# Wireless Access Technologies for Vehicular Network Safety Applications

**Hassan Aboubakr Omar, Ning Lu, and Weihua Zhuang**

**Abstract**

Road safety is becoming urgent due to a large number of traffic accidents each year and its severe socio-economic impact on a global scale. A promising solution to improve road safety is to deploy VANETs, a technology that can make driving safer by enabling a variety of advanced road safety applications, through broadcasting of safety messages by vehicles and roadside units. This article discusses the ability of existing wireless technologies to provide reliable broadcast of safety messages, which are necessary to realize any road safety application. The wireless technologies under consideration are the IEEE 802.11p standard, the current cellular network standards, and a time-division multiple access protocol, known as VeMAC, recently proposed for VANET safety applications. The performance of the IEEE 802.11p standard is compared with that of the VeMAC protocol via computer simulations in different highway and city scenarios, including a traffic bottleneck situation caused by emergency parking of a vehicle on a highway. We also review recent developments of the VeMAC protocol, including prototype experiments and on-road demonstrations of VeMAC-based safety applications implemented in real cars.

As an indispensable part of modern life, motor vehicles have continued to evolve since they were invented during the Second Industrial Revolution. Nowadays, people spend a significant amount of times on roads, which requires a future vehicle to be safer, greener (e.g., less $CO_2$ emission), fully autonomous, and more comfortable and entertaining for passengers. Realization of all these features relies on a key technology: wireless communications. The technology can enable a variety of applications related to road safety, passenger infotainment, car manufacturer services, and vehicle traffic optimization [1, 2]. Among these categories of applications, road safety is the most urgently needed today due to a high number of road accidents happening each year, which result in a considerable number of deaths and injuries in many countries. For instance, there have been 26,000 fatalities on the roads of the European Union in 2013, and for each fatality, there is an estimated 4 permanently disabling injuries (e.g., brain damage), 8 serious injuries, and 50 minor injuries [3]. This critical public health issue is accompanied by a huge financial loss, as much as US$871 billion in the United States in 2010 [4], as a result of economic loss and societal harm due to vehicle crashes.

Given the real necessity to improve road safety, the European Commission implemented a mandatory communication system, eCall, for emergency services in cars starting in 2015. Also, in August 2014, the U.S. Department of Transportation (DOT) issued an advance notice of proposed rulemaking (ANPRM) to begin the implementation of vehicle-to-vehicle (V2V) communication technology [5]. Hence, equipping automobiles with wireless communication and networking capabilities is becoming the frontier to reduce the risk and severity of road crashes. By means of V2V communications, as shown in Fig. 1, and vehicle-to-roadside unit (V2R) communications, as shown in Fig. 2, a technology known as a vehicular ad hoc network (VANET) is realized. Based on VANET technology, many advanced safety applications can be implemented, including lane change warning, highway merge assistance, in-vehicle signage, and cooperative forward collision avoidance [1], which can play a vital role in improving public safety standards. By deploying such VANET-based safety applications, analyses done by the National Highway Traffic Safety Administration (NHTSA) at the U.S. DOT show that approximately 80 percent of road crash scenarios can be prevented [6], indicating the great potential of VANETs in providing a safer environment for drivers, passengers, and pedestrians on roads.

The majority (if not all) of the VANET safety applications require that each node (i.e., vehicle or roadside unit [RSU]) *broadcasts* safety messages to *all* the surrounding nodes. For example, in Fig. 1, the information broadcast by the braking vehicle should be successfully received by all the nearby vehicles to avoid any forward collision following the hard brake. Similarly, in Fig. 2, the information broadcast by the RSU near the traffic light should be delivered to all approaching vehicles so that the in-vehicle system can warn the driver (in case he/she is expected to be in violation) or calculate the optimal speed such that the vehicle reaches the traffic light during the green light period. The broadcast safety messages can be classified into periodic and event-driven messages [1]. The periodic messages are automatically broadcast by each node at regular intervals, while the event-driven messages are broadcast only in case of an unexpected event, such as a hard brake, an approaching emergency vehicle, or hazardous road condition detection. Hence, given that any failure or

*The authors are with the University of Waterloo.*

*Hassan Aboubakr Omar is also with Cairo University.*


0890-8044/16/$25.00 © 2016 IEEE

delay in delivering a periodic or event-driven safety message may result in undesired consequences, it is necessary that a wireless access technology proposed for VANETs supports a reliable broadcast service, which allows each node to successfully and promptly deliver its safety messages to all the surrounding nodes. Such a broadcast service is crucial to meet the quality of service (QoS) requirements of the high-priority safety applications in VANETs. In this article, we first discuss the feasibility of supporting safety applications via the current wireless communication standards: IEEE 802.11p, also known as the wireless access in vehicular environments (WAVE), and the widely available cellular network technologies. Then we present a recently developed time-division multiple access (TDMA) protocol, called VeMAC, which is proposed to overcome the limitations of the existing solutions by providing reliable broadcast of safety messages in VANETs. Computer simulations are presented to compare the performance of the VeMAC protocol with that of IEEE 802.11p, in terms of delivering periodic and event-driven safety messages in different scenarios. Also, we review recent investigations on the feasibility of the VeMAC protocol via prototype development, laboratory experiments using multiple prototype units, and demonstrations of road safety applications implemented based on VeMAC for collision avoidance in a road curve and emergency brake alert. Other wireless access technologies that have been previously proposed for VANETs, such as space-division multiple access (SDMA) and code-division multiple access (CDMA), are discussed in [7].

## IEEE 802.11p

The IEEE 802.11p standard is the main solution currently proposed for wireless access in VANETs [8]. The standard is based on the legacy IEEE 802.11 standard (WiFi), which was developed mainly for unicast communications, such as between a user device and a WiFi access point. Consequently, to support the broadcast-based safety applications in VANETs, IEEE 802.11p has considerable limitations.

The main reason for the poor performance of IEEE 802.11p in supporting safety applications is the high probability of "collision" of the broadcast safety messages. That is, if two nodes in proximity of each other are simultaneously broadcasting their safety messages, the messages will "collide" at each surrounding node that is located within the communication range of the two transmitting nodes. Consequently, these surrounding nodes cannot successfully receive any of the two colliding messages. For unicast communications, as specified in IEEE 802.11p standard, the probability of a transmission collision is reduced by using a two-way handshaking mechanism before the actual transmission of data. That is, if a source node needs to transmit a packet[1] to a destination node, it first transmits a short control packet, known as request-to-send (RTS), and waits until the destination node replies by another control packet, known as clear-to-send (CTS). Following the RTS/CTS exchange, all the surrounding nodes defer accessing the wireless channel (in order to avoid any transmission collision) until the source and destination nodes complete the exchange of the actual data, that is, the source transmits a data packet and the destination replies by an acknowledgment (ACK) packet. Unlike the unicast case, according to IEEE 802.11p, no RTS/CTS exchange should be used for broadcast packets, and no ACK should be transmitted by any recipient of the packet. Consequently, this lack of RTS/CTS exchange results in a high probability of a transmission collision, which reduces the rate

[1] The term "packet" is used to indicate the protocol data unit of the medium access control (MAC) layer.

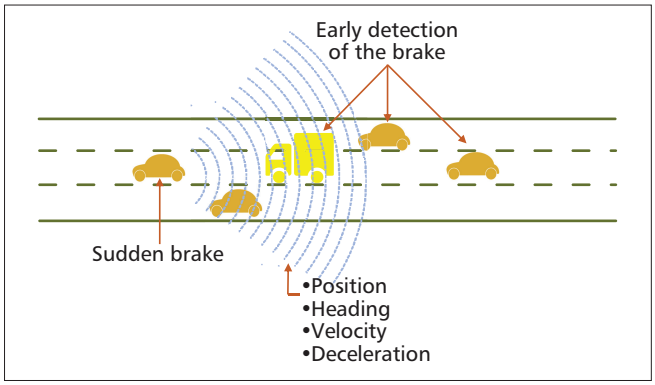


Figure 1. Illustration of V2V communications.

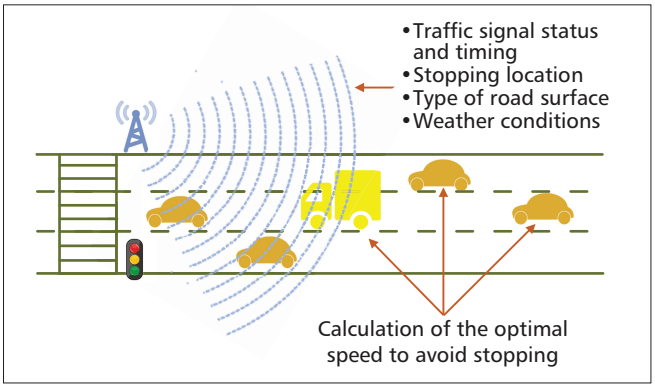


Figure 2. Illustration of V2I communications.

of successful packet delivery of the IEEE 802.11p broadcast service, especially with the absence of ACK packets.

Another limitation of the IEEE 802.11p standard is related to the enhanced distributed channel access (EDCA) scheme [8, 9], which is employed by the standard to support the QoS requirements of VANET safety applications. As shown in Fig. 3, in the EDCA scheme, there are four access categories (ACs) at each node, each of which contends to access the wireless channel by using the fundamental IEEE 802.11 technique of carrier sense multiple access with collision avoidance (CSMA/CA), but with a different set of CSMA/CA parameters assigned to each AC. This differentiation of CSMA/CA parameters, such as the contention window (CW) size, is to allow a high-priority AC to get access to the channel quicker than a low-priority one. Now, by employing the EDCA scheme to support safety applications, the safety messages will likely be assigned to the high-priority ACs, which contend for the wireless channel using a small CW size, as specified in IEEE 802.11p. Although this small CW size allows safety messages to be transmitted with small delays, it increases the probability of transmission collisions when multiple nodes within the same communication range are simultaneously trying to broadcast their safety messages. Moreover, unlike the unicast case, the CW size is not doubled when a collision happens among the broadcast safety messages (the increase of CW size reduces the probability of a transmission collision), since there is no collision detection for the broadcast service due to the absence of CTS and ACK packets.

## Cellular Network Standards

Cellular network technologies, such as the Long-Term Evolution (LTE) standard, are currently being used by car manufacturers to provide their vehicles with some applications and services, such as BMW ConnectedDrive, Audi connect, and OnStar (a subsidiary of General Motors). Such cellular network services are mainly targeted at applications providing

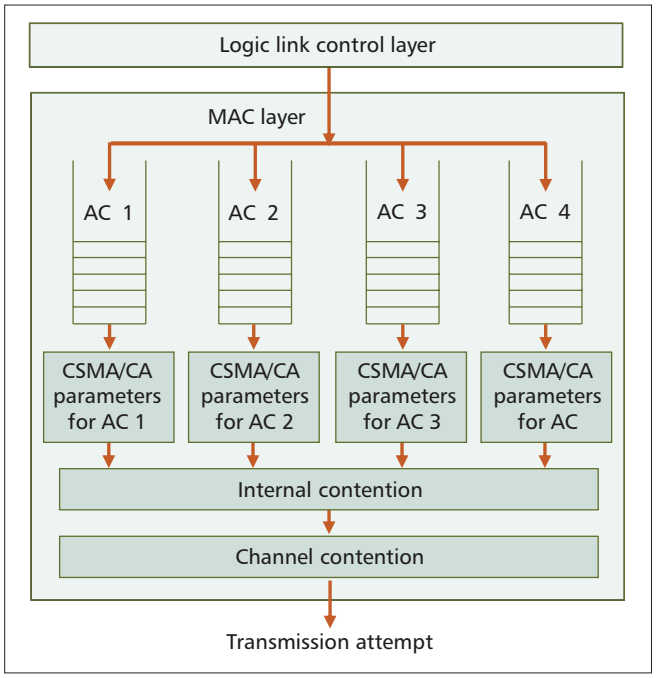


Figure 3. A simplified version of Fig. 2 of the IEEE 1609.4 standard for WAVE-multichannel operation [9].

driving assistance (e.g., turn-by-turn navigation), passenger entertainment (e.g., Internet connectivity), and remote vehicle diagnostics. However, there is no current solution for supporting VANET-based safety applications via cellular networks, even with the deployment of LTE-Advanced, which is the latest fourth generation (4G) mobile communications standard. The reasons are: first, as mentioned above, the high-priority VANET safety applications are based on broadcasting of safety messages by each node to all nearby nodes. How this location-based broadcast service can be achieved through the cellular network, within a delay that is suitable to realize road safety applications, still needs a lot of investigation. Second, it is not guaranteed that the capacity of a cellular network can accommodate the periodic and event-driven safety messages generated by a large number of vehicles, especially during rush hours, without a significant impact on the QoS provisioning for other (non-vehicular) cellular network applications, such as voice and data services. Third, by supporting road safety applications through a cellular network, these applications will not be enabled in a region that is out of the coverage map of the network operator, which may result in undesirable consequences (e.g., accidents) due to intermittent provisioning of such high-priority applications. Fourth, even if we assume that road safety applications can be perfectly realized via cellular networks, it is likely that they are going to be provided for customers by subscription, which may not be cost effective, especially in countries that have high prices of cellular network services. Finally, by employing a cellular network for providing VANET safety applications, the radio spectrum that is allocated for V2V and V2R communications in the 5.9 GHz band, for example, by the European Telecommunications Standards Institute (ETSI) or the U.S. Federal Communication Commission (FCC), will not be utilized, as the currently deployed cellular network standards operate on lower frequency bands.

## VeMAC Protocol

In order to overcome the limitations of the current solutions discussed previously, the VeMAC protocol has recently been proposed to support the periodic and event-driven safety messages in VANETs by employing TDMA [10, 11]. That is, the time is partitioned to frames consisting of a constant number of equal-duration time slots, and each second contains an integer number of frames, as shown in Fig. 4. Based on this time partitioning, VeMAC allows each node to determine in a distributed way (i.e., without need for any central controller) the time slots that the node can access to successfully broadcast its safety messages to all the surrounding nodes. This distributed time slot assignment employed by VeMAC ensures that all the nodes located in proximity of each other are assigned different time slots, and consequently provides a reliable broadcast service by eliminating the transmission collision caused by simultaneous broadcast of safety messages. If a transmission collision occurs due to node mobility (when two nodes accessing the same time slot approach each other), each colliding node can detect the collision and acquire a new time slot in order to prevent further transmission collision of safety messages. How the nodes determine which time slots to access and how they dynamically reorganize their access of the time slots to avoid any transmission collision in a distributed way are the main contributions of the VeMAC protocol.

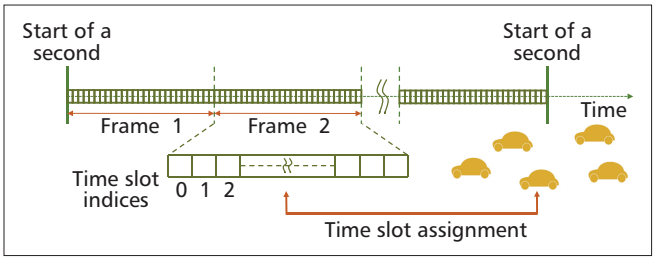


Figure 4. Time partitioning into frames and time slots.

To illustrate the VeMAC operation, consider the node configuration as shown in Fig. 5. In such a scenario, vehicles *a* and *c* cannot be assigned the same time slot; otherwise, their simultaneous broadcast of safety messages will collide at vehicle *b*, which is located within the communication range of both vehicles. Hence, vehicles *a*, *b*, and *c* are assigned different time slots by the VeMAC protocol to avoid any transmission collision of their safety messages. Note that VeMAC allows the same time slot in a frame to be simultaneously accessed by vehicles that are far from each other. For example, vehicles *a* and *d* in Fig. 5 are accessing the same time slot, since their simultaneous broadcast of safety messages is not going to collide at any vehicle. However, when vehicle *a* approaches vehicle *d*, as shown in Fig. 6, the transmission of the safety messages from vehicles *a* and *d* in the first frame will collide at vehicle *c*. In that case, vehicles *a* and *d* each detects the transmission collision and acquires another available time slot in the second frame. Details of the collision detection and time slot assignment techniques employed by VeMAC are explained in detail in [11].

Since the VeMAC protocol is based on TDMA, it is necessary for each node to be slot-synchronized, that is, to correctly determine the index of the current time slot in a frame. To perform this slot synchronization, a VeMAC implementation method recently presented in [12] proposes a slot synchronization procedure by using the 1 pulse per second (1PPS) signal provided by a Global Positioning System (GPS) receiver. The 1PPS signal is accurately aligned with the start of every GPS second, and hence is used as a common time reference by a microcontroller unit (MCU) which implements the VeMAC protocol at each node. Details of the VeMAC implementation method including the slot synchronization procedure are described in [12].

## Performance Evaluation

Due to the limitations of the current cellular network standards in supporting road safety applications, as discussed previously, this section focuses only on evaluating the performance of the VeMAC protocol in comparison with the IEEE 802.11p standard. The abilities of these two solutions to deliver periodic and event-driven safety messages are compared via

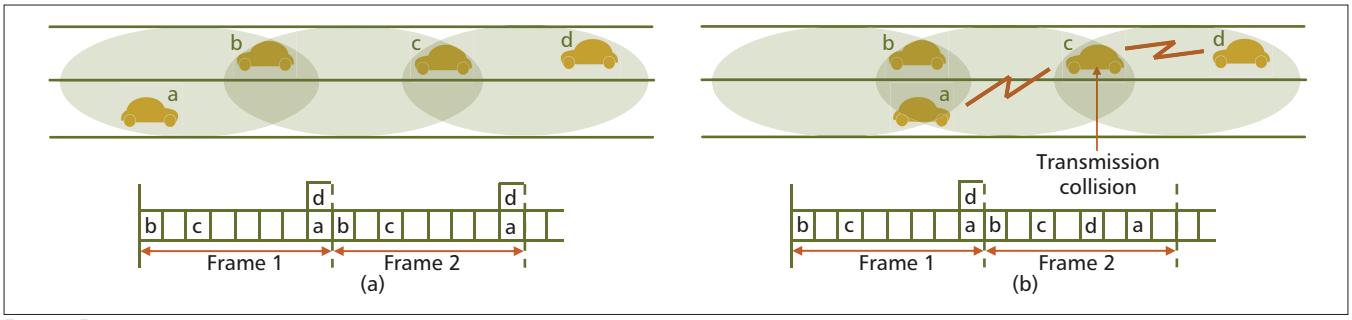


Figure 5. Illustration of the time slot assignment and transmission collision detection in VeMAC: a) time slot assignment for four nodes on a road (each frame consists of eight time slots); b) transmission collision due to node mobility, and detection of the collision by nodes a and d. A group of nodes is surrounded by an ellipse if and only if any two nodes in the group are within the communication range of each other, that is, can reach each other in one hop.

computer simulations, in terms of different performance metrics, including the safety message delivery delay and the percentage of safety messages successfully delivered by a node to all the nodes in its communication range [11]. The computer simulations are carried out by using network simulator ns-2 and microscopic vehicle traffic simulator VISSIM in three different simulation scenarios. The simulation scenarios consist of the roads around the University of Waterloo (UW), a segment of Highway 401 of the Canadian province of Ontario, and an urgent situation, in which a vehicle suddenly parks and creates a traffic bottleneck on the Highway 401 segment. Videos of the conducted simulations in all scenarios can be found at [13]. For each of the three simulation scenarios, the VISSIM generates a vehicle trace file (including the position and speed of each vehicle at the end of each simulation step), which is input to ns-2 in order to compare the performance of VeMAC and IEEE 802.11p in each scenario. For the VeMAC protocol, the periodic and event-driven safety messages are queued and served as explained in [11], while for the IEEE 802.11p standard, the EDCA scheme is employed, and the event-driven and periodic safety messages are mapped to AC_VO and AC_VI [14], respectively, that is, the highest and second-highest priority ACs as shown in Fig. 3. More details about the ns-2 and VISSIM simulation parameters are described in [11].

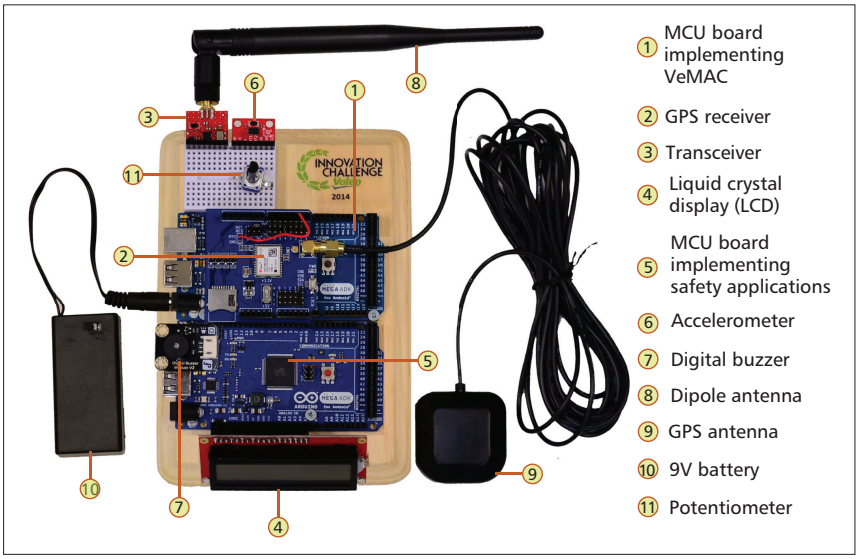


Figure 6. VeMAC prototype.

| Protocol | Scenario | | | | | |
|---|---|---|---|---|---|---|
| | Periodic messages | | | Event-driven messages | | |
| | Highway | Emergency | City | Highway | Emergency | City |
| VeMAC | 99.67 | 99.62 | 99.79 | 98.92 | 98.03 | 100 |
| IEEE 802.11p | 77.15 | 77.03 | 84.4 | 67.30 | 67.47 | 78.79 |

Table 1. Percentage of successfully delivered periodic and event-driven safety messages.

Table 1 shows the significant difference in the percentage of successfully delivered safety messages achieved by the VeMAC protocol and the IEEE 802.11p standard. In all the simulation scenarios, VeMAC allows a node to deliver almost all its broadcast periodic and event-driven safety messages to all the nodes in its communication range. On the other hand, IEEE 802.11p provides a very low percentage of successfully delivered safety messages, for example, around 67 percent for the event-driven messages in the highway scenario, which is unacceptable QoS support for the road safety applications in VANETs. The main reason for IEEE 802.11p having such degraded performance is the high probability of transmission collision of safety messages, as discussed previously and demonstrated via simulation results in [11]. Also, VeMAC can deliver the periodic and event-driven messages in around 50 ms in all the simulation scenarios [11], a value that is much lower than the 100 ms delay bound requirement for high-priority safety applications [1]. Furthermore, it is shown that VeMAC can achieve this high QoS support for safety applications, while providing fairness among all the nodes in broadcasting their safety messages, even in dense vehicle traffic scenarios [11].

The promising performance of the VeMAC protocol in supporting safety applications, as indicated from the computer simulation results, has motivated the implementation and experimental testing of VeMAC in real scenarios. Hence, a VeMAC prototype has been recently developed, as shown in Fig. 7, to evaluate the performance of VeMAC via different laboratory and on-road experiments [12]. The laboratory experiments are conducted mainly to test the VeMAC distributed time slot assignment, and to demonstrate the accuracy of the slot synchronization method proposed in [12], by using multiple units of the VeMAC prototype. Also, the prototype

is used to evaluate the interaction of the VeMAC protocol with an application layer for road safety, by implementing two safety applications: for collision avoidance in a road curve and emergency brake alert. The two applications are tested on the road in order to demonstrate the successful and timely delivery of safety messages provided by the VeMAC protocol. A video that presents all the VeMAC Lab experiments and on-road demonstrations can be found at [13].

## Conclusions and Future Work

This article elaborates on the feasibility of different wireless access technologies for supporting VANET road safety applications, including the IEEE 802.11p standard, the current cellular network standards, and the recently proposed VeMAC protocol. By identifying the limitations of the cellular network standards and demonstrating the poor performance of IEEE 802.11p via computer simulations in different scenarios, we highlight the promising potential of VeMAC for supporting the stringent QoS requirements of high priority safety applications in VANETs. However, the optimal values of VeMAC parameters, such as the slot duration and the number of time slots per frame, still need further investigation, since the choice of these parameter values can significantly affect the VeMAC performance in terms of safety message delivery delay, protocol fairness, and probability of transmission collision of a safety message. Also, combining ideas from the VeMAC protocol with the IEEE 802.11p standard (e.g., by adaptively switching between the two schemes), as well as dynamic spectrum access based on cognitive communications [15], may further improve the VANET ability to support safety and non-safety-related applications.

### Acknowledgments

We would like to sincerely thank Valeo, a well-known automotive supplier (www.valeo.com), for providing strong industrial support for us to accomplish this work. We would also like to thank Sailesh Bharati, a postdoctoral fellow at the University of Waterloo, for his great participation in preparing the contents of this article.

### References

[1] CAMP Vehicle Safety Commun. Consortium, "Vehicle Safety Communications Project Task 3 Final Report," tech. rep. DOT HS 809 859, Mar. 2005.
[2] K. Ota *et al.*, "MMCD: Cooperative Downloading for Highway VANETs," *IEEE Trans. Emerging Topics Comp.*, no. 1, pp. 1, PrePrints, doi:10.1109/TETC.2014.2371245.
[3] European Commission road safety statistics; http://ec.europa.eu/transport/road_safety/specialist/statistics/index_en.htm.
[4] L. Blincoe *et al.*, "The Economic and Societal Impact of Motor Vehicle Crashes, 2010," NHSTA tech. rep. DOT HS 812 013, May 2014; http://www-nrd.nhtsa.dot.gov/Pubs/812013.pdf.
[5] "U.S. Department of Transportation Issues Advance Notice of Proposed Rulemaking to Begin Implementation of Vehicle-to-Vehicle Communications Technology," NHTSA press releases, Aug. 2014; http://www.nhtsa.gov/About+NHTSA/Press+Releases/2014/NHTSA-issues-advanced-notice-of-proposed-rulemaking-on-V2V-communications.
[6] http://icsw.nhtsa.gov/safercar/old-ConnectedVehicles/pages/v2v.html.
[7] H. A. Omar and W. Zhuang, "Time Division Multiple Access for Vehicular Communications," *Springer Briefs in Computer Science*, 2014.
[8] IEEE Std 802.11p-2010, July 15, 2010, pp. 1–51.
[9] IEEE Std 1609.4-2010 (revision of IEEE Std 1609.4-2006), Feb. 2011, pp. 1–89.
[10] H. A. Omar, W. Zhuang, and L. Li, "VeMAC: A TDMA-Based MAC Protocol for Reliable Broadcast in VANETs," *IEEE Trans. Mobile Comp.*, vol. 12, no. 9, Sept. 2013, pp. 1724–36.
[11] H. A. Omar *et al.*, "Performance Evaluation of VeMAC Supporting Safety Applications in Vehicular Networks," *IEEE Trans. Emerging Topics Comp.*, vol. 1, no. 1, June 2013, pp. 69–83.
[12] H. A. Omar *et al.*, "Method, System and Apparatus for Enabling Vehicular Communications," patent application PCT/CA2015/051038, 2016.
[13] https://www.youtube.com/watch?v=BqCWmPebu_w.
[14] IEEE Std 802.11-2012 (revision of IEEE Std 802.11-2007), Mar. 2012, pp. 1–2793.
[15] T. Wang, L. Song, and Z. Han, "Coalitional Graph Games for Popular Content Distribution in Cognitive Radio VANETs," *IEEE Trans. Vehic. Tech.*, vol. 62, no. 8, Oct. 2013, pp. 4010–19.

### Biographies

HASSAN BOUBAKR OMAR received a Ph.D. degree in electrical and computer engineering from the University of Waterloo, Canada, in 2014, and an M.Sc. degree in engineering mathematics from Cairo University, Egypt, in 2009. Since 2014, he has been a postdoctoral fellow at the University of Waterloo, and he was a recipient of the best paper award from IEEE GLOBECOM in 2013. He is currently an assistant professor with the Engineering Mathematics and Physics Department, Cairo University. His current research interests include vehicular ad hoc networks, heterogeneous networks, and optimization.

NING LU received his B.Sc. and M.Sc. degrees from Tongji University, Shanghai, China, in 2007 and 2010, respectively. He recently received his Ph.D. degree from the University of Waterloo. All of his degrees are in electrical engineering. His current research focuses on wireless communications and networking, with special interest in vehicular communication systems. He was a co-recipient of the best paper award from IEEE GLOBECOM in 2014.

WEIHUA ZHUANG has been with the Electrical and Computer Engineering Department, University of Waterloo, since 1993, where she is currently a professor and Tier I Canada Research Chair in Wireless Communication Networks. She was Editor-in-Chief of *IEEE Transactions on Vehicular Technology* (2007–2013) and a recipient of the Premiers Research Excellence Award from the Ontario Government (2001). Her current research focuses on resource allocation and QoS provisioning in wireless networks and smart grid.