time. Each logical frame contains $\left\lfloor \frac{N}{k} \right\rfloor + 1$ slots numbered from 0 through $\left\lfloor \frac{N}{k} \right\rfloor$. Also, all slots are the same size; the slot τ is known to all vehicles in the cluster. We also assume that one CCH, channel k, is used by the vehicles and CH for disseminating status and/or control messages; we anticipate the size of a mini-slot to be sufficient to allow individual vehicles to communicate their status information. By virtue of synchronization, the vehicles know frame and slot boundaries. The number of vehicles (N) may change dynamically, and the CH is responsible for updating N and for informing all vehicles in the cluster of the new value of N.

Each vehicle in the cluster will receive a local ID. This local ID is a number from 0 to $N-1$. The CH will have always ID 1, while ID 0 is reserved for a “virtual vehicle.” Other than exceptionally, we do not expect all N vehicles in the cluster to be communicating, or active, simultaneously. The CH keeps a list of all the currently active vehicles and disseminates this list to all the members of the cluster using one of the mechanisms discussed below.

In each logical frame, vehicle j $(0 \leq j \leq N-1)$ owns:

- channel $j \bmod k$ during timeslot $\left\lfloor \frac{j}{k} \right\rfloor$; we also say that vehicle j owns the ordered pair $\left(j \bmod k,\ \left\lfloor \frac{j}{k} \right\rfloor\right)$
- the jth mini-slot of slot $\left(\left\lfloor \frac{j}{k} \right\rfloor - 1\right) \bmod \left\lfloor \frac{N}{k} \right\rfloor$, on channel k, as illustrated in Figure 17.10 below; we use the convention that $\left(-1 \bmod \left\lfloor \frac{N}{k} \right\rfloor\right)$ is the $\left\lfloor \frac{N}{k} \right\rfloor$-th slot of the previous logical frame (as shown in Table 17.2).

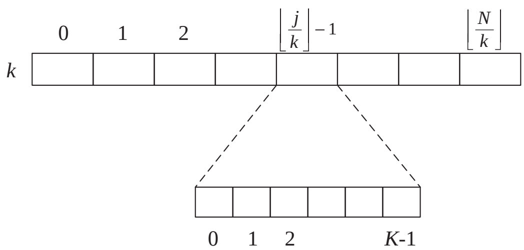

Figure 17.10 Mini-slots on channel k; car j owns a mini-slot in the slot preceding its own slot.

The basic idea is that in each logical frame, while idle, vehicle j listens to channel $j \bmod k$ in slot $\left\lfloor \frac{j}{k} \right\rfloor$ and sets the corresponding byte in the CCH in order for other vehicles to be aware. Notice that the Integer Division Theorem guarantees that if $i \neq j$, then either

$\left\lfloor \frac{i}{k} \right\rfloor \neq \left\lfloor \frac{j}{k} \right\rfloor$ or
$i \bmod k \neq j \bmod k$, or both

This confirms that no two vehicles own the same ordered pair. For an illustration, let $N = 61$ and $k = 6$. As shown in the Table 17.2, car 39 owns channel $(39 \bmod 6) = 3$ during slot $\left\lfloor \frac{39}{6} \right\rfloor = 6$, as well as the 4th mini-slot on the control channel in slot $6 - 1 = 5$.

In intra-cluster communication, we are looking at the single-hop cluster case first; multihop cluster intra-cluster communication will be investigated later. Our goal is to design lightweight communication protocols that avoid, to the largest extent possible, the involvement of the CH in setting up connections between vehicles. As a single-hop cluster, all vehicles in the cluster can communicate directly. Consequently, the vehicles do not need to discover their neighbors.

17.4.2 Random Access

Random access MAC protocols, also known as contention-based protocols, are based on the notion of CSMA. The goal of MAC protocols is to increase throughput, so protocols under this category aim to keep packet collisions to a minimum. The advantage of random access protocols is that they are not sensitive to underlying mobility and topology changes. So, vehicle movement does not impose any reconfiguration overhead due to the network topology changes. Also, CSMA protocols are efficient in low-load scenarios. However, in networks such as VANET, the hidden terminal problem and exposed terminals affect the system performance. Several random access MAC protocols for VANETs have been proposed, some of which will be described below.

17.4.2.1 Carrier-Sense Multiple Access with Priority and Polling (PP-CSMA). Yang et al. [21] proposed carrier-sense multiple access with priority and polling (PP-CSMA) as a MAC protocol for VANETs that is based on a priority scheme in CSMA using different backoff time spacing (BTS). The authors claim that their protocol will provide high-priority messages with fast access to the medium.

PP-CSMA proposes the prioritization scheme as a combination of the closeness of the transmitting vehicle to the receiving vehicle and the message type. The position of the transmitting vehicle to the receiving vehicle will determine the vehicle range (far, medium, low, and close); if the range is short, the priority gets higher. Also, the type of message (emergency or general) will have an effect on the priority; emergency messages have higher priority than general messages. Table 17.3 shows four different levels of priority, the high priority level backs off for the least amount of time.

Table 17.2 Shows the Logical Frames

Channel\Slot	0	1	2	3	4	5	6	7	8	9	10
5	5	11	17	23	29	35	41	47	53	59	Unused
4	4	10	16	22	28	34	40	46	52	58	Unused
3	3	9	15	21	27	33	39	45	51	57	Unused
2	2	8	14	20	26	32	38	44	50	56	Unused
1	1	7	13	19	25	31	37	43	49	55	61
0	Reserved	6	12	18	24	30	36	42	48	54	60
Mini-slot ownership	[6–11]	[12–17]	[18–23]	[24–29]	[30–35]	[36–41]	[42–47]	[48–53]	[54–59]	[60–65]	[1–5]

Table 17.3 Priority Scheme with four Levels (Based on Table from reference 21)

	Description	
Priority Level	Vehicle Range	Message Type
Level 0	Far	General
Level 1	Medium	General
Level 2	Low	General
Level 3	Close	Emergency

Besides the priority scheme, the PP-CSMA protocol implements a polling scheme in which the receiving vehicle polls only vehicles with the highest priority level available. Each vehicle maintains a polling table that holds information about other vehicles' positions. If a vehicle has an emergency message to be sent, it generates a tone, which is out of the frequency band used for data transmission. If the vehicle is in the receiver's polling table, the receiver will clear for the sender to transmit the message. If the polling vehicle does not generate a tone, the receiver vehicle will know it is not an emergency message. The PP-CSMA protocol guarantees that the highest-priority messages will always have access to the medium faster than the low priority messages. However, the authors did not mention broadcasting, which is an important challenge in VANET.

17.4.2.2 Priority-Based Intervehicle Communication in Vehicular Ad Hoc Networks Using IEEE 802.11e. In this protocol, Suthaputchakun and Ganz [22] proposed a MAC protocol for VANETs that is based on different message priorities, as in IEEE 802.11e EDCA MAC protocol, with a repetitive transmission mechanism. This protocol aims to increase the communication reliability by using the appropriate number of repetitions per priority class.

Since most of the communications in VANET are broadcast messages with no RTS/CTS or acknowledgment, the network reliability can be low. To solve this problem, the authors proposed a mechanism of retransmission the messages based on the priority of the message. Table 17.4 shows the priority levels as well as the number of repetitions for each level.

17.4.2.3 Improvement in Congestion Control, Broadcast Performance, and Multichannel Operation for Safety Communications in VANET. Jiang et al. [23] proposed a set of protocols for safety communications in VANETs. They define three different protocols: CCH congestion control protocol, broadcast performance enhancement protocol, and concurrent multichannel operation protocol. These protocols are designed to address the issues of the current standard and meet the requirements of safety communications in VANETs.

The CCH congestion control protocol is designed around adjusting the generation rate of routine safety (periodic) messages and the transmission power. Based on the communication density [24], vehicles should be able to calculate the generation rate and transmission power of routine safety messages which will maintain a reasonable

Table 17.4 Different Message Priorities with Parameters; Based on reference 22.

Priority Level	Type	Example	CWmin	CWmax	AIFS	Number of Repetitions
Level 1	Accident	• Air bag sensor • Vehicle's body sensor	$CW_{min}/4$	$CW_{min}/2$	2	3
Level 2	Possibility of accident	• Thermal sensor • Hard break	$CW_{min}/2$	CW_{min}	3	1
Level 3	Warning	• Surface condition • Blind crossing • Road work warning • Pressure sensor in wheels	CW_{min}	CW_{max}	3	1
Level 4	General	• Traffic report • Weather condition	CW_{min}	CW_{max}	7	1

CCH load. These adjustments are done by each vehicle individually. Each vehicle will listen and understand the targeted channel usage and then ensure that its share of the channel will keep a reasonable channel congestion level.

For the broadcast performance enhancement, the authors proposed a mechanism that aims to ensure the best possible reception rate for the event safety (event-driven) messages. The way it works is by the sending vehicle collecting feedback from other vehicles on its recent safety message. This feedback will help the safety application(s) on retransmitting the safety message, if needed. The feedback from other vehicles is provided by piggybacking some acknowledgments in their safety messages [25]. For the acknowledgments, vehicles will include the following information in each outgoing safety message: sender's position, the intended range of reception, a randomly generated message ID, IDs of most recently received messages, and the reception time of the earliest message in the acknowledgment list.

In the concurrent multichannel operation protocol, the authors intend to increase the level of SCHs utilization, for non-safety messages, with satisfying the safety messages requirements. In VANETs, channel switching between CCH and SCHs is operated every 100 ms. Vehicles will operate the switching in order to listen to safety and non-safety messages; if the number of safety messages is high, non-safety messages will have less time to be transmitted. To increase the SCHs utilization, this protocol is built on the concept of listening to all safety messages is not required if (1) routine safety messages from all nearby vehicles are heard every few seconds and (2) all event safety messages from nearby vehicles are received without excessive delay. To do that, the authors used the Peercast. The Peercast concept relies on trusting peer vehicles' description of recent control channel messaging activities. The following steps will describe the Peercast concept: (1) Each vehicle must switch to the CCH every time it has a safety message to transmit. (2) Each vehicle must switch to the CCH (e.g., every 100 ms) to hear a few safety messages from its neighbors. (3) while on the CCH: (a) if it hears no safety messages, it may switch back to SCH,

(b) else, if it hears an event safety message, it passes it to safety applications and may switch to SCH; (c) else, if it hears an event safety message with unknown ID, it must stay on CCH to capture the repetition of the message before switching back to SCH. (4) Each vehicle must switch to CCH every time a safety application requested. (5) Each vehicle must switch to CCH every a few second for a short period of time to reorient itself with other vehicles' routine messages.

17.4.3 Taking Turns

Taking turns MAC protocols use either polling (master–slave) or token ring techniques. Such techniques provide fairness by giving each node a turn to transmit. They also provide a real time bandwidth allocation. If the node is not transmitting during its turn, the time will be not wasted at the current node. We describe an example of a token-ring-based MAC protocol for VANETs in this section.

17.4.3.1 A Multichannel Token Ring Protocol for QoS Provisioning in Intervehicle Communication (MCTRP). In this work, Bi et al. [26] proposed a multichannel token ring MAC protocol for intervehicle communications in VANET (MCTRP). The protocol aims to reduce the delay of safety messages and improve the dissemination of nonsafety messages, based on the multichannel structure defined in IEEE 802.11p. This can be achieved through adapting multiple rings operating on different service channels.

MCTRP is designed to support more than one token ring at a time. These rings are formed according to the velocity of vehicles and the road conditions. As shown in Figure 17.11, vehicles forming one ring may have different states: (1) *ring founder node (RFN)*: a node that sets up a ring and has the authority to cancel the ring, adding new nodes to the ring, and deleting nodes from the ring; (2) *token holder node* (*THN*): a node that in the ring and holds the token; (3) *ring member node* (*RMN*): a node in the ring, but does not hold the token. Vehicles that are not members of a ring may also have different states: (1) *semidissociative node* (*SDN*): a node that received the joining invitation from the RFN; (2) *dissociative node* (*DN*): a node that does not belong to any ring and not in the process of joining any ring.

Vehicles in MCTRP are equipped with two transceivers, I and II. All vehicles in the DN state operate over channel 178 using transceiver I, while other vehicles

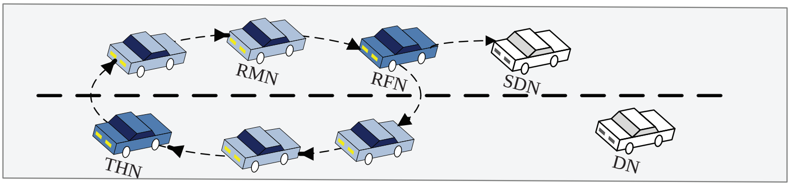

Figure 17.11 Token ring in MCTRP with different types of vehicles in the proposed protocol.

(non-DN) simultaneously operate over channel 178 using transceiver I and over one of the service channels over transceiver II. All vehicles in the system are time-synchronized using GPS.

MCTRP employs three different subprotocols for resource utilization: a ring coordination protocol, an emergency message exchange protocol, and a data exchange protocol. The ring coordination protocol contains several processes for ring management, such as ring initialization, joining, leaving, ring update, and ring termination. The emergency message exchange protocol is designed to broadcast emergency messages as fast and reliable as possible. That can be done in four steps: (1) when a RMN detects an accident, it transmit an emergency message to the RFN by adopting CSMA/CA (with Radio-II during the safety period); (2) an RFN replies with an acknowledgment to the sender RMN and then broadcasts the message to all other RMNs (with Radio-II for intra-ring notification); (3) at the same time, the RFN broadcasts the message to its neighboring DNs and other RFNs (with Radio-I for inter-ring notification); (4) the other RFN rebroadcasts the emergency message to its RMNs. The data exchange protocol is designed on having to data buffers in each node. The intra-ring data buffer (IADB) holds packets to be transmitted to other RMNs in the same ring, and the inter-ring data buffer (IRDB) holds packets to be transmitted to nearby DNs, SDNs, and RMNs. For intra-ring data communications, an RMN will send packets when it receives the token, and the IADB is not empty. The transmission time of the THN is controlled by the token maximum hold time T_{MTH}. Once the T_{MTH} is reached, the THN will pass the token to its successor. To ensure token delivery, THN will retransmit the token if it does not receive an acknowledgment (ACK) from its successor and the retransmission timer has expired. If the maximum number of retransmissions is reached with no ACK from the successor, the THN will report to the RFN, and the RFN will delete the successor from the ring and update the ring as well as informing other RMNs. For the inter-ring data communications, data packets are transmitted with CSMA/CA mechanism.

MCTRP shows that it can deliver emergency messages in fast way and enhance the network throughput. It also provides fairness among vehicles, in terms of (a) channel sharing and (b) token holding time adjustment.

17.5 CONCLUSION

In this chapter we have presented a broad overview of MAC protocols for VANETs, including the standards and some alternative MAC protocols for VANETs. We have discussed the characteristics of VANETs that influence the design of MAC protocol and make it different than MANET's MAC protocols. Then we have summarized the MAC metrics that need to be considered in evaluating MAC protocols.

Some changes have been made at IEEE 802.11 MAC to meet the nature of VANET, IEEE 802.11 p, as well as introducing IEEE 1609.4 standard. There are still some issues in the standards for the MAC protocols for VANETs, and they need to be altered to meet the transmission requirements of VANET applications.

Several proposed MAC protocols have been published for VANETs to solve the issues in the standards. We have listed them in three different categories, channel partitioning, random access, and taking turns. Some examples have been explained under each category.

REFERENCES

1. J. J. Blum, A. Eskandarian, and L. J. Hoffman. Challenges of intervehicle ad hoc networks. Presented at *IEEE Transactions on Intelligent Transportation Systems*, 2004, pp. 347–351.
2. M. Almalag. Safety-related vehicular applications. In *Vehicular Networks: From Theory to Practice*, Stephan Olariu and Michele C. Weigle, Eds. Chapman & Hall/CRC, Boca Raton, FL, 2009, pp. 5-1–5-26.
3. S. Ni, Y. Tseng, Y. Chen, and J. Sheu. The broadcast storm problem in mobile ad hoc network. In *Proceedings of ACM MOBICOM*, 1999, pp. 152–162.
4. S. Biswas, R. Tatchikou, and F. Dion. Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety. *IEEE Communications Magazine* **44**(1):74–82, 2006.
5. R. Chen, W.-L. Jin, and A. Regan. Broadcasting safety information in vehicular networks: Issues and approaches. *IEEE Network: The Magazine of Global Internetworking* **24**(1):20–25, 2010.
6. Verizon Wireless [Online]. Available: http://www.verizonwireless.com/.
7. US Department of Transportation. Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems—5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications. ASTM E2213-03, 2003.
8. IEEE Draft. Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)—Architecture. P1609.0, February 2007.
9. IEEE Standards 1609.1-2006. Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)—Resource Manager, 2006.
10. IEEE Standards 1609.2-2006. Trial-Use Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages, 2006.
11. IEEE Standards 1609.3-2006. Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services, 2006.
12. IEEE Standards 1609.4, 2006. Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)—Multi-channel Operation, 2006.
13. IEEE WG, IEEE 802.11p/D2.01, Draft Amendment to Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Wireless Access in Vehicular Environments, March 2007.
14. D. Jiang and L. Delgrossi. IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments. In *Proceedings of IEEE Vehicular Technology Conference (VTC)*, Spring 2008, pp. 2036–2040.
15. Z. Wang and M. Hassan. How Much of DSRC is Available for Non-Safety Use? In *Proceedings of the Fifth ACM International Workshop on VehiculAr Inter-NETworking*, September 15, 2008, San Francisco.

16. J. Kurose and K. Ross. *Computer Networking: A Top-Down Approach*, 5th edition, Addison Wesley, Boston, MA, 2010.
17. P. Djukic and P. Mohapatra. Soft-TDMAC: A software TDMA-based MAC over Commodity 802.11 hardware. *INFOCOM 2009*, April 2009, IEEE, New York, pp. 1836–1844.
18. F. Yu and S. Biswas. Self-configuring TDMA protocols for enhancing vehicle safety with DSRC based vehicle-to-vehicle communications. *IEEE Journal on Selected Areas of Communications* **25**(8):1526–1537, 2007.
19. H. Omar, W. Zhuang, and L. Li. VeMAC: A novel multichannel MAC protocol for vehicular ad hoc networks. In *Proceedings of IEEE Infocom'11, Workshop on Mobility Management in the Networks of the Future World*, April 2011.
20. S. Mohammad Almalag and Michele C. Weigle. Using traffic flow for cluster formation in vehicular Ad-hoc networks. In *Proceedings of the Workshop On User MObility and VEhicular Networks (ON-MOVE)*. Denver, CO, October 2010, pp. 631–636.
21. S. Yang, H. H. Refai, and X. Ma. CSMA based inter-vehicle communication using distributed and polling coordination. In *Proceedings of the IEEE International Conference on ITS*, Vienna, Austria, September 2005, pp. 167–171.
22. C. Suthaputchakun and A. Ganz. Priority based inter-vehicle communication in vehicular ad-hoc networks using IEEE 802.11e. In *Proceedings of the 65th IEEE Vehicular Technology Conference (VTC-S'07)*, Dublin, April 2007, pp. 2595–2599.
23. D. Jiang, V. Taliwal, A. Meier, and W. Holfelder. Design of 5.9 GHz DSRC-based vehicular safety communication. *IEEE Wireless Communications* **13**(5):36–43, 2006.
24. V. Taliwal and D. Jiang. Mathematical analysis of IEEE 802.11 broadcast performance in a probabilistic channel. DaimlerChrysler Technical Paper, 2005.
25. D. Jiang and V. Taliwal. Vehicular safety broadcast performance assessment with piggybacked acknowledgment. DaimlerChrysler Technical Paper, 2006.
26. Y. Bi, K. H. Liu, L. X. Cai, X. Shen, and H. Zhao. A multi-channel token ring protocol for QoS provisioning in inter-vehicle communications. *IEEE Transactions on Wireless Communications* 8(11):5621–5631, 2009.