Performance Evaluation of VeMAC Supporting Safety Applications in Vehicular Networks

Hassan Aboubakr Omar, *Student Member, IEEE,* Weihua Zhuang, *Fellow, IEEE,*
Atef Abdrabou, *Member, IEEE,* and Li Li, *Member, IEEE*

Abstract—Vehicular ad hoc networking is an emerging paradigm which is expected to increase the public safety standards and enhance the safety level of drivers/passengers and pedestrians on road through a variety of applications. We have recently proposed VeMAC, a medium access control protocol which supports a reliable one-hop broadcast service necessary for high priority safety applications in VANETs [1], [2], [3]. This paper explains how the VeMAC protocol can deliver both periodic and event-driven safety messages in vehicular networks, and presents a detailed delivery delay analysis, including queueing and service delays, for both types of safety messages. The probability mass function of the service delay is first derived, then the D/G/1 and M/G/1 queueing systems are used to calculate the average queueing delay of the periodic and event-driven safety messages respectively. As well, a comparison between the VeMAC protocol and the IEEE 802.11p standard [4] is presented via extensive simulations using the network simulator ns-2 [5] and the microscopic vehicle traffic simulator VISSIM [6]. A real city scenario is considered and different performance metrics are evaluated, including the network goodput, protocol overhead, channel utilization, protocol fairness, probability of a transmission collision, and message delivery delay.

Index Terms—TDMA, medium access control, delay analysis, safety messages, and vehicular ad hoc networks.

1 Introduction

A vehicular ad-hoc network (VANET) is a special type of mobile ad-hoc networks, which consists of a set of vehicles, equipped with a communication device called on-board unit (OBU), and a set of stationary units along the road, referred to as road side units (RSUs). Each vehicle OBU has a wireless network interface which allows the vehicle to directly connect to other vehicles and RSUs within its communication range. Some RSUs can act as a gateway for connectivity to other communication networks, such as the Internet. Based on these vehicle-to-vehicle (V2V) and vehicle-to-RSU (V2R) communications, VANETs can support a wide variety of applications in road safety, passenger infotainment, and vehicle traffic optimization [8], [9]. The primary category of VANET applications is to enhance the public safety standards and provide a safer environment for people on road, which is the main reason that VANETs have received significant support from government, academia, and industrial organizations over the globe. The Vehicle Safety Communications (VSC) project [9] is established by seven car manufacturers (including GM, BMW, and Ford), in partnership with the United States Department of Transportation (USDoT), in order to estimate the potential benefits of VANET safety applications and define their communication requirements. In the VSC project, the VANET safety applications are classified into periodic and event-driven safety applications, based on the way that the corresponding safety messages are transmitted by each node (i.e., vehicle or RSU). The periodic safety applications (e.g., blind spot warning) require automatic transmission of safety messages by each node at regular time intervals, while the event-driven safety applications (e.g., pre-crash sensing [9]) require transmission of safety messages only in case of an event such as a hard brake, approaching an emergency vehicle, and dangerous road condition detection.

Most (if not all) of the safety applications, either periodic or event-driven, are based on one-hop broadcasting of safety messages to all the nodes within the communication range. For instance, an application such as the emergency electronic brake light [9] requires each vehicle to broadcast information about its position, speed, acceleration, etc., to all the vehicles within its one-hop neighbourhood. Similarly, for an application such as the traffic signal violation warning [9], an RSU near the traffic signal should broadcast to all the coming vehicles information related to the traffic light status and timing, road surface type, weather conditions, stopping position, and so on. Given that any inaccuracy in the broadcasted safety messages may result in serious consequences, such as vehicles damage or drivers injuries, it is necessary that a medium access control (MAC)

- *H. A. Omar and W. Zhuang are with the Center for Wireless Communications, Department of Electrical and Computer Engineering, University of Waterloo, 200 University Avenue West, Waterloo, Ontario, Canada, N2L 3G1.*
  E-mail: {h3omar,wzhuang}@uwaterloo.ca
- *A. Abdrabou is with the Department of Electrical Engineering, UAE University, Al-Ain, Abu Dhabi, UAE.*
  E-mail: atef.abdrabou@uaeu.ac.ae
- *L. Li is with the Communications Research Center, Ottawa, Ontario, Canada, K2H 8S2.*
  E-mail: li.li@crc.ca

This work is submitted in part to IEEE GlOBECOM 2013 [7].
This work was supported by a research grant from the Natural Science and Engineering Research Council (NSERC) of Canada.

protocol proposed for VANETs provides an efficient one-hop broadcast service to support the quality-of-service (QoS) requirements of the high priority safety applications. The IEEE 802.11p is a current standard proposed for MAC in VANETs [4]. However, as will be shown in this paper, the standard does not provide an efficient one-hop broadcast service. Different works have been done to evaluate/enhance the performance of the IEEE 802.11p standard [10], [11], [12]. For instance, in [10], [11], mathematical analysis is presented to model the IEEE 802.11p enhanced distributed channel access (EDCA) scheme for single-transceiver nodes, while in [12], an extension to the EDCA scheme is proposed to support the QoS requirements of the non-safety related VANET applications. On the other hand, the VeMAC is a time division multiple access (TDMA) protocol that we recently proposed for MAC in VANETs to support a reliable one-hop broadcast service [1], [2], [3]. The VeMAC is designed specifically for a VANET scenario over the physical layer of different standards, including IEEE 802.11p. The protocol supports multichannel operation over one control channel (CCH) and multiple service channels (SCHs) to be consistent with the seven dedicated short range communication (DSRC) channels specified by the Federal Communications Commission (FCC) for V2V and V2R communications.

The main objectives of this paper are to define how the VeMAC protocol serves the periodic and event-driven safety messages, to analyze the total delivery delay of both types of safety messages, which is a crucial QoS metric for VANET safety applications, and to present a detailed comparison between the VeMAC protocol and the IEEE 802.11p standard in a realistic city scenario, using various performance metrics. Different from the previous works [1], [2], [3], this paper defines two different VeMAC protocol data units (exchanged between two peer VeMAC entities) and describes the necessary techniques for each node to access multiple time slots in a time frame on the CCH. This flexibility in the number of time slots that a node is allowed to access on the CCH can be useful to support the safety applications with a large message size or stringent delay requirements. Based on the results in this paper, the VeMAC protocol parameters can be determined to satisfy the QoS requirements of periodic and event-driven safety applications (which is necessary for the hardware implementation and real testing of the protocol in the future).

The rest of the paper is organized as follows: Section 2 describes the system model and Section 3 discusses details of the VeMAC protocol to support safety applications. The delay analysis of periodic and event-driven safety messages is presented in Section 4 and the numerical results are given in Section 5. Section 6 compares the performances of the VeMAC protocol with that of the IEEE 802.11p standard via simulations in a square network and a realistic city scenario, and finally Section 7 concludes this study and suggests some further research topics.

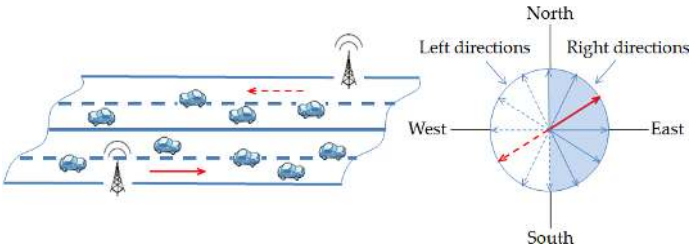


Fig. 1: Right and left directions of vehicle movement.

2 System Model

The VANET under consideration consists of a set of RSUs and a set of vehicles moving in opposite directions on two-way vehicle traffic roads, as shown in Fig. 1. A vehicle is said to be moving in a left (right) direction if it is currently heading to any direction from north/south to west (east). Based on this definition, as shown in Fig. 1, if two vehicles are moving in opposite directions on a two-way road, regardless of the orientation of the road, it is guaranteed that one vehicle is moving in a left direction while the other vehicle is moving in a right one. The vehicles and RSUs broadcast periodic and event-driven safety messages for the purpose of safety applications. A two-hop set (THS) is defined as a set of nodes in which each node can reach any other node in two hops at most. In this paper, the term 'packet' refers to a MAC layer protocol data unit, while the term 'message' refers to a MAC layer service data unit (MSDU), i.e., the unit of information arriving to the MAC layer entity from the layer above. The periodic safety messages broadcasted by different vehicles have the same (fixed) message size[1]. Similarly, the periodic safety messages broadcasted by an RSU have equal message size, which may differ from the size of the periodic messages broadcasted by another RSU depending on the application.

The VANET has one CCH and multiple SCHs. Each node has two transceivers, one is always tuned to the CCH, while the other switches among the SCHs. Although the VeMAC is a multichannel protocol, this paper focuses only on the operation of the VeMAC on the CCH, over which the high priority periodic and event-driven safety messages under consideration are transmitted. As shown in Fig. 2, the periodic and event-driven safety messages are mapped to two different queues, which are served independently by the VeMAC protocol, as described in details in Section 3. The time is partitioned to frames consisting of a constant number S of equal-duration time slots. Based on a given transmission rate determined by the physical layer, the VeMAC maximum transmission unit (MTU) is defined as the maximum amount of data (without the physical layer overhead) which can be transmitted in the duration of one time

1. A generic safety message format, called the Basic Safety Message (BSM), is specified in the SAE J2735 application layer standard [13] to be periodically broadcasted by vehicles. The BSM exploits the large overlap among the vehicle state information required by various V2V applications in order to avoid using application-specific messages and wasting the wireless network resources [14].

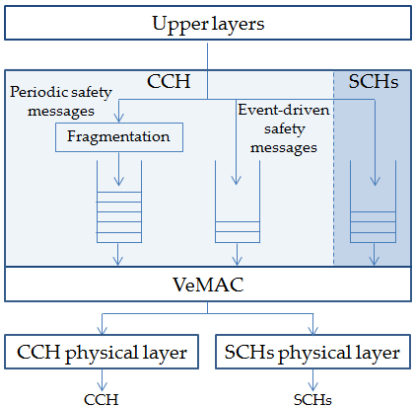


Fig. 2: Safety message queues.

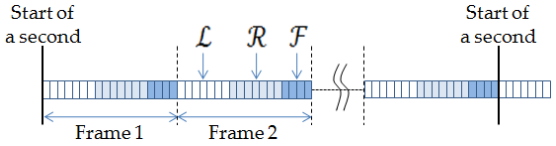


Fig. 3: Partitioning of each frame into $\mathcal{L}, \mathcal{R}$ and $\mathcal{F}$ sets.

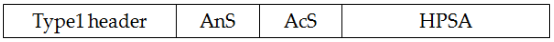
slot. The duration of a time slot is chosen such that the MTU is equal to the size of a periodic safety message broadcasted by a vehicle plus the maximum size of control information introduced by the VeMAC protocol. For RSUs, if the size of a periodic safety message plus the VeMAC control information exceeds the MTU, the message is fragmented to be transmitted as multiple VeMAC packets, as indicated in Fig. 2. This fragmentation is typical for applications such as curve speed warning and left turn assistant [9], in which the size of a periodic safety message broadcasted by an RSU is considerably larger than that of the periodic messages broadcasted by vehicles [9]. On the other hand, all the event-driven safety messages are assumed to be small enough to fit in a single VeMAC packet, without fragmentation. Each VeMAC packet carries at most one safety message and only one VeMAC packet can be transmitted per time slot. Each second contains an integer (fixed) number of frames, and each frame is partitioned into three sets of time slots: $\mathcal{L}$, $\mathcal{R}$, and $\mathcal{F}$, in that order, as shown in Fig. 3. The $\mathcal{F}$ set is reserved for RSUs, while the $\mathcal{L}$ and $\mathcal{R}$ sets are associated with vehicles moving in left and right directions respectively. Each time slot is identified by the index of the time slot within a frame (the index starts from 0 to $S-1$), and each node is identified by a unique MAC address and a set of short identifiers (IDs). Each node ID corresponds to a certain time slot that the node is accessing per frame on the CCH (more details in Section 3). For a certain node, x, the following two sets are defined: a) $N(x)$: the set of IDs of the one-hop neighbours of node x on the CCH, from which node x has received packets on the CCH in the previous S slots; b) $T(x)$: the set of time slots that node x must not use on the CCH in the next S time slots. The set, $T(x)$, is used by node x to determine which time slots it can access on the CCH without causing any hidden terminal problem. How each node x constructs and updates the set is discussed in Section 3 as follows.

3 VeMAC Protocol

3.1 VeMAC Basics

In the VeMAC protocol, in order to serve the two safety message queues in Fig. 2, each node must acquire at least one time slot per frame on the CCH. A time slot acquired by a certain node is referred to as a periodic or event-driven slot, according to the type of the safety message transmitted during this time slot. The number of periodic slots that the node acquires per frame, denoted by k_p, is constant and depends on the fixed size and arrival rate of the periodic safety messages. Similarly, the number of event-driven slots that the node can access per frame, denoted by k_e, is constant and depends on the average arrival rate of the event-driven safety messages. A node should use a unique node ID to access each of the k_p and k_e slots. Each node ID is chosen by the node at random, included in the header of each packet transmitted in the corresponding time slot, and changed if the node detects that its ID is already in use by another node [15]. The k_p and k_e values are chosen such as to satisfy the delay constraints of the periodic and event-driven safety messages based on the delay analysis in Section 4. Once a node acquires a periodic or event-driven slot, it keeps using the same slot in all subsequent frames unless there is no packet waiting for transmission in the corresponding queue or a transmission collision is detected. Two types of transmission collision can happen on the CCH [2]: access collision and merging collision. An access collision happens when two or more members of the same THS attempt to acquire the same available time slot. On the other hand, a merging collision happens when two or more nodes acquiring the same time slot become members of the same THS due to node activation or node mobility. In VANETs, merging collisions are more likely to occur among vehicles moving in opposite directions or between a vehicle and a stationary RSU since they approach each other with a much higher relative velocity as compared to vehicles moving in the same direction.

Two different types of VeMAC packets can be transmitted on the CCH, as shown in Fig. 4. A Type1 packet is divided into four main fields: Type1 header, announcement of services *(AnS)*, acceptance of services *(AcS)*, and high priority safety applications *(HPSA)*. The *HPSA* field is to include the periodic and event-driven safety messages, while the *AnS* and *AcS* fields are used to control the communications over the SHCs [2]. A Type2 packet does not contain any control information: it consists of an *HPSA* field and a short Type2 header (the difference between Type1 and Type2 headers will be discussed). Each node must transmit exactly one Type1 packet in each frame using one of its acquired periodic time slots, and if the node is accessing more than one time slot per frame, Type2 packets are transmitted over the rest of time slots. The transmission of one Type1 packet in each frame is mandatory since the information in the Type1 header, *AnS* and *AcS* fields, is necessary for other



(a) Type1 packet.

(b) Type2 packet.

Fig. 4: VeMAC packet types.

nodes to decide which time slots they can access on the SCHs [2] and CCH. On the other hand, the transmission of Type2 packets is to decrease the protocol overhead by removing all the control information which needs to be transmitted only once per frame. As the event-driven safety messages are always transmitted using Type2 packets (i.e., without control information and with a large *HPSA* field in the packet), fragmentation is not considered for this type of safety messages.

3.2 Accessing Slots on the CCH

For the purpose of time slot assignment on the CCH, in the header of each Type1 packet transmitted on the CCH, the transmitting node y should include set $N(y)$ and the time slot corresponding to each node ID in set $N(y)$. Note that, different node IDs in set $N(y)$ may correspond to a single one-hop neighbour of node y which is accessing multiple time slots per frame. The short IDs in set $N(y)$ serve to decrease the overhead as compared to including the MAC address of each one-hop neighbour in the header of each transmitted Type1 packet. The main difference between Type1 and Type2 headers is that the Type2 one is shorter as it does not contain the set $N(y)$ or the corresponding time slots. Suppose node x is just powered on and needs to acquire a time slot. It starts listening to the CCH for S successive time slots (not necessarily in the same frame). At the end of the S slots, node x can determine $N(x)$ and the time slot corresponding to each node ID in $N(x)$. In addition, since each one-hop neighbour w of node x announces (in the header of its transmitted Type1 packet) the set $N(w)$ and the time slot corresponding to each node ID in $N(w)$, node x can determine all the time slots used by each of its two-hop neighbours. Accordingly, node x sets $T(x)$ to the set of time slots used by all nodes within its two-hop neighbourhood. Then, sets $N(x)$ and $T(x)$ are updated by node x at the end of each time slot (always based on the packets received in the previous S slots).

Given $T(x)$, node x determines the set of accessible time slots, $A(x)$, (to be discussed) and then attempts to acquire a time slot by randomly accessing any time slot in $A(x)$, say time slot k. If no other node in the two-hop neighbourhood of node x simultaneously attempts to acquire time slot k, then no access collision happens. In this case, the attempt of node x is successful and each one-hop neighbour w of node x adds node x's ID (denoted by ID_x) to set $N(w)$ and records that time slot k corresponds to ID_x. On the other hand, if at least one node within the two-hop neighbourhood of node x accesses time slot k, then all the transmissions in the slot fail and time slot k is not acquired by any of the contending nodes. Node x will determine whether or not its attempt was successful by observing the $S-1$ time slots following k. The attempt of node x is considered successful iff the Type1 packets received from each node w, with $ID_w \in N(x)$, indicate that $ID_x \in N(w)$. Otherwise, node x re-accesses one of the time slots in $A(x)$ until it successfully acquires a time slot. Once node x acquires a time slot, it keeps using the same slot in all subsequent frames unless a merging collision happens. Similar to an access collision, a merging collision is detected by node x as soon as it receives a Type1 packet from a node w, with $ID_w \in N(x)$, indicating that $ID_x \notin N(w)$. Upon detection of a merging collision, each colliding node should release its time slot and acquire a new one using the same procedure. At the end of each time slot, the collision detection by a certain node x should be done before updating the set $N(x)$ in order to prevent the nodes from unnecessarily releasing their time slots when they just enter the communication range of each other [2]. In order to acquire more than one time slot per frame, node x employs the same procedure using a unique node ID for accessing each extra time slot.

When a node, x, is attempting to acquire a time slot, a parameter called the split up parameter, denoted by τ, determines how node x accesses the time slots belonging to the $\mathcal{L}$, $\mathcal{R}$, and $\mathcal{F}$ sets. Consider that node x is moving in one of the right directions. Initially, node x limits set $A(x)$ to the available time slots associated with the right directions, i.e., $A(x) = \overline{T(x)} \cap \mathcal{R}$. If after τ frames node x cannot acquire a time slot, then node x augments $A(x)$ by adding the time slots associated with the opposite direction, i.e., $A(x) = \overline{T(x)} \cap (\mathcal{R} \cup \mathcal{L})$. If, after τ more frames, node x still cannot acquire a time slot, node x will start to access any available time slot, i.e., $A(x) = \overline{T(x)}$. The same procedure applies for a vehicle moving in a left direction by replacing $\mathcal{R}$ with $\mathcal{L}$. Similarly, if node x is an RSU, for the first τ frames $A(x) = \overline{T(x)} \cap \mathcal{F}$, and then $A(x) = \overline{T(x)}$. Note that, when $\tau = \infty$, regardless of the number of access collisions that node x has encountered to acquire a time slot, it can only access the time slots reserved for its moving direction (i.e., in the $\mathcal{R}$ set). On the other extreme, when $\tau = 0$, node x can access any available time slot on the CCH even if it does not experience any access collision. The choice of the τ value can significantly affect the network throughput and the rates of access collisions and merging collisions [2], [3]. In the analysis in Section 4, the effect of the τ value on the delay of periodic and event-driven safety messages is investigated for the two extreme cases $\tau = 0$ and $\tau = \infty$.

4 Delay Analysis

The total delay that a safety message experiences on the CCH before reaching all the one-hop neighbours consists of five components: 1) *upper layers delay* from the time that a safety message is generated at the application layer until it is assigned to one of the two queues in Fig. 2, including the fragmentation time of periodic

safety messages; 2) *queueing delay* between the time that a safety message (or a fragment of a safety message) is assigned to one of the queues in Fig. 2 and the time that it becomes the head of line (HOL); 3) *access delay* from the time that a safety message (or a fragment of a safety message) becomes the HOL until the start of its transmission. This delay is mainly the time spent by the transmitting node waiting for one of its acquired periodic or event-driven time slots; 4) *transmission duration* of a safety packet; 5) *propagation delay* until the safety packet completely reaches the farthest one-hop neighbour. The *upper layers delay* and *propagation delay* are not considered in the following analysis since they are negligible as compared to the other delay components. The *transmission duration* of any safety packet is assumed to be equal to the duration of one time slot. Note that, the duration of one time slot represents the maximum *transmission duration* which can be experienced by a safety packet on the CCH. However, the difference between the maximum and actual *transmission durations* (fraction of a time slot) is negligible as compared to the *queueing delay* and *access delay* (multiple time slots). The sum of the *access delay* and *transmission duration* is referred to as the *service delay*. To simplify the analysis of the *service delay* and *queueing delay*, denoted by W_s and W_q respectively, we assume that a node releases its periodic or event-driven time slot(s) and acquires a new one(s) after the transmission of each periodic or event-driven safety packet respectively. This assumption guarantees that the *service delays* of the successive periodic and event-driven safety messages assigned to the two queues in Fig. 2 form two sequences of independent and identically distributed random variables, which is a necessary condition for the application of the D/G/1 and M/G/1 queuing systems in Subsection 4.2. The assumption is reasonable in scenarios with high rates of access collisions and merging collisions, where the nodes frequently release their time slots and acquire new ones. The total delay, denoted by W, is the sum of W_s and W_q, and all delays are represented in the unit of a time slot. For any discrete random variable X, the probability mass function (PMF) and the cumulative distribution function (CDF) are denoted by f_X and F_X respectively, while the first and second moments are denoted by $\overline{X}$ and $\overline{X^2}$ respectively. If random variable X takes only non-negative integer values, its probability generating function (PGF) is denoted by $G_X(z) = \overline{z^X} = \sum_x f_X(x) z^x$, while $G'_X(z)$ denotes $\frac{d}{dz} G_X(z)$. The *service delay* and *queueing delay* are considered separately in Subsections 4.1 and 4.2 in the following. The accuracy of the analysis in this section under the simplified assumptions has been studied via MATLAB simulations in [7].

4.1 Service Delay

Since the VeMAC protocol serves the two queues in Fig. 2 independently using the k_p and k_e time slots, the PMF f_{W_s} is similar for both queues and differs only due to the difference between the k_p and k_e values. Hence, the PMF f_{W_s} is derived in a generic way (i.e., irrespective of the type of the transmitted safety message) given that the transmitting node is accessing k time slots per frame. For the periodic and event-driven safety messages, the PMF f_{W_s} can be calculated just by replacing k in the generic f_{W_s} with k_p and k_e respectively. Let random variable J denote the index of the time slot at the start of which a safety message becomes the HOL. Note that, since the transmission delay is equal to 1, if the inter-arrival time of periodic safety messages is an integer value, it is guaranteed that a periodic message becomes the HOL at the start of a time slot. On the other hand, due to random arrivals of event-driven safety messages with non-integer inter-arrival times, it is possible that, when the queue is empty, an arriving event-driven message becomes the HOL within the duration of a certain time slot. In this case, we neglect a fraction of time slot in the calculation of the *service delay* and assume that the event-driven message becomes the HOL at the start of the next slot. Hence, the *service delay* W_s can take only integer values ranging from 1 to $S-k+1$. The calculation of $f_{W_s}(i), i = 1, ..., S-k+1$, is considered separately for the two extreme values of the split up parameter, $\tau = 0$ and $\tau = \infty$.

4.1.1 $\tau = 0$

In this case, if a safety message becomes the HOL at the start of time slot j, the transmitting node can be accessing any k of the S time slots following (and including) time slot j with equal probabilities. Hence,

$$p(W_s = i | J = j) = \frac{C_{k-1}^{S-i}}{C_k^S},$$
$$1 \leq k \leq S, 1 \leq i \leq S-k+1, 0 \leq j \leq S-1$$

where $C_k^n = \frac{n!}{(n-k)!k!}$. The denominator is the number of ways that the transmitting node can access k time slots among the S time slots following (and including) time slot j, while the numerator is the number of ways that one of the k time slots that the node is accessing is the i^{th} time slot starting from j, denoted by $j_a = (j+i-1) \text{mod} S$, and the remaining $k-1$ time slots are among the $S-i$ time slots following time slot j_a. In other words, the numerator is the number of ways that the node is accessing the i^{th} time slot starting from j but not any of the $i-1$ time slots following (and including) time slot j. Note that, with $\tau = 0$, the probability $p(W_s = i | J = j)$ is independent of the value of j since the transmitting node is allowed to access all the available time slots in a frame with equal probabilities. Hence,

$$\begin{aligned} f_{W_s}(i) &= \sum_{j=0}^{S-1} p(W_s = i | J = j) \times f_J(j) \\ &= \sum_{j=0}^{S-1} \frac{C_{k-1}^{S-i}}{C_k^S} \times f_J(j) = \frac{C_{k-1}^{S-i}}{C_k^S}, \end{aligned}$$
$$1 \leq i \leq S-k+1, 1 \leq k \leq S.$$

4.1.2 $\tau = \infty$

Consider that a node is moving in one of the left directions. When a safety message becomes the HOL at the start of time slot j, the transmitting node can be accessing any k time slots in set $\mathcal{L}$ with equal probabilities. There is no probability that the node accesses any of the time slots in sets $\mathcal{R}$ and $\mathcal{F}$. Hence, unlike the $\tau = 0$ case, the probability $p(W_s = i|J = j)$ depends on the value of j.

a) For $|\mathcal{L}| \leq j \leq S-1$, we have

$$p(W_s = i|J = j) = \begin{cases} \frac{C_{k-1}^{|\mathcal{L}|-[i-(S-j)]}}{C_k^{|\mathcal{L}|}}, & S-j+1 \leq i \leq \\ & S-j+1+|\mathcal{L}|-k, \\ & 1 \leq k \leq |\mathcal{L}|, \\ 0, & \text{elsewhere.} \end{cases}$$

The denominator represents the total number of ways that the node can access k slots among the $|\mathcal{L}|$ time slots, while the numerator represents the number of ways which result in W_s equal to i. Note that, the smallest possible value of W_s is $S-j+1$, since $j \in \mathcal{R} \cup \mathcal{F}$ while the node cannot access any time slot in set $\mathcal{R} \cup \mathcal{F}$.

b) For $0 \leq j \leq |\mathcal{L}|-1$, we have the following two cases

- If $j < k$, we have $W_s \leq |\mathcal{L}|-k+1$, since at least one of the k time slots that the node is accessing is among the next $|\mathcal{L}|-j$ time slots starting from time slot j. Then

$$p(W_s = i|J = j) = \begin{cases} \frac{C_{k-1}^{|\mathcal{L}|-i}}{C_k^{|\mathcal{L}|}}, & 1 \leq i \leq |\mathcal{L}|-k+1, \\ 0, & \text{elsewhere.} \end{cases}$$

- If $j \geq k$, there is a probability that the k time slots that the node is accessing are all before time slot j, which results in W_s taking values between $S-j+1$ and $S-k+1$. Hence

$$p(W_s = i|J = j) = \begin{cases} \frac{C_{k-1}^{|\mathcal{L}|-i}}{C_k^{|\mathcal{L}|}}, & 1 \leq i \leq |\mathcal{L}|-j, \\ \frac{C_{k-1}^{S-i}}{C_k^{|\mathcal{L}|}}, & S-j+1 \leq i \leq S-k+1, \\ 0, & \text{elsewhere.} \end{cases}$$

Given $p(W_s = i|J = j)$ for all $0 \leq j \leq S-1$, we have

$$f_{W_s}(i) = \sum_{j=0}^{S-1} p(W_s = i|J = j) \times f_J(j),$$
$$1 \leq i \leq S-k+1, 1 \leq k \leq |\mathcal{L}|.$$

For a node moving in a left direction, we assume that

$$f_J(j) = \begin{cases} \frac{1}{|\mathcal{L}|}, & 0 \leq j \leq |\mathcal{L}|-1, \\ 0, & \text{elsewhere.} \end{cases}$$

This assumption means that, first, a safety message cannot become the HOL at the start of time slots in set $\mathcal{R} \cup \mathcal{F}$ and, second, a safety message becomes the HOL at the start of time slots in set $\mathcal{L}$ equally likely. Note that, although the transmitting node is not allowed to access time slots in set $\mathcal{R} \cup \mathcal{F}$, a safety message still can become the HOL at the start of a time slot belonging to this set, e.g., when a message arrives at the start of a time slot $j \in \mathcal{R} \cup \mathcal{F}$ and finds the queue empty. The same procedure in this subsubsection can be used to derive f_{W_s} for a node moving in a right direction or for an RSU.

4.2 Queueing Delay

Although the PMF of the *service delay* is the same for periodic and event-driven safety messages, their *queueing delays* are different due to different arrival patterns for the two different types of safety messages.

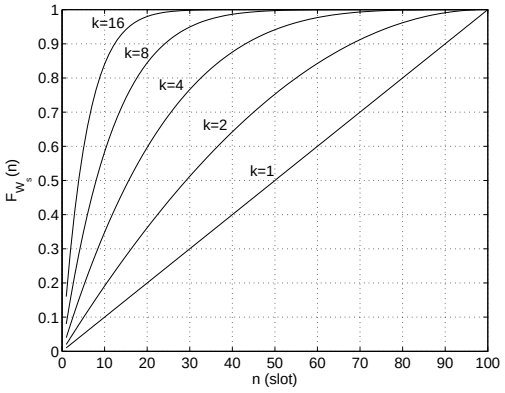
4.2.1 Event-driven Safety Messages

As mentioned in Section 1, the event-driven safety messages are triggered by certain events such as a sudden brake, road feature notification, approaching an emergency vehicle, etc. Given the variety of such events, it is reasonable to assume that their arrival process has independent and stationary increments, with no group arrivals. That is, the numbers of events occurring in disjoint time intervals are independent, the PMF of the number of events occurring in a time interval only depends on the length of the interval, and there is no simultaneous arrival of events. Based on these properties, the arrival process of the event-driven safety messages can be modeled by a Poisson process with rate λ message/slot. Hence, the event-driven safety message queue in Fig. 2 is an M/G/1 queue with the *service delay* distribution f_{W_s} as derived in Subsection 4.1. Consequently, provided that $\overline{W_s} < \frac{1}{\lambda}$, which is the necessary and sufficient condition for stability of the event-driven safety message queue [16], by applying the P-K formula [17], we have

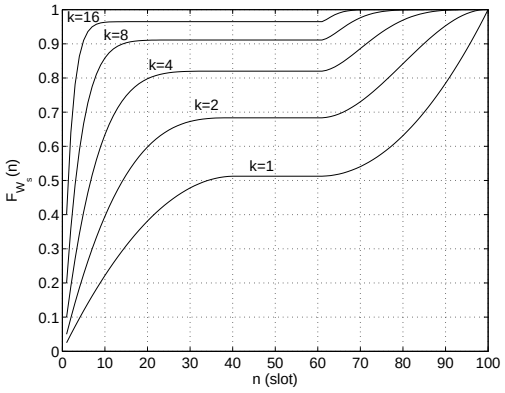
$$\overline{W_q} = \frac{\lambda \overline{W_s}^2}{2(1-\lambda \overline{W_s})}.$$

4.2.2 Periodic Safety Messages

Based on the assumption of fixed-size periodic safety messages, the number of fragments of a periodic safety message is assumed to be fixed for a given node. If n_f denotes the number of fragments of a periodic safety message for a certain node, the arrival of each periodic safety message results in a simultaneous arrival of n_f fragments in the periodic safety message queue in Fig. 2. Consequently, this queue can be modeled as a D/G/1 queue with fixed-size batch arrivals. Hence, the *queueing delay* that a tagged fragment of a periodic safety message experiences consists of two components: the delay since the batch (to which the tagged fragment belongs) enters the queue until the first fragment of the batch becomes the HOL, plus the *service delay* of all the fragments queued before the tagged fragment within the batch. The two components of the *queueing delay* are independent and denoted by W_{q_1} and W_{q_2} respectively. Let integer N denote the inter-arrival time of periodic safety messages, i.e., the batch inter-arrival time. The PGF of the *service*

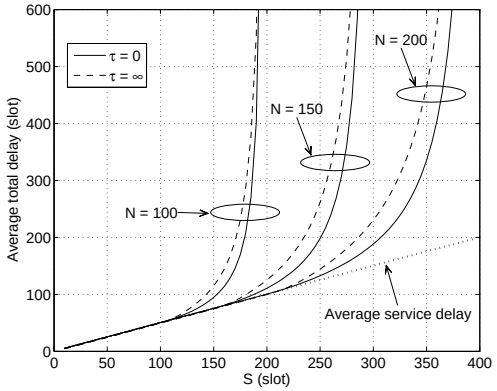


(a) Split up parameter $\tau = 0$.

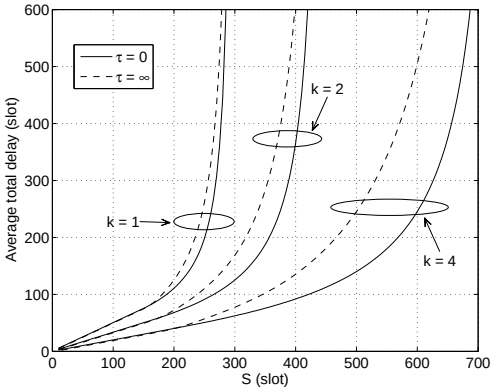


(b) Split up parameter $\tau = \infty$.

Fig. 5: The CDF of the *service delay*, F_{W_s}, for a node moving in a left direction with 100 time slots per frame and 40 time slots associated with the left direction, i.e., $S = 100$ and $|\mathcal{L}| = 40$.



(a) Number of time slots accessed per frame $k = 1$.



(b) Periodic message inter-arrival time $N = 150$.

Fig. 6: The average total delay, $\overline{W}$, of a single-fragment periodic message ($n_f = 1$) for a node moving in a left direction with 40 percent of the time slots associated with the left direction, i.e., $|\mathcal{L}| = 0.4S$.

delay of one batch, denoted by $W_b(z)$, is

$$G_{W_b}(z) = \big(G_{W_s}(z)\big)^{n_f}.$$

Hence, provided that $\overline{W_b} = G'_{W_b}(1) < N$, which is the necessary and sufficient condition for stability of the periodic safety message queue [16], the PGF of W_{q_1} can be calculated as follows [18], [19]

$$G_{W_{q_1}}(z) = \frac{\xi\big[\prod_{i=1}^{N-1}(z - z_i)\big](z-1)}{z^N - G_{W_b}(z)}$$

where

$$\xi = \lim_{z\to 1} \frac{z^N - G_{W_b}(z)}{\big[\prod_{i=1}^{N-1}(z - z_i)\big](z-1)}$$

and complex numbers $z_1, z_2, \ldots, z_{N-1}$ are the roots of the function $z^N - G_{W_b}(z)$, which are on or inside the unit circle but not equal to 1. The PGF, $G_{W_{q_2}}(z)$, can be calculated by noting that $W_{q_2} = \sum_{i=0}^{I} W_s$, where I is a random variable representing the number of fragments queued before the tagged fragment within the batch. Since the tagged fragment can be any fragment within the batch with equal probabilities, $f_I(i) = \frac{1}{n_f}, i = 0, \ldots, n_f - 1$, and $G_I(z) = \frac{1}{n_f}\sum_{i=0}^{n_f-1} z^i$. Hence, by using the law of total expectation,

$$G_{W_{q_2}}(z) = G_I(G_{W_s}(z)).$$

Consequently,

$$G_{W_q}(z) = G_{W_{q_1}}(z) \times G_{W_{q_2}}(z)$$
$$\overline{W_q} = G'_{W_q}(1).$$

5 Analytical Results

We use MATLAB R2011b and the Symbolic Math Toolbox V5.7 for the calculation of the average delays as described in Section 4. Figs. 5a and 5b show F_{W_s} for a node moving in a left direction with $\tau = 0$ and $\tau = \infty$ respectively. The main difference between the two cases is that, when $\tau = \infty$, $F_{W_s}(n)$ remains constant for a certain range of n. With $\tau = \infty$, the node can only access time slots in set $\mathcal{L}$. As a result, there should be a range of n where $f_{W_s}(n) = 0$. For instance, if $k = 2, S = 100$, and $|\mathcal{L}| = 40$, $f_{W_s}(n) = 0, \forall n \in \{40, \ldots, 61\}$.

Fig. 6a shows the average total delay $\overline{W}$ of a periodic safety message with $n_f = 1$ (a typical case for vehicles) for a node moving in a left direction with $k = 1$. Both

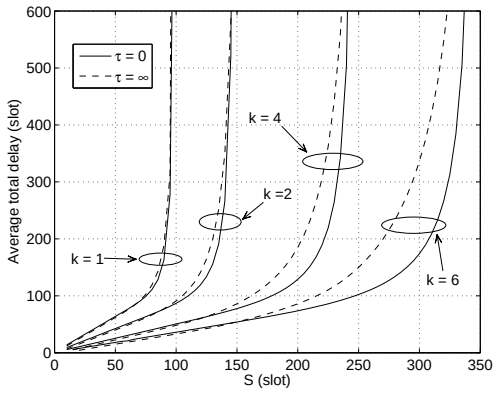


Fig. 7: The average total delay, $\overline{W}$, of a fragment of a four-fragment periodic message ($n_f = 4$) for an RSU with 200 time slots message inter-arrival time and 40 percent of the time slots associated with RSUs, i.e., $N = 200$ and $|\mathcal{F}| = 0.4S$.

$\tau = 0$ and $\tau = \infty$ cases are plotted in Fig. 6a for various N values. Although the $\tau = 0$ and $\tau = \infty$ cases have different F_{W_s} (in Figs. 5a and 5b), when $k = 1$, both τ values result in the same $\overline{W_s}$, which is represented by the straight line in Fig. 6a. As shown in Fig. 6a, if $S \leq N$, $\overline{W}$ is the same as $\overline{W_s}$ since each safety message is served before the next one arrives, i.e., $\overline{W_q} = 0$. When $S > N$, the queueing component W_q is added to the total delay W, and the value of $\overline{W}$ continues to increase with S and approaches ∞ when S tends to the instability value S^* at $\overline{W_s} = N$. Eventually, the value of S^* increases with the number of time slots, k, that the node is allowed to access per frame. To illustrate the effect of k on the total delay W, Fig. 6b shows $\overline{W}$ for $N = 150$ and different k values. As shown in Fig. 6b, while a frame duration $S = 300$ results in instability for the $k = 1$ case, when k is increased to 2, the value of $\overline{W}$ remains below 200 slots for both $\tau = 0$ and $\tau = \infty$. To consider a case of large-size periodic safety messages (typically for RSUs), Fig. 7 shows the total delay $\overline{W}$ of a fragment of a periodic safety message with $n_f = 4$ for an RSU when $N = 200$ and $|\mathcal{F}| = 0.4S$. The different components of $\overline{W}$ for such multi-fragment periodic safety messages, i.e., $\overline{W_s}, \overline{W_{q_1}}$, and $\overline{W_{q_2}}$, are verified via MATLAB simulations in [7].

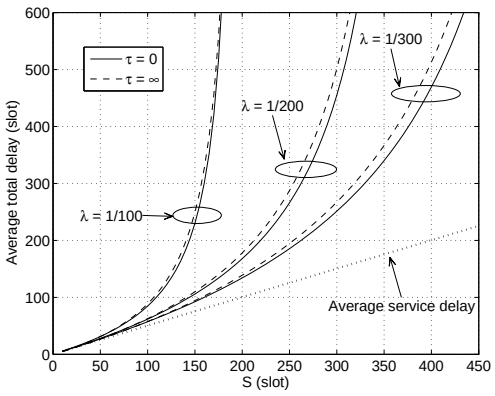
Fig. 8a illustrates the average total delay $\overline{W}$ of an event-driven safety message for a node moving in a left direction with $k = 1$. Unlike the periodic safety messages case in Fig. 6a, due to the Poisson arrival of event-driven safety messages, even if $S \leq \frac{1}{\lambda}$, the queueing delay $W_q > 0$ and $\overline{W} > \overline{W_s}$. The effect of k on the total delay of event-driven safety messages is shown in Fig. 8b for $\lambda = \frac{1}{200}$ message/slot.

Based on the numerical results in this section, it is observed that the delay performance of the VeMAC with $\tau = 0$ is better than $\tau = \infty$ for both periodic and event-driven safety messages, especially for large k and N, and small λ values. If the size of the periodic safety messages broadcasted by vehicles is 150 bytes, a VeMAC MTU of 675 bytes is suitable to include one periodic safety message and all the VeMAC control information which should be transmitted on the CCH. For a transmission rate of 18 Mbps, which is one of the rates supported by the IEEE 802.11p OFDM physical layer for the 5 GHz band, the VeMAC MTU transmission time is 0.3 ms. By including guard periods and considering the physical layer overhead, a slot duration of 0.35 ms can be assumed. Given this slot duration, for the periodic safety messages of vehicles, if $N = 200$ slots $= 70$ ms, and each vehicle is allowed to access one periodic time slot per frame, then from Fig. 6a, a frame duration $S = 300$ results in an average total delay around 185 slots (65 ms) for the $\tau = 0$ case. Similarly, for the event-driven safety messages in Fig. 8a, if $\lambda = \frac{1}{300}$ message/slot $= 9.5$ message/s, and if the transmitting node is allowed to access only one event-driven time slot per frame, a frame duration of 300 slots results in an average delay around 250 slots (88 ms). Note that, the frame duration S represents the maximum number of time slots available for any THS in the network. For instance, if $S = 300$ slots and the transmission range is 200 m (corresponding to the maximum length of 400 m occupied by a THS on a road segment), the total number of time slots available for all the nodes on a road segment of any 400 m is equal to 300 slots. The results in this section help to determine the VeMAC parameters, such as $\tau, k_p, k_e,$ and$S$, used for the comparison with the IEEE 802.11p standard as follows.

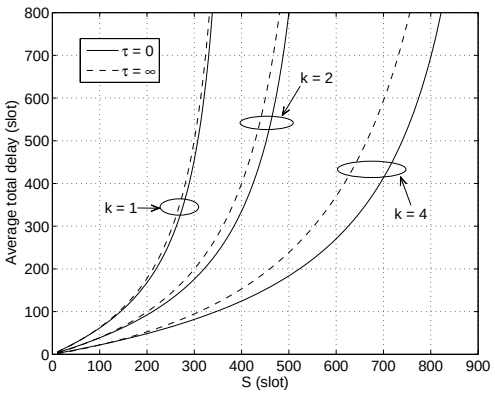
6 Simulation Results

Computer simulations are conducted using the network simulator ns-2 [5] to evaluate the performance of the VeMAC protocol in comparison with the IEEE 802.11p standard in broadcasting the safety messages. Periodic safety messages are generated continuously, while event-driven safety messages are generated according to an exponential ON/OFF model (i.e., the ON and OFF periods are exponentially distributed) at each node in the simulations. For the VeMAC protocol, the periodic and event-driven safety messages are queued and served as specified in Sections 2 and 3 [2]. On the other hand, for the IEEE 802.11p, we have employed the EDCA scheme, which assigns any MSDU to one of four different access categories (ACs) [21]. The event-driven and periodic safety messages are respectively assigned to the highest and second-highest priority ACs, i.e., AC_VO and AC_VI [4]. Two simulation scenarios are considered: a square network and a realistic city scenario. For both scenarios, the ns-2 parameters are summarized in Table 1. The IEEE 802.11p parameter values in Table 1 are as specified by the IEEE 802.11p OFDM physical layer for the 5 GHz band [4], [21]. The carrier frequency of 5.89 GHz represents the center frequency of the DSRC channel 178 (the CCH), and the transmission power of 33 dBm is the maximum power allowed on this channel for private OBUs and RSUs as in the ASTM E2213 standard

2. Our ns-2 implementation of the VeMAC protocol, including the periodic and event-driven message queues, will be made available online [20] to interested researchers.



(a) Number of time slots accessed per frame $k = 1$.



(b) Event-driven message average arrival rate $\lambda = \frac{1}{200}$ message/slot.

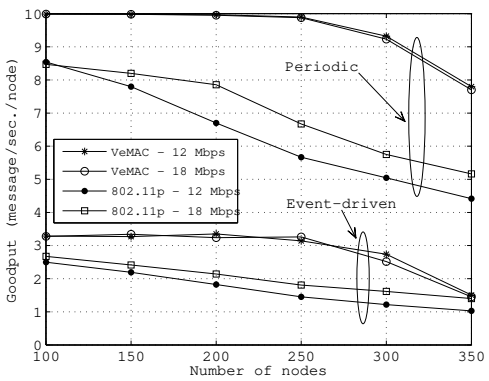
Fig. 8: The average total delay, $\overline{W}$, of an event-driven safety message for a node moving in a left direction with 40 percent of the time slots associated with the left direction, i.e., $|\mathcal{L}| = 0.4S$.

TABLE 1: ns-2 simulation parameters

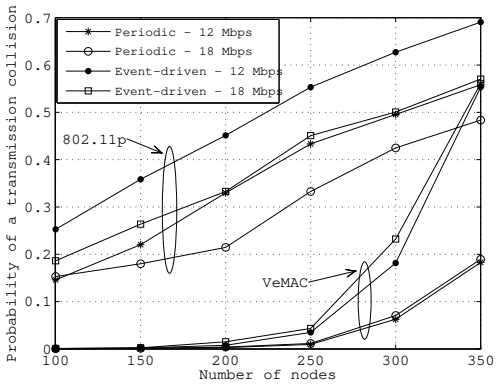
Periodic messages		**Event-driven messages**				**Physical layer**			
Parameter	***Value***	***Parameter***	***Value***	***Parameter***	***Value***	***Parameter***	***Value***	***Parameter***	***Value***
Size	150 bytes	Size	450 bytes	Average OFF time	2 s	RXThresh	1.45683×10^{-09} w	CSThresh	8.19468×10^{-10} w
Arrival rate	10 message/s	Average ON time	1 s	Arrival rate during ON time	10 message/s	Carrier frequency	5.89 GHz	Transmission power	33 dBm
						CPThresh	10	Transmission rate	12-18 Mbps
						Antenna	Omni-directional	Channel model	free space
Higher layer protocols		**VeMAC**				**IEEE 802.11p**			
Layer	***Protocol***	***Parameter***	***Value***	***Parameter***	***Value***	***Parameter***	***Value***	***Parameter***	***Value***
Transport layer	UDP	S	275 slots	Slot duration	0.35 ms	aSlotTime	13 μs	SIFS	32 μs
Network layer	dumb agent	k_p	1	k_e	1	AC_VO CW size	3	AC_VO AIFS	58 μs
		τ	0	MTU	450-675 bytes	AC_VI CW size	7	AC_VI AIFS	71 μs
		#bits of a node ID	9	#bits of a slot index	9	Preamble length	32 μs	PLCP header length	8 μs
Simulation time: 1 min. for square network and 5 min. for city						FCS	4 bytes	Header length	32 bytes

[22]. Given these values of the carrier frequency and the transmission power, the receiving threshold (RxThresh) and the carrier sensing threshold (CSThresh) in Table 1 result in a communication range of 150 m and a carrier sensing range of 200 m for free space propagation. The capture threshold (CPThresh) is the minimum ratio between the powers of two received signals required for the receiver to capture the signal with the higher power and discard the one with the lower power. The dumb agent used in the network layer just passes the data from the transport layer to the MAC layer while sending, and vice versa while receiving (since all the safety messages under consideration are single-hop broadcast messages).

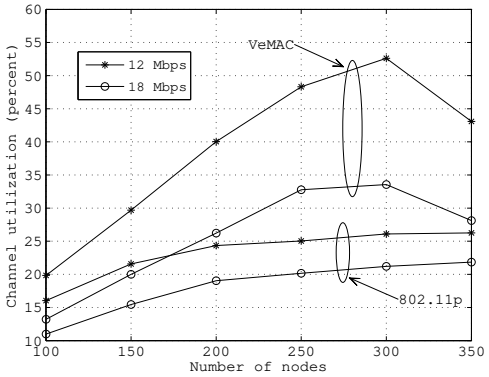
In addition to the total delay (as defined in Section 4), the following performance metrics are considered: 1) goodput which is the average rate of safety messages which are successfully delivered to all the one-hop neighbours; 2) channel utilization defined as the percentage of time that the channel is used for successful transmission of payload data (a transmission is considered successful only if it is correctly received by all the one-hop neighbours); 3) overhead defined as the percentage of control information relative to the total information transmitted on the channel; 4) probability of a transmission collision, i.e., the probability that a transmitted safety message experiences a collision at one or more one-hop neighbours; and 5) fairness indicator. A metric is calculated for each node x, denoted by $r(x)$, which is the ratio of the number of safety messages *transmitted* by node x to the total number of safety messages *transmitted* by all nodes. The fairness indicator is the deviation (in percentage) of $r(x)$ from a fair share, $f(x)$, that equals the total number of safety messages *generated* at node x normalized by the total number of safety



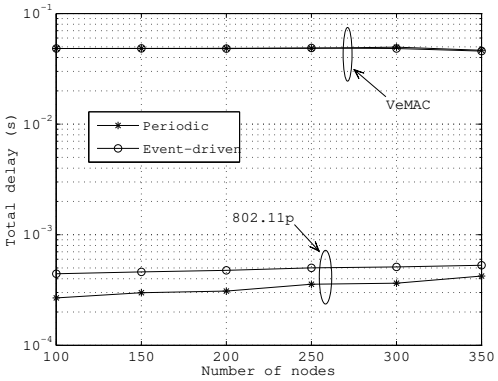
(a) Goodput.



(b) Probability of a transmission collision.



(c) Channel utilization.



(d) Average delay for a transmission rate of 12 Mbps.

Fig. 9: Simulation results for the square network.

messages *generated* at all nodes. That is, the fairness indicator for a node x is equal to $\mid \frac{r(x)-f(x)}{f(x)} \mid \times 100$. All the performance metrics, except the overhead and the channel utilization, are calculated separately for the periodic and event-driven safety messages.

6.1 Square Network

The first scenario under consideration is a set of stationary nodes uniformly distributed in a square network with side length of 500 m. Fig. 9a shows the periodic and event-driven message goodputs of the VeMAC and the IEEE 802.11p protocols using two different physical layer transmission rates. Note that, based on the parameters in Table 1, the average rates of periodic and event-driven safety messages generated at each node are 10 messages/s and 3.3 messages/s respectively. As shown in Fig. 9a, the VeMAC outperforms the IEEE 802.11p for all the node densities and transmission rates under consideration. For instance, when the number of nodes in the network is 250, the VeMAC protocol can successfully deliver almost all the periodic and event-driven safety messages to all the one-hop neighbours, while the IEEE 802.11p fails to deliver around 50% of the event-driven messages and more than 40% of the periodic messages using a transmission rate of 12 Mbps. This outperforming of the VeMAC protocol in terms of safety message goodput is due to its ability to reduce the probability of a transmission collision as compared with the IEEE 802.11p standard. As shown in Fig. 9b, there is a significant difference between the probability of a transmission collision achieved by the two protocols. For the VeMAC protocol, the probability of a transmission collision of an event-driven safety packet is higher than that of a periodic safety packet, especially at high node densities. The reason is that, when the event-driven safety message queue is empty, a node releases its event-driven time slot (i.e., no information is transmitted in the slot) and re-acquires a new one when the next event-driven safety message is generated. This technique relatively increases the rate of access collisions of the event-driven safety packets, as compared with that of the periodic ones. Note that, if the periodic safety message queue is empty, a node must transmit a Type1 packet (including only control information in this case) in its periodic time slot, which allows the node to keep reserving its periodic time slot even when there is no periodic safety packet waiting for transmission. In Figs. 9a and 9b, the performance of the IEEE 802.11p improves with the higher transmission rate, since the transmission duration of each packet is reduced, which decreases the probability of a transmission collision from the neighbouring nodes. On the other hand, the effect of the channel rate on the performance of the VeMAC in Figs. 9a and 9b is negligible. As the VeMAC protocol achieves a higher message goodput than the IEEE 802.11p, it also provides a better channel utilization, as illustrated in Fig. 9c.

TABLE 2: VISSIM simulation parameters

Vehicle input		**Desired speed (Km/h) distribution**		**Car following (Wiedemann 74)**		**Lane changing**			**Vehicle characteristics**		
Parameter	***Value***	***Location***	***Distribution***	***Parameter***	***Value***	***Parameter***	***Lane changer***	***Trailing vehicle***	***Parameter***	***Car***	***Bus***
λ_v	1000 vehicles/hour	Ring road	$U(32, 48)$	AX	2 m	Maximum deceleration	-4 m/s^2	-3 m/s^2	Average length	4.44 m	11.54 m
t_w	5 min.	All other roads	$U(55, 72)$	BX$_{add}$	2 m	-1m/s^2 per distance	100 m	100 m	Width	1.5 m	2.5 m
t_{in}	2, 4, 6, and 7 min.	Right turns	$U(12, 18)$	BX$_{mult}$	3 m	Accepted deceleration	-1 m/s^2	-1 m/s^2	Percentage of the total # vehicles	95%	5%
# vehicles	292, 603, 839, and 948	Left turns	$U(20, 30)$	**Simulation time:** 5 min.		Default VISSIM maximum/desired acceleration and deceleration functions for cars and buses as described in [26] have been used.					

Fig. 10: A snap shot of the simulations showing the simulated roads in blue.

The channel utilization in Fig. 9c improves with the lower transmission rate, due to an increase in the packet transmission duration, which consequently increases the percentage of time that the channel is used for successful transmissions. When the transmission rate decreases from 18 Mbps to 12 Mbps, the channel utilization of the VeMAC protocol increases by a factor of 1.5 (the same ratio between the two transmission rates), while that of the IEEE 802.11p increases by a factor less than 1.5, as the probability of a transmission collision also increases with the lower transmission rate.

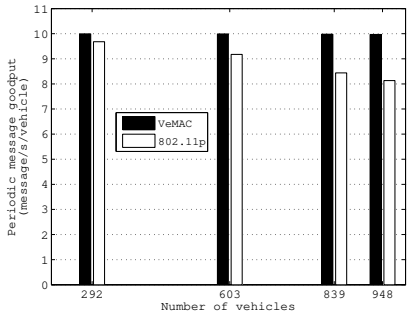
Fig. 9d shows the total delay of the VeMAC and the IEEE 802.11p protocols. For both periodic and event-driven safety messages, the total delay of the VeMAC protocol is dominated by the *access delay* component, which is around 48ms (one half the duration of a frame). At the lowest node density in Fig. 9d, the total delay of the periodic safety messages for the IEEE 802.11p protocol is around 280 μs, which is the sum of the durations of one AC_VI AIFS (71 μs), one periodic safety packet *transmission duration* (164 μs), and the average backoff time ($\frac{\text{CW size}}{2} \times \text{aSlotTime} = 45.5$ μs). This delay increases with the node density, due to an increase in the number of backoff cycles that a periodic safety packet encounters. The delay of the event-driven safety messages for the IEEE 802.11p protocol is higher than that of the periodic safety messages, due to a large size of the event-driven messages, which results in a higher *transmission duration*. Although the VeMAC has a higher total delay than the IEEE 802.11p protocol, it is well below the 100 ms delay bound required for most of the safety applications [9].

6.2 City Scenario

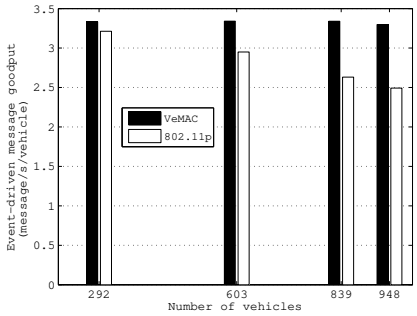
We consider the city scenario as shown in Fig. 10, which consists of a set of roads around the University of Waterloo (UW) campus. To simulate vehicle traffic, the microscopic vehicle traffic simulator VISSIM is employed [6]. The simulator generates a vehicle trace file, which is transformed to an ns-2 scenario file using a MATLAB parser [3]. At the start of the simulation, vehicles enter the road network from every possible entry according to a Poisson process with rate λ_v. After a certain time duration t_{in}, the vehicle input to the road network is stopped, and after an additional warm up period t_w (to reduce transient state effects), the position and speed of each vehicle are recorded at the end of every simulation step. Two types of vehicles are considered: cars and buses. The two vehicle types differ mainly in the vehicle dimensions, as well as the maximum/desired acceleration and deceleration as functions of the vehicle speed. All cars and buses have the same desired speed distribution, which differs from one road to another, and during the left and right turns at intersections. Every intersection in the road network is controlled either by a traffic light, or a stop sign, based on how the intersection is controlled in reality. At signalized intersections, left turns are controlled by the traffic light controller, and right turns are allowed during the red signal phase. Before a vehicle enters an intersection area, it decides whether to turn left, turn right, or not to make any turn, according to a certain probability mass function, which differs from one intersection to another.

The car following model used is the Wiedemann 74 model [23] developed for urban traffic. A vehicle can be in one of four modes: free driving, approaching, following, and braking. In each mode, the vehicle acceleration is a function of the vehicle speed, the characteristics of the driver and the vehicle, as well as the distance and

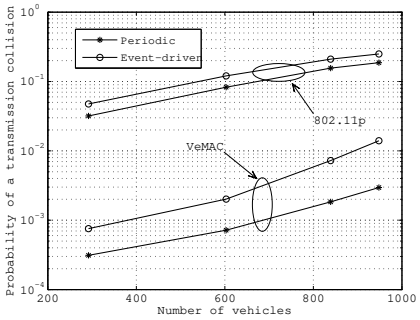
3. Videos of the VISSIM and ns-2 simulations have been recorded and uploaded to [24] and [25] respectively.



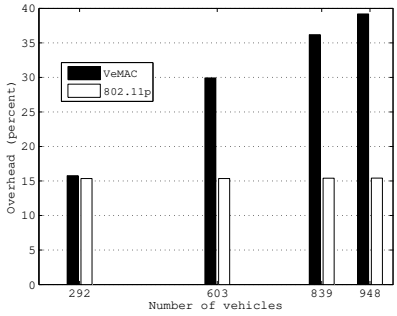
(a) Periodic message goodput.



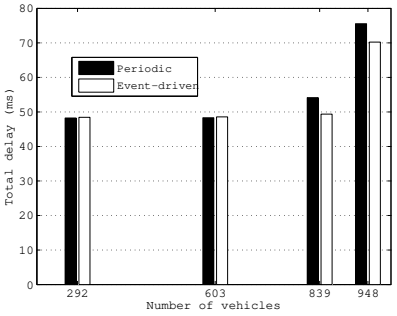
(b) Event-driven message goodput.



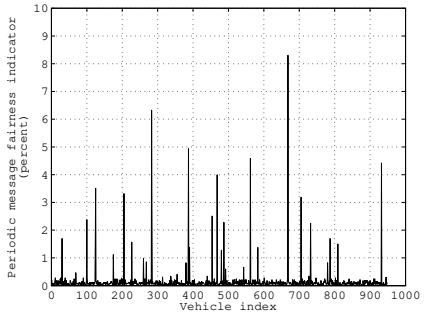
(c) Probability of a transmission collision.



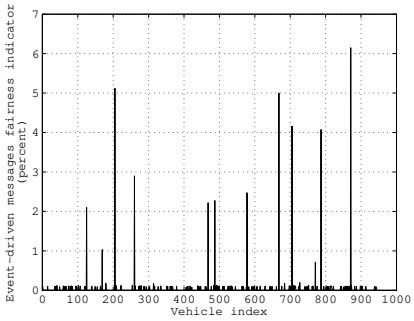
(d) Overhead.



(e) Average total delay for VeMAC.



(f) Periodic fairness indicator for VeMAC.



(g) Event-driven fairness indicator for VeMAC.

Fig. 11: Simulation results for the city scenario.

the speed difference between the subject vehicle and the vehicle in front [23]. The last two variables also determine the thresholds between the four driving modes of a vehicle. The Wiedemann 74 model uses three parameters: the average standstill distance (AX), the additive part of the safety distance (BX$_{add}$), and the multiplicative part of the safety distance (BX$_{mult}$). The AX parameter is the average desired distance between stationary vehicles, and is used with the BX$_{add}$ and BX$_{mult}$ parameters to determine the desired following distance of a vehicle [23]. A vehicle can perform a lane change, either to turn left or right, or because it has a higher speed than the vehicle in front and there is more space in an adjacent lane. The lane change decision depends on the desired safety distance parameters (i.e., BX$_{add}$ and BX$_{mult}$), as well as on the speeds and decelerations of the vehicle making the lane change and the vehicle coming from behind in the destination lane. The VISSIM simulation parameters are summarized in Table 2.

As shown in Figs. 11a and 11b, for all the vehicle densities under consideration, the VeMAC protocol can successfully deliver almost all the periodic and event-driven safety messages to all the vehicles in the one-hop neighbourhoud. At the highest vehicle density, the VeMAC protocol achieves around 23% and 32% higher goodput respectively in the periodic and event-driven safety message goodputs, as compared to the IEEE 802.11p. Fig. 11c shows the significant difference in the probability of a transmission collision achieved by the two protocols. For instance, when the number of vehicles is 839, the probability of a collision of a periodic (event-driven) safety message for the IEEE 802.11p is around 2 order of magnitude (1.5 order of magnitude) greater than for the VeMAC protocol. One main reason of the high probability of a transmission collision for the IEEE 802.11p is the hidden terminal problem, since for broadcast packets, no handshaking [request to send/clear to send (RTS/CTS)] information exchange is used and no acknowledgement is transmitted from any recipient of the packet [21]. Another reason is that, although the

small CW size assigned to the AC_VO and AC_VI allows the safety packets to be transmitted with small delays, it increases the probability of a transmission collision when multiple vehicles within the same THS are simultaneously trying to broadcast their safety packets. Further, if a transmission collision of a broadcast packet happens, the CW size is not doubled (such as in the unicast case), as there is no collision detection without CTS and acknowledgment packets.

The reduction in the probability of a transmission collision by the VeMAC protocol, which results in the high periodic and event-driven message goodputs in Figs. 11a and 11b, is achieved at the expense of an increase in the protocol overhead as shown in Fig. 11d. The main source of the VeMAC overhead is that every Type1 packet transmitted by a certain vehicle x includes the set of one-hop neighbour IDs, $N(x)$, and the time slot index corresponding to each node ID in set $N(x)$ (as indicated in Table 1). On the other hand, the overhead of the IEEE 802.11p protocol is due to control information such as the frame check sequence (FCS) and the physical layer convergence procedure (PLCP) header. At low vehicle density, the overheads of the VeMAC protocol and IEEE 802.11p are similar, as shown in Fig. 11d. However, when the vehicle density increases, the overhead of the IEEE 802.11p remains the same, while that of the VeMAC protocol increases due to a large number of one-hop neighbours of each vehicle, which results in a large amount of control information included in the header of transmitted Type1 packets. Note that, all the VeMAC control information is transmitted on the CCH, which is reserved only for the transmission of safety messages and control information. As well, the VeMAC control information provides each vehicle with knowledge about all the other vehicles in the two-hop neighbourhood. This knowledge can reduce the overhead of some layer 3 protocols, such as the elimination of the Hello messages of position based routing protocols. On the other hand, in a high vehicle density scenario, a large size of the VeMAC control information may increase the number of fragments of each periodic safety message broadcasted by an RSU. This excess fragmentation can result in higher delay of a periodic safety message, unless the RSU accesses more periodic time slots per frame, k_p, to serve the periodic safety message queue. The VeMAC overhead can be significantly reduced if each vehicle broadcasts the set N and the corresponding time slot indices once every m frames, instead of once in every frame as described in Section 3. However, since the set N and the corresponding time slot indices broadcasted by a certain node are required for the one-hop neighbours to detect any transmission collision, as described in Subsection 3.2, the lack of broadcasting this control information in each frame (i.e., $m > 1$) may result in a longer time duration for a colliding node to detect a transmission collision, and consequently to resolve the collision by releasing its time slot and acquiring a new one, a behaviour which can increase the rates of access collisions and merging collisions. The effect of the reduction of the VeMAC overhead when $m > 1$ on the other performance metrics and on the VeMAC multihop broadcast service described in [2] needs further investigation.

The total delay of the VeMAC protocol for the periodic and event-driven safety messages is shown in Fig. 11e. For both types of safety messages, the VeMAC achieves a total delay that is well below 100 ms. One reason of the relative increase in the VeMAC delays at the highest vehicle density is the high contention on the time slots among different vehicles which may force a vehicle to delay the transmission of a safety packet until a time slot is available. To study the fairness of the VeMAC protocol, Figs. 11f and 11g show the fairness indicators of the periodic and event-driven messages respectively at the highest vehicle density under consideration. The periodic (event-driven) message fairness indicator is below 0.3% (0.2%) for most of the vehicles, with a maximum value of 8.3% (6.2%). These results indicate that, even in a high vehicle density, the VeMAC protocol allows all the vehicles to transmit their safety messages in a fair way.

7 Conclusions and Future Work

This paper focuses on how the VeMAC protocol supports the high priority safety application messages in VANETs and compares its performance with that of the IEEE 802.11p standard. How the periodic and event-driven safety messages are queued and served by the VeMAC protocol has been described, and necessary modifications to the VeMAC protocol have been defined to allow each node to access multiple time slots per frame on the control channel. A detailed message delay analysis, including queueing and service delay, has been presented for periodic and event-driven safety messages, taking into consideration the size and the arrival pattern of the safety messages. Simulation results show that the VeMAC protocol can deliver both types of safety messages to all the nodes in the one-hop neighbouhoud with an acceptable average delivery delay (less than 100 ms). Moreover, it is shown that the VeMAC has a low probability of a transmission collision, which results in a higher safety message goodput and better channel utilization, as compared to the IEEE 802.11p standard. In the future, we plan to extend the simulations presented in this paper by considering realistic vehicle traces in city and highway scenarios, to perform hardware implementation and real testing of the VeMAC protocol on the control channel, and to evaluate its performance on the service channels via analysis and simulations.

Acknowledgments

We would like to thank Alex Leung (an Undergraduate Research Assistant) for his help in creating the road network around the UW campus in VISSIM, and Usama Shahdah (a PhD student in the Transportation Systems Research group) for his strong support in using VISSIM. We also would like to thank the reviewers for their

comments and suggestions which helped to improve the quality of this paper.

REFERENCES

[1] H. A. Omar, W. Zhuang, and L. Li, "VeMAC: a novel multichannel MAC protocol for vehicular ad hoc networks," in *Proc. IEEE INFOCOM MobiWorld 2011*, Apr. 2011, pp. 413–418.

[2] H. A. Omar, W. Zhuang, and L. Li, "VeMAC: A TDMA-based MAC protocol for reliable broadcast in VANETs," *IEEE Trans. Mobile Comput.*, 2012 (to appear).

[3] H. A. Omar, W. Zhuang, and L. Li, "Evaluation of VeMAC for V2V and V2R communications under unbalanced vehicle traffic," in *Proc. IEEE VTC2012-Fall*, Sep. 2012.

[4] *IEEE Std 802.11p-2010*, pp. 1–51, Jul. 15, 2010.

[5] http://nsnam.isi.edu/nsnam/index.php/Main_Page

[6] http://vision-traffic.ptvgroup.com/en-uk/products/ptv-vissim/

[7] H. A. Omar, W. Zhuang, and L. Li, "Delay analysis of VeMAC supporting periodic and event-driven safety messages in VANETs," *Submitted to IEEE GLOBECOM*, Dec. 2013.

[8] R. Baldessari *et al.*, "Car-2-car communication consortium manifesto," Tech. Rep. Version 1.1, Aug. 2007.

[9] "Vehicle safety communications project task 3 final report," The CAMP Vehicle Safety Communications Consortium, Tech. Rep. DOT HS 809 859, Mar. 2005.

[10] J. Misic, G. Badawy, and V. Misic, "Performance characterization for IEEE 802.11p network with single channel devices," *IEEE Trans. Veh. Technol.*, vol. 60, no. 4, pp. 1775–1787, 2011.

[11] S. Ozturk, J. Misic, and V. Misic, "Reaching spatial or networking saturation in VANET," *EURASIP J WIREL COMM*, pp. 1–12, Nov. 2011.

[12] M. Amadeo, C. Campolo, and A. Molinaro, "Enhancing IEEE 802.11p/WAVE to provide infotainment applications in VANETs," *Ad Hoc Networks*, vol. 10, no. 2, pp. 253–269, Mar. 2012.

[13] "Dedicated short range communications (DSRC) message set dictionary," *SAE J2735 Standard*, Nov. 19, 2009.

[14] F. Zaid *et al.*, "Vehicle safety communications-applications (VSC-A) second annual report," The CAMP Vehicle Safety Communications 2 Consortium, Tech. Rep. DOT HS 811 466, Aug. 2011.

[15] F. Borgonovo, A. Capone, M. Cesana, and L. Fratta, "ADHOC MAC: New MAC architecture for ad hoc networks providing efficient and reliable point-to-point and broadcast services," *Wireless Networks*, vol. 10, pp. 359–366, Jul. 2004.

[16] D. V. Lindley, "The theory of queues with a single server," *MATH PROC CAMBRIDGE*, vol. 48, pp. 277–289, 1952.

[17] D. Bertsekas and R. Gallager, *Data networks*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1987.

[18] L. D. Servi, "D/G/1 queues with vacations," *OPER RES*, vol. 34, no. 4, pp. 619–629, 1986.

[19] W. Song and W. Zhuang, "Performance analysis of probabilistic multipath transmission of video streaming traffic over multi-radio wireless devices," *IEEE Trans. Wireless Commun.*, vol. 11, no. 4, pp. 1554 –1564, Apr. 2012.

[20] https://code.google.com/p/vemac/

[21] *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)*, pp. 1–1184, Jun. 2007.

[22] ASTM Standard E2213, 2003 (2010).

[23] R. Wiedemann, "Modeling of RTI-Elements on multi-lane roads," in *Advanced Telematics in Road Transport, Proc. the Drive Conference*, Feb. 1991.

[24] http://youtu.be/48daRU6ZpjI

[25] http://youtu.be/GjYWe7eLJ3s

[26] PTV Planung Transport Verkehr AG, *VISSIM 5.40-User Manual*, 2012.

Hassan Aboubakr Omar (S'11) received the M.Sc. (2009) degree in Engineering Mathematics and the B.Sc. degree (2005) in Electronics and Communications Engineering, both from Cairo University, Egypt. From 2005 to 2008, he was a Research Assistant at the Science and Technology Research Center, at the American University in Cairo. Since 2010, he has been working toward a Ph.D. degree at the Department of Electrical and Computer Engineering, University of Waterloo, Canada. Mr. Omar's current research interest includes medium access control, routing, and road side unit placement in vehicular ad hoc networks.

Weihua Zhuang (M'93-SM'01-F'08) has been with the Department of Electrical and Computer Engineering, University of Waterloo, Canada, since 1993, where she is a Professor and a Tier I Canada Research Chair in Wireless Communication Networks. Her current research focuses on resource allocation and QoS provisioning in wireless networks. She is a co-recipient of the Best Paper Awards from the IEEE Multimedia Communications Technical Committee in 2011, IEEE Vehicular Technology Conference (VTC) Fall 2010, IEEE Wireless Communications and Networking Conference (WCNC) 2007 and 2010, IEEE International Conference on Communications (ICC) 2007, and the International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (QShine) 2007 and 2008. She received the Outstanding Performance Award 4 times since 2005 from the University of Waterloo, and the Premier's Research Excellence Award in 2001 from the Ontario Government. Dr. Zhuang is the Editor-in-Chief of IEEE Transactions on Vehicular Technology, and the Technical Program Symposia Chair of the IEEE Globecom 2011. She is a Fellow of the IEEE, a Fellow of the Canadian Academy of Engineering (CAE), a Fellow of the Engineering Institute of Canada (EIC), and an elected member in the Board of Governors of the IEEE Vehicular Technology Society. She was an IEEE Communications Society Distinguished Lecturer (2008-2011).

Atef Abdrabou (M'09) received the Ph.D. degree in Electrical Engineering from the University of Waterloo, Waterloo, ON, Canada, in 2008. In 2010, he joined the Department of Electrical Engineering, United Arab Emirates University, Al-Ain, Abu Dhabi, UAE, where he is an Assistant Professor. His research interests include smart grid communication, network resource management, quality-of-service provisioning, and information dissemination in self-organizing wireless networks. Dr. Abdrabou is a co-recipient of a Best Paper Award of IEEE WCNC 2010. In 2009, he received the National Science and Engineering Research Council of Canada (NSERC) postdoctoral fellowship for academic excellence, research potential, communication, and leadership abilities. He is an Associate Editor of the Journal of Circuits, Systems, and Computers.

Li Li (M'03) received the M.Sc. (1990) degree in Electrical Engineering from Southeast University, Nanjing, China and Ph.D (1993) degree in Electrical Engineering from University of Ottawa, Ottawa, ON, Canada. From 1993 to 1999, she was with Nortel Networks Ltd. as a system architect and then product manager. From 1999 to 2003, she was the chief architecture at SS8 Networks Inc. Since 2003, she has been with Communications Research Centre (CRC), Ottawa, ON, Canada, where she is a research scientist. She has contributed previously to ITU-T and IETF standard working groups, co-authored IETF RFC and has been awarded with several US patents. Her current research focuses on mobile tactical radio networking and adaptive networks, with particular interests in mobile network optimization, networking protocols and algorithms, and performance modeling of mobile networks. She has served as an Associated Editor for Springer's Journal on Peer-to-peer Networking and Applications. Dr. Li has served as Co-chair for the IEEE PERCOM MP2P'06-08 workshops, track co-chair for IEEE VTC2010-Fall, and session co-chair for IEEE MILCOM'08-11, and track co-chair for IEEE MILCOM 2012. She is an Associate Editor for IEEE Transactions on Vehicular Technology.