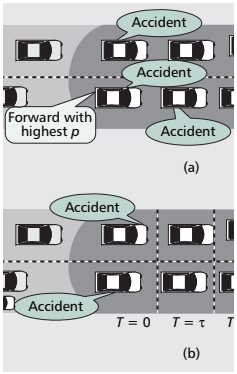
ACCEPTED FROM OPEN CALL

BROADCAST STORM MITIGATION TECHNIQUES IN VEHICULAR AD HOC NETWORKS

N. WISITPONGPHAN AND O. K. TONGUZ, CARNEGIE MELLON UNIVERSITY
J. S. PARIKH, P. MUDALIGE, F. BAI, AND V. SADEKAR, GENERAL MOTORS CORPORATION



The authors quantify the impact of broadcast storm in VANET in terms of message delay and packet loss rate in addition to the conventional metrics such as message reachability and overhead.

ABSTRACT

Several multihop applications developed for vehicular ad hoc networks use broadcast as a means to either discover nearby neighbors or propagate useful traffic information to other vehicles located within a certain geographical area. However, the conventional broadcast mechanism may lead to the so-called *broadcast storm* problem, a scenario in which there is a high level of contention and collisions at the link layer due to an excessive number of broadcast packets. While this is a well-known problem in mobile ad hoc wireless networks, only a few studies have addressed this issue in the VANET context, where mobile hosts move along the roads in a certain limited set of directions as opposed to randomly moving in arbitrary directions within a bounded area. Unlike other existing works, we quantify the impact of broadcast storms in VANETs in terms of message delay and packet loss rate in addition to conventional metrics such as message reachability and overhead. Given that VANET applications are currently confined to using the DSRC protocol at the data link layer, we propose three probabilistic and timer-based broadcast suppression techniques: *weighted p-persistence*, *slotted 1-persistence*, and *slotted p-persistence schemes*, to be used at the network layer. Our simulation results show that the proposed schemes can significantly reduce contention at the MAC layer by achieving up to 70 percent reduction in packet loss rate while keeping end-to-end delay at acceptable levels for most VANET applications.

INTRODUCTION

Vehicular ad hoc networks (VANETs) differ from usual mobile ad hoc networks (MANETs) in many different aspects. First, VANETs consist of mostly highly mobile nodes moving in the same or opposite directions. Vehicles moving along different but nearby roads may or may not be able to communicate with one another due to obstructions. Second, the network shape can be best described by either a one-dimensional line (for a single-lane road) or a strip (for a multilane road) rather than a square or torus shape. Last but not least, most applications targeting VANETs rely heavily on broadcast transmission to disseminate traffic related information to all reachable nodes within a certain geographical area rather than a query for a route to a certain host.

Because of the shared wireless medium, blindly broadcasting packets may lead to frequent contention and collisions in transmission among neighboring nodes. This problem is sometimes referred to as the *broadcast storm* problem. While multiple solutions exist to alleviate the broadcast storm in the usual MANET environment, only a few solutions have been proposed to resolve this issue in the VANET context. In this article, we:

- Explore how serious the broadcast storm problem is in VANETs using a case study of a four-lane highway scenario
- Propose three lightweight broadcast techniques (i.e., weighted p-persistence, slotted 1-persistence, and slotted p-persistence) that can provide 100 percent reachability in a well-connected network and up to approximately 70 percent reduction in broadcast redundancy and packet loss ratio on a well connected vehicular network

The proposed schemes are distributed and rely on GPS information (or received signal strength when a vehicle cannot receive a GPS signal), but do not require any other prior knowledge about network topology.

The remainder of this article is organized as follows. First, we provide the necessary background on VANETs and related research. Then we quantify the impact of the broadcast storm problem in VANETs and provide a detailed discussion. Next, we present the three proposed broadcast mitigation algorithms, and briefly explain the network model and assumptions used in evaluating the performance of the proposed schemes. Finally, the performance of the three broadcast techniques is presented along with the main findings and contributions of this article.

1536-1284/07/$20.00 © 2007 IEEE

Background and Related Work

VANETs: System Overview and Applications

Very much different from other forms of MANETs reported in the literature [1], a VANET consists of mostly mobile vehicles that can intelligently communicate with one another over the 5.9 GHz frequency band via a dedicated short-range communication (DSRC) [2] based device. Currently, American Society for Testing and Materials (ASTM) Standardization Committee E17.51 is working on the development of the overall architecture of DSRC to support both public safety and licensed private operations over vehicle-to-vehicle and roadside-to-vehicle communication channels.

A wide spectrum of services in VANETs include, but are not limited to, public safety, traffic management, freight/cargo transport, transit, and traveler information. It is anticipated that vehicles in the future will be equipped with DSRC devices capable of communicating with nearby vehicles in one-hop or multihop fashion in order to extend the drivers' range of awareness to beyond what they can directly see. Emergency information such as collision or emergency braking can be propagated along the road to notify drivers ahead of time so that necessary action can be taken to avoid accidents. In addition to an emergency warning, drivers can also plan a trip in accordance with traffic conditions received from other vehicles or roadside units in order to save time on the road. The scope of applications can also be expanded to cover other services, which are of private business or automotive industry interests, such as on-road entertainment streaming/downloading and Internet access.

Related Work

Since the DSRC medium access control (MAC) protocol is based on a variant of the widely used IEEE 802.11a transmission standard, testing and developing VANETs is plausible because of the wide availability of 802.11a devices. In the following we briefly describe related research activities on VANETs and other broadcast techniques proposed for general MANETs.

Unlike other forms of MANETs [1], applications developed for VANETs have a very specific and clear goal of providing intelligent and safe transport systems. Emergency warning for public safety is one of many applications that is highly time-critical and requires a more intelligent broadcast mechanism than just blind flooding. In [3] the authors study how broadcast performance scales in VANETs and propose a priority-based broadcast scheme that gives higher priority to nodes that need to transmit time-critical messages. The proposed algorithm categorizes nodes in the network into multiple classes with different priorities and schedules packet transmission accordingly. Although this technique is not designed to solve the broadcast storm problem, it can indirectly mitigate the severity of the storm by allowing nodes with higher priority to access the channel as quickly as possible.

In [4] the authors propose a role-based multicast protocol that suppresses broadcast redundancy by assigning shorter waiting time prior to rebroadcasting to more distant receivers. However, the focus of this study is on achieving maximum reachability in a sparsely connected or fragmented network where the broadcast storm is *not* the main problem. The focus of our study, on the other hand, is on a well connected network where a broadcast storm may be a serious problem.

An efficient 802.11-based urban multihop broadcast (UMB) protocol, proposed in [5], is designed to suppress broadcast redundancy by only allowing the furthest vehicle from the transmitter to rebroadcast the packet. While UMB uses a *black-burst* (channel jamming signal) contention approach [6] to determine the furthest vehicle in the transmission range (essentially a MAC-based approach), our approach, albeit employing a similar distance-based suppression technique, *aims to reduce the load submitted from the network layer to the data link layer* (as opposed to modifying the MAC layer) by combining the probabilistic broadcast technique with timer-based suppression. In addition to reducing the overhead, the mechanism we propose also guarantees that all vehicles receive the broadcast message if the network is fully connected and the broadcast region covers only one section of a highway/road with no ramps or intersections. To guarantee reachability in a Manhattan grid topology or sparsely connected network, however, the protocol should be able to detect the intersection or network fragmentation and handle the message accordingly (*store-carry-forward* the message [4], disseminate the packet into different directions when passing by the intersections [7], rely on fixed infrastructures to provide network connectivity [5], etc.). Since our focus in this article is on a well connected network, in this work we only consider the broadcast storm problem on major highways.

In the MANET context, on the other hand, several approaches have been proposed to cope with the broadcast storm. Distributed *gossip-based* routing, introduced by Haas *et al.* [8], is designed to tackle the overhead problem by suggesting that each node reforward the packet with some probability $p \leq 1$. Inspired by [8], we also propose probabilistic schemes that utilize GPS information in order to improve the packet penetration rate.

In [9] various threshold-based techniques were proposed by Tseng *et al.*, such as the *counter-based*, *distance-based*, and *location-based* schemes. Depending on the scheme considered, a node receiving the broadcast packet compares the predetermined threshold value with its local information, (e.g., the number of duplicate packets received, the relative distance between itself and the sender, or the additional area that can be covered if it rebroadcasts the message). The criteria to adaptively adjust the thresholds according to the number of neighbors were also presented in [10] by Ni *et al.* The results show that with the aid of a positioning device such as the GPS, the location-based scheme seems to offer the best performance in terms of packet penetration rate and link load. Although our schemes employ a similar concept to the schemes in [9, 10], we use a lightweight distributed algo-

Although this technique is not designed to solve the broadcast storm problem, it can indirectly mitigate the severity of the storm by allowing nodes with higher priority to access the channel as quickly as possible.

Because of the highly dynamic vehicular networking environment, the proposed algorithms can be executed in a completely distributed manner without using any prior knowledge about the neighbors' state information.

rithm to calculate the forwarding probability and/or waiting time before rebroadcast instead of using threshold values.

Instead of making a decision at the receiver, Laouiti *et al.* have proposed a sender-based multipoint relay (MPR) technique [11] where the sender controls the number of retransmissions by selecting a subset of its neighbors to relay the message. Although MPR can significantly reduce broadcast redundancy, the amount of overhead introduced by this scheme may be high as it requires that each node have perfect knowledge about its one- and two-hop neighbors in real time in order to properly choose the set of relay nodes. In our work the proposed schemes do not require a node to keep track of its neighbors.

In addition to the transmission logic set by either the sender or receiver, there are some studies that tackle the broadcast storm problem by using the available hardware. In [12] a directional antenna is used by Hu *et al.* to mitigate broadcast redundancy and alleviate contention at the MAC layer. In [13] Lipman *et al.* propose the use of a reliable minimum spanning tree (RMST) algorithm in conjunction with a wireless interface that has multiple transmit power levels. Although the use of a spanning tree algorithm ensures 100 percent reachability, the practicality of the algorithm may be limited to the hardware used since most wireless cards only provide limited access to adjust the physical parameters, and there are typically only 4–7 transmit powers available, which might not be sufficient for this algorithm.

Ongoing Research and Previous Work

The GrooveSim simulator [14], developed at Carnegie Mellon University, operates in five different modes:

- *Drive mode* allows visualization of the real VANET while driving. This mode is especially useful for testing and debugging the protocols under real traffic and channel conditions.
- *Simulation mode* provides the capability to create a large number of virtual vehicles for ease of development and testing the network protocol.
- *Playback mode* playbacks the movement and connectivity of vehicles recorded during the drive mode.
- *Hybrid simulation mode* provides the ability to create virtual vehicles to interact with real vehicles during test drives.
- *Test generation mode* provides easy test scenario generation of multiple vehicles with different communication and mobility models.

For evaluation and testing, each vehicle is equipped with multiple networking and communication devices that consist of a DSRC-based transceiver, a differential GPS receiver, a cellular modem, audio/video equipment, and a Linux-based laptop running GrooveSim in drive mode. As opposed to generic point-to-point MANET routing protocols [15, 16], vehicular networks have well defined applications that mostly favor broadcast protocols. Hence, we also introduce a geographic broadcast protocol, GrooveNet, which is designed to disseminate messages to within a prespecified bounded region with minimal handshaking and state sharing information. Each vehicle running GrooveNet follows a simple set of broadcast rules specified in the broadcast packet header received. The current set of rules include maximum relative distance to the originator of the message, range of the vehicle's heading, and range of the vehicle's speed. Only vehicles whose local information satisfies all the rules rebroadcast the message and take necessary action in response to the message received.

Although routing messages in this manner allows only relevant vehicles to receive and rebroadcast the packets, the current version of the protocol does not have a mechanism for preventing the broadcast storm problem from happening. We propose three novel broadcast suppression techniques in this article to alleviate the packet contention at the link layer. Because of the highly dynamic vehicular networking environment, the proposed algorithms can be executed in a completely distributed manner without using any prior knowledge about the neighbors' state information. The proposed algorithms are tested against realistic highway-like scenarios with several different network densities.

The Broadcast Storm in MANETs and VANETs

It is well known that excessive broadcast redundancy as a result of a broadcast storm leads to severe contention at the link layer, packet collisions, inefficient use of bandwidth and processing power, and, most important, service disruption due to high contention. Typically, mobile hosts in MANETs discover the routes during an explicit route discovery process by flooding the network with a route request (RREQ) broadcast packet. Upon receiving the RREQ packet for the first time, a mobile node either rebroadcasts the packet or replies to the source if it has a route to the destination or is the destination of the RREQ packet.

Some routing protocols, however, have various features designed to avoid flooding the network and creating a broadcast storm [15, 16]. Techniques specified in the protocol standard include the use of *Expanding Ring Search* to help control the broadcast region to within a few hops away from the source. A node can cache each routing entry for a longer time and can also reply on behalf of the destination (Gratuitous Route Reply) to speed up the discovery process. A node running Dynamic Source Routing (DSR) can be in promiscuous mode so that it can construct a routing table by eavesdropping on other nodes' conversations.

Other techniques described earlier can also further suppress broadcast redundancy, but may reduce network connectivity and prolong the route discovery process. Since the goal of route discovery is to acquire the route in the least amount of time without injecting excessive traffic into the network, the main drawbacks of the broadcast storm in MANETs is the contention delay, which may prolong route acquisition and disrupt other ongoing communications, both of which are very undesirable consequences.

In VANETs, however, broadcast is typically used to disseminate traffic-related information

(e.g., detour route, accident alert, construction warning) within a certain area, as shown in Fig. 1. While these may not be as time-critical as requesting a route, a traffic message should persist in a network for *a longer period of time* (e.g., a few hours up to a few days). Therefore, the roadside unit (RSU) that broadcasts traffic information should periodically rebroadcast the message to keep it alive for as long as needed. As a result, a broadcast storm may arise if the traffic density on the road and the frequency at which the RSU broadcasts the message are high. The direct impact of a broadcast storm in this case is waste of processing time and bandwidth, and increased medium access delay. Although these imply that the message will take a few seconds longer to reach vehicles that are many hops away from the broadcast unit, as we show in this article, this increase in delay is negligible from the end user's perspective. However, a more serious impact of the broadcast storm is safety-related service disruption. For example, other urgent safety messages might get lost or delayed during a broadcast storm. In the following we present a simulation study to illustrate and quantify the impact of the broadcast storm in VANETs.

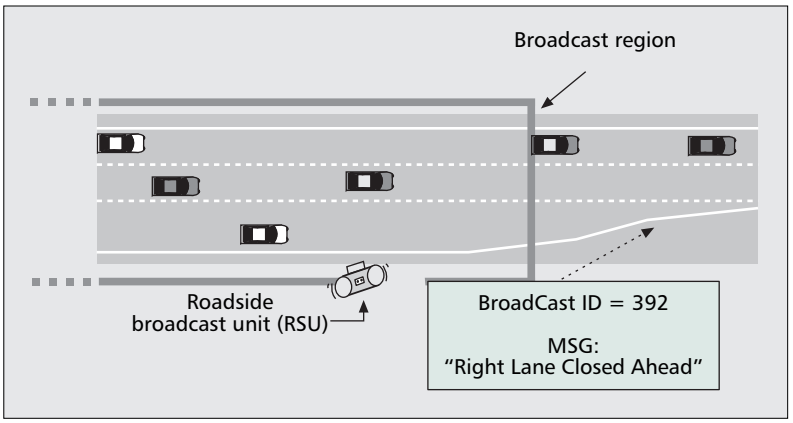


Figure 1. *Traffic alert system.*

Four-Lane Traffic Case Study

In order to understand how the broadcast packet gets propagated in VANETs, we modified ad hoc on demand vector routing (AODV) in OPNET v. 11 to include the broadcast mechanism and studied how the network behaves under different traffic densities from 10 cars/km/lane to 100 cars/km/lane on a 10 km road section with four lanes. The vehicles in the network communicate with one another using a 5.9 GHz 802.11a communication device with a 10 MHz channel. The transmission power is set to 20 mW, and the receiver sensitivity threshold is –95 dBm so that the transmission range is approximately 1 km, according to the Friis propagation model used in OPNET. In the scenario considered, the RSU broadcasts a 25 kb packet on a 10 km road section. The message is broadcast once, and various statistics (contention delay, packet loss ratio, propagation delay, etc.) are collected during the broadcast storm.

The link layer contention delay statistics, measured from all vehicles receiving the broadcast packet during the broadcast storm, at four different traffic densities are shown in Table 1. Results presented are averaged over 1000 simulation runs. Observe that although the average contention delay does not differ much as traffic density increases, the worst case delay differs by one order of magnitude. The increase in medium access delay is due to the increase in the number of vehicles in the same collision domain (or within the carrier sensing range, which is typically twice the transmission range).

In MANETs this wide range of contention delay may cause inefficient route selection if the routing protocol uses the shortest path algorithm. For example, the RREQ packet from the shortest path route may get lost or delayed because of high contention in a dense network. As shown in the traffic jam scenario with 100 cars/km/lane in Table 1, it takes almost 20 hops to propagate the broadcast message to the farthest node, while it takes only about 15 hops under light traffic conditions.

The rest of Table 1 shows the time it takes to propagate the broadcast message to a node that is 10 km away and the packet loss statistics under four different traffic conditions. Interestingly, despite the carrier sensing and backoff mechanism used in 802.11a, there is a high chance of packet collision in the dense network: packet loss ratio is 60 percent in a traffic jam. This is because nodes that receive the broadcast packet within the same period of time and contend for a chance to retransmit the packet are likely to be in the same collision domain and may pick the same backoff time slot.

In an 802.11 network, after sensing an idle channel for a distributed interframe space (DIFS) period of time, a node has to do a random backoff before it can transmit a data packet by randomly picking a time slot from 0 to the minimum contention window size, which is 15 in

Traffic condition	Traffic density (cars/km/lane)	MAC delay (ms)			Number of hops	Total delay (ms)	Packet loss ratio (%)
		Avg.	Max.	95th percentile			
Light	10	0.05	0.72	0.40	14.74	14.14	15.90
Moderate	25	0.32	2.22	1.43	17.06	16.58	34.70
Heavy	50	1.45	7.77	4.20	18.93	17.44	49.07
Jam	100	3.71	13.48	9.30	19.76	21.09	60.32

Table 1. *Broadcast propagation statistics on a 10 km road.*

Unlike the p-persistence or the gossip based scheme, weighted p-persistence assigns higher probability to nodes that are located farther away from the broadcaster given that the GPS information is available and accessible from the packet header.

802.11a. During backoff, a node decreases the backoff timer by one for each idle slot, pauses if the channel is sensed busy, and resumes if the channel is idle again for a DIFS time duration. Finally, when the timer reaches zero, the packet can be transmitted. Therefore, the chance of packets colliding with one another will be high in a dense network given that there are only 15 backoff time slots. This is because nodes who pick the same time slot will transmit the packet at the same time and cause packet collision.

The major impact of a broadcast storm in a VANET, however, is neither the extra number of hops taken nor the long delay because the total end-to-end delay in the traffic jam scenario is only a few milliseconds longer than that in light traffic conditions. This implies that even in high traffic density conditions (100 cars/km/lane), it takes less than 25 ms for vehicles that are 10 km away from the RSU to receive the first broadcast message. To drivers, this delay is negligible if the broadcast packets do not contain an urgent message. However, as also shown in Table 1, the high packet loss ratio during a broadcast storm may cause other urgent safety messages to get lost. Therefore, in order to avoid losing important messages, it is crucial to design a routing protocol that can suppress the broadcast redundancy in VANETs. In the following section we outline three such distributed broadcast techniques.

Broadcast Suppression Techniques

The basic broadcast techniques follow either a *1-persistence* or *p-persistence* rule. Despite the excessive overhead, most routing protocols designed for multihop ad hoc wireless networks follow the brute force 1-persistence flooding rule, which requires that all nodes rebroadcast the packet with probability 1 because of the low complexity and high packet penetration rate. A gossip-based approach, on the other hand, follows the p-persistence rule, which requires that each node reforward with a predetermined probability p. This approach is sometimes referred to as probabilistic flooding [8]. In both schemes repeated reception of the same message or any expired messages should be ignored by broadcasting nodes in order to avoid inevitable service disruptions due to network saturation.

In the following we propose three different broadcast schemes that allow each node to calculate its own reforwarding probability based only on its local information.

Distance-Based Schemes

Weighted p-Persistence Broadcasting

Rule — *Upon receiving a packet from node* i*, node* j *checks the packet ID and rebroadcasts with probability* p_{ij} *if it receives the packet for the first time; otherwise, it discards the packet.*

Denoting the relative distance between nodes i and j by D_{ij} and the average transmission range by R, the forwarding probability, p_{ij}, can be calculated on a per packet basis using the following simple expression:

$$p_{ij} = \frac{D_{ij}}{R}. \quad (1)$$

Note that if node j receives duplicate packets from multiple sources within the waiting period of WAIT_TIME (e.g., 2 ms) before retransmission, it selects the smallest p_{ij} value as its reforwarding probability; that is, each node should use the relative distance to the nearest broadcaster in order to ensure that nodes who are farther away transmit with higher probability. If node j decides *not* to rebroadcast, it should buffer the message for an additional WAIT_TIME + δ ms, where δ is the one-hop transmission and propagation delay, which is typically less than WAIT_TIME. In order to prevent message *die out* and guarantee 100 percent reachability, node j should rebroadcast the message with probability 1 after WAIT_TIME + δ ms if it does not hear the retransmission from its neighbors.

Unlike the p-persistence or gossip-based scheme, weighted p-persistence assigns higher probability to nodes that are located farther away from the broadcaster given that GPS information is available and accessible from the packet header. This is illustrated in Fig. 2a.

Slotted 1-Persistence Broadcasting

Rule — *Upon receiving a packet, a node checks the packet ID and rebroadcasts with probability* ***1*** *at the assigned time slot* $T_{S_{ij}}$ *if it receives the packet for the first time and has not received any duplicates before its assigned time slot; otherwise, it discards the packet.*

Given the relative distance between nodes i and j, D_{ij}, the average transmission range, R, and the predetermined number of slots N_s, $T_{S_{ij}}$ can be calculated as

$$T_{S_{ij}} = S_{ij} \times \tau \quad (2)$$

where τ is the estimated one-hop delay, which includes the medium access delay and propagation delay, and S_{ij} is the assigned slot number, which can be expressed as

$$S_{ij} = N_s\left(1 - \left\lceil \frac{\min(D_{ij}, R)}{R} \right\rceil\right). \quad (3)$$

The time slot approach follows the same logic as the weighted p-persistence scheme, but instead of calculating the reforwarding probability, each node uses the GPS information to calculate the waiting time to retransmit. For example, in Fig. 2b the broadcast coverage is spatially divided into four regions, and a shorter waiting time will be assigned to the nodes located in the farthest region. Hence, when a node receives duplicate packets from more than one sender, it takes on the smallest D_{ij} value. Similar to the p-persistence scheme, this approach requires transmission range information in order to agree on a certain value of slot size or number of slots. Note that N_s is a design parameter that should be carefully chosen. Although N_s should theoretically be a function of the traffic density (i.e., the denser the traffic, the smaller the slot size and the larger the number of slots), it is very hard for each vehicle to predict what the traffic density is and to arrive at a single value of N_s in practice. Hence, network designers can, at best, fix this value or adaptively change this value over time; for example, the protocol should use five

slots during morning and evening rush hours, and three slots during non-rush hours.

Slotted p-Persistence Broadcasting

Rule — *Upon receiving a packet, a node checks the packet ID and rebroadcasts with the pre-determined probability* p *at the assigned time slot* T_{Sij}, *as expressed by Eq. 2, if it receives the packet for the first time and has not received any duplicates before its assigned time slot; otherwise, it discards the packet.*

Each node in this scheme should also buffer the message for a certain period of time (e.g., $[N_s - 1] \times$ WAIT_TIME + δ ms) and retransmits with probability 1 if nobody in the neighborhood rebroadcasts in order to prevent the message's dying out. Figure 2c illustrates the concept of slotted p-persistence with four slots. Similar to the p-persistence case, the performance of this scheme also depends on the value chosen for the reforwarding probability p. We address this problem in detail later.

Received-Signal-Strength-Based Schemes

Because vehicles may not be able to receive GPS signals in some areas (e.g., tunnels, shadowed areas, urban areas with many high-rise buildings), the proposed broadcast techniques can also be modified to use the packet received signal strength (RSS) information instead of GPS information. We note that instantaneous measurement of RSS can only provide rough estimation of the corresponding distance between the transmitter/receiver pair because of multipath fading. In order to get rid of the small-scale fading effect and get a closer estimate of the relative distance to the transmitter, each vehicle should periodically probe its neighbors in order to keep track of the time averaged RSS, which can better represent the actual distance of a vehicle from the transmitter. However, doing so may increase traffic load in the system, which may not be desirable. Hence, in the absence of GPS signal and periodic neighbor probing, each node can, at best, obtain the RSS of the broadcast packet received from the DSRC device driver and determine whether or not to rebroadcast the packet based on the instantaneous RSS measured and prior knowledge of transmit power and receiver sensitivity. In the following we outline the modifications needed to change the proposed broadcast schemes described earlier to use RSS information.

In the weighted p-persistence scheme each node can compare the RSS of the received packet to the range of RSS, which is given by

$$\mathrm{RSS}_{\mathrm{range}} = \mathrm{RSS}_{\mathrm{max}} - \mathrm{RSS}_{\mathrm{min}} \quad (4)$$

where the $\mathrm{RSS}_{\mathrm{max}}$ and $\mathrm{RSS}_{\mathrm{min}}$ correspond to the maximum and minimum possible values of RSS measured in the considered environment; these values can be either obtained experimentally or calculated by applying an appropriate propagation model (e.g., the Friis or two-ray model [17]).

Given that $\mathrm{RSS}_{\mathrm{range}}$ is the same for all vehicles, Eq. 3 can be reformulated as

$$p_{ij} = \frac{\mathrm{RSS}_{ij} - \mathrm{RSS}_{\mathrm{min}}}{\mathrm{RSS}_{\mathrm{range}}} \quad (5)$$

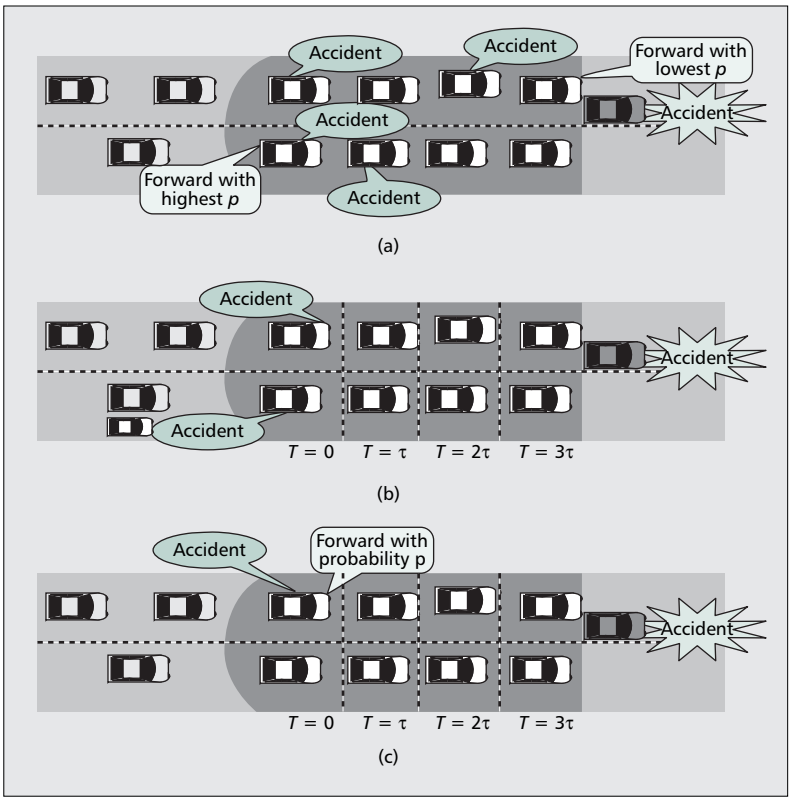


Figure 2. *Broadcast suppression techniques: a) weighted p-persistence; b) slotted 1-persistence; c) slotted p-persistence.*

where RSS_{ij} is the RSS of the broadcast packet received at node j.

Similarly, the slotted schemes could be modified to use RSS information instead of relative distance to determine waiting time. Given the number of slots, Eq. 3 can be modified as follows:

$$S_{ij} = N_s - \left\lceil \frac{\min(\mathrm{RSS}_{\mathrm{range}}, (\mathrm{RSS}_{ij} - \mathrm{RSS}_{\mathrm{min}})) \times N_s}{\mathrm{RSS}_{\mathrm{range}}} \right\rceil. \quad (6)$$

Network Model and Assumptions

Although most MANET studies typically assume a two-dimensional network with random topology, in this work we claim that a one-dimensional line network can best capture the topology of a vehicle-based ad hoc network on a highway or in an urban area where mobile nodes are more likely to be on a well defined path and road. Therefore, we consider two types of network topologies in this article: a one-dimensional line or single-lane network and a multilane network. In the former case adjacent nodes are separated by a distance D that is exponentially distributed with mean $\overline{D}$. A multilane network is modeled with multiple single-lane networks.

In order to understand the fundamental impact each of the broadcast schemes has on network performance, we developed a network simulator to create a broadcast scenario on a straight road, similar to that shown in Fig. 1, where each vehicle can perform the basic broadcast operations proposed earlier without the

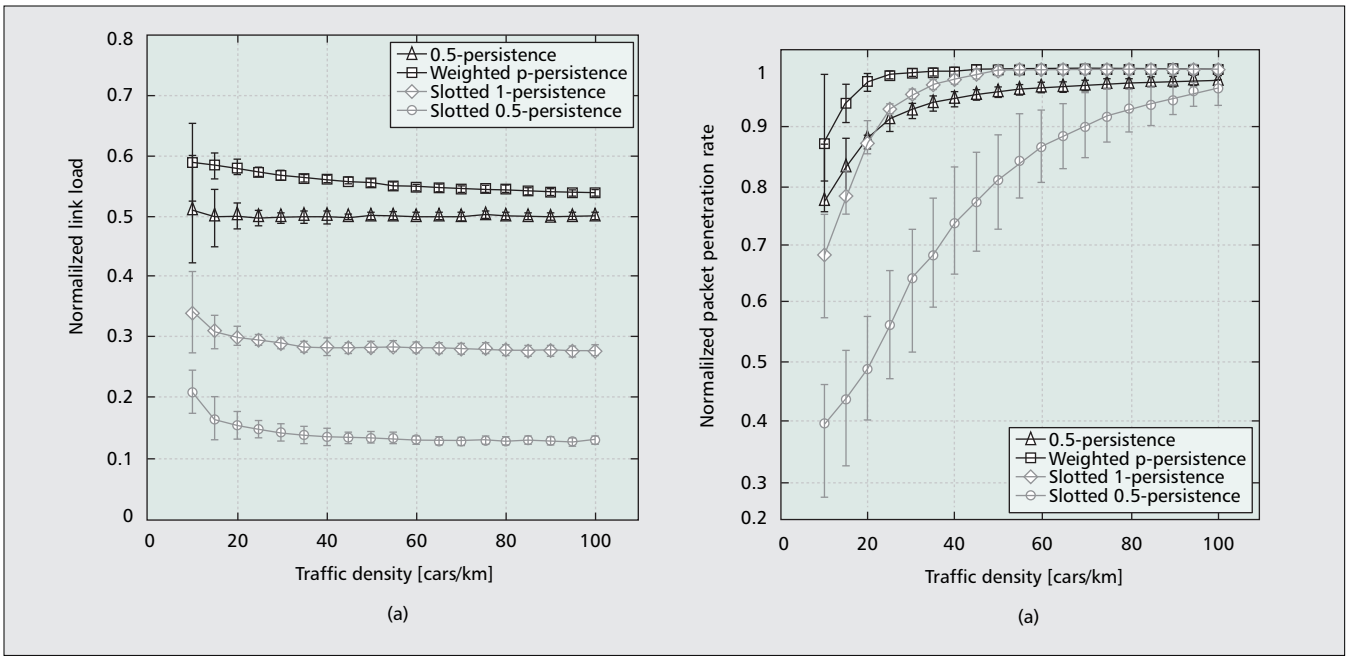


Figure 3. *a)Link load; b) packet penetration rate performance measured from a single-lane network with random traffic distribution.*

complication of the MAC and MANET routing protocol. For each simulation run, a new topology is created and one broadcast message is propagated for 100 hops; the time to live (TTL) of the packet is set to 100. Given the type of VANET applications considered earlier, we assume that there is only one active source in the network, and all the nodes within the broadcast range of the transmitter can correctly receive the packet. Upon receiving the broadcast message, each node keeps track of the number of packets it receives and immediately retransmits the packet according to the rules described earlier. Other statistics such as packet loss ratio and propagation delay are presented later; we also include the effect of 802.11a MAC and the routing protocol.

Performance Analysis

In this section we compare the performance of the proposed broadcast schemes with conventional 1-persistence and p-persistence flooding schemes. Each node has a broadcast range of 500 m. The slot size is assumed to be 100 m so that the broadcast coverage can be divided into five time slots. The reforwarding probability is assumed to be 0.5 in the p-persistence and slotted p-persistence cases. Figure 3 shows the statistical average of 500 simulation runs per data point with 95 percent confidence interval.

Single-Lane Network

Link Load — The link load measures the amount of broadcast traffic received at each node over a unit time. Obviously, the higher the load, the lower the useful throughput. Figure 3a shows the link load, normalized with respect to the link load measured from the 1-persistence case, at different network densities for all the techniques mentioned earlier. Intuitively, the link load depends on the number of retransmitting nodes; for example, if every node decides to retransmit, as in the 1-persistence case, a high link load is expected. The p-persistence is introduced in order to reduce the number of nodes required to reforward the broadcast packets. Typically, given reforwarding probability p, the amount of packets received at each node, on average, will be reduced by a factor of $1 - p$. Besides lowering the reforwarding probability, one can further reduce the load by partitioning the network into multiple broadcast regions, as in the slotted cases. By doing so, nodes in the farthest broadcast region retransmit with high probability, while closer ones refrain from retransmitting. As a result, the link load is reduced dramatically when the slotted scheme is employed.

Packet Penetration Rate — According to the results presented previously, it can be observed that the smaller the reforwarding probability, the better the performance in terms of link load. However, the reforwarding probability also affects the rate at which the packet propagates across the network (i.e., the packet penetration rate). In a typical route discovery case where the source seeks to establish a route to a known destination, this metric also affects the route acquisition time: the faster the packet penetration rate, the faster the route acquisition time. For certain applications such as an on-the-road emergency warning system, this rate determines how fast the warning message travels across the network.

Figure 3b shows the packet penetration rate normalized with respect to the rate achieved by the conventional 1-persistence scheme. It can be observed that both slotted 1-persistence and weighted p-persistence can achieve excellent performance since the farthest node in the broadcaster's coverage retransmits with probability one or close to one. Slotted 1-persistence, on the other hand, performs poorly in a sparse network because of the waiting delay prior to packet

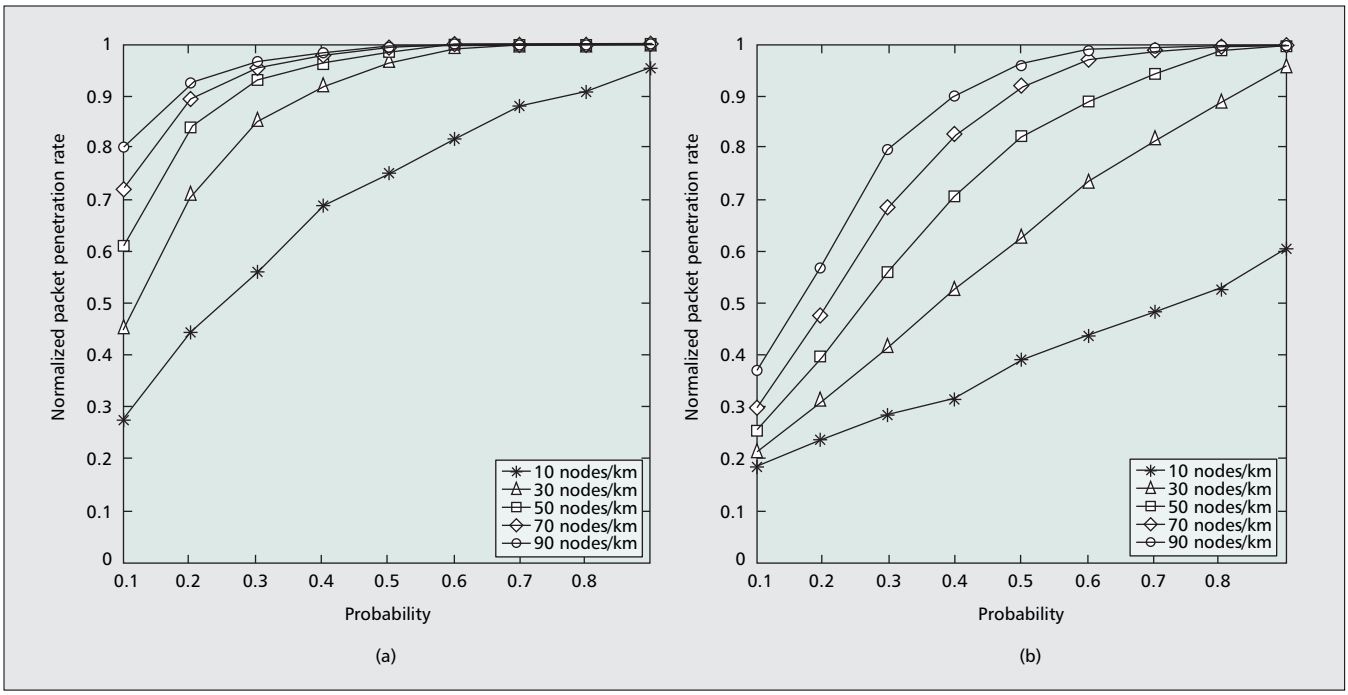


Figure 4. *Achievable packet penetration rate using: a) p-persistence scheme; b) slotted p-persistence scheme.*

retransmission. However, the normalized rate converges to one if on average there are 50 vehicles/km.

As for p-persistence, the achievable performance depends on the preassigned probability parameter p. Intuitively, the smaller the probability, the lower the link load. However, small probability may also result in poor packet penetration rate in a sparse network. According to the simulation results, shown in Fig. 4, there is almost no benefit in using the reforwarding probability under a very light traffic condition as in the 10 nodes/km case, which corresponds to the case where each node has approximately nine neighbors in the network considered. However, at higher traffic density the reforwarding probability should be set to at least 0.5 in the p-persistence case and 0.8 in the slotted p-persistence case in order to achieve at least 80 percent of the maximum performance.

How to choose the number of slots (N_s) and forwarding probability p is certainly an important design issue, and different solutions are possible. One simple, albeit suboptimum, solution is to design the protocol for the worst case scenario (i.e., traffic jam scenario), and use the same fixed value of N_s and p for other scenarios as well. Although setting the forwarding probability to a certain fixed value without precise information about traffic density might yield a suboptimal packet penetration rate, we show later that the end-to-end delay performance is still acceptable (less than 150 ms) for the VANET safety applications considered, even in a sparse network scenario. Since all mobile nodes should agree on certain values of p and number of slots, one solution is for the working standard [2] to make a *centralized decision* or *centralized recommendation* for these values. For example, the number of slots should depend on the transmission range of the wireless device considered, while the chosen forwarding probability p should yield reasonable performance in the worst case scenario (e.g., p should be at least 0.5 in order to achieve reasonable performance in a dense traffic scenario). Other more sophisticated, adaptive, and distributed solutions might also be plausible (e.g., one could use two values of p, one for daytime and another for nighttime, or one value for commute hours and another value for the rest of the day).

Multilane Network

A multilane network is simply a collection of multiple single-lane networks. Intuitively, if we assume that the traffic in each lane is identically distributed, overall traffic density will increase by n-fold in an n-lane network. However, if we were to fix the overall traffic density so that the average number of vehicles per kilometer is the same in both single-lane and multilane networks, the traffic density per lane in the n-lane network case decreases by a factor of $1/n$. Given that we know the traffic density per lane, we can predict the performance in terms of link load and packet penetration rate that can be achieved by each scheme based on the results obtained in the single-lane network presented earlier.

Link load performance depends only on the overall traffic density. Hence, if the overall traffic density is kept constant, the link load in the n-lane network will be the same as that in the single-lane case. If, on the other hand, the overall density increases by n-fold, the average link load also increases by the same factor. Note that although average link load increases with increasing traffic density, the relative performance with respect to the 1-persistence base case does not depend on traffic density but rather on the broadcast parameters (i.e., preassigned reforwarding probability and number of slots or slot size). Therefore, regardless of the

In general, high link load causes high contention at the link layer and, hence, high packet loss rate. Similarly, low packet penetration rate also implies long delay. Therefore, in order to create a realistic broadcast storm scenario for collecting these statistics, we resort to OPNET simulator.

number of lanes considered, the normalized link load will be the same as that shown in Fig. 3a.

The packet penetration rate, on the other hand, is mainly governed by single-lane density rather than overall traffic density. Hence, in the case where the overall density is kept constant (i.e., lower density per lane), it is expected that the packet penetration rate in a multilane network performs worse than that presented in Fig. 3b. However, if the density per lane in a multilane network is the same as that in the single-lane case, the performance is expected to be slightly better than that presented in Fig. 3b. The improvement is particularly large at the lower density per lane because of the redundancy provided by nodes in additional lanes.

Packet Loss Ratio and Delay Analysis and Discussion

In the previous section we have shown that significant improvement in terms of link load and packet penetration rate can be achieved by using the proposed broadcast suppression schemes. However, in order to quantify how much each scheme can alleviate the impact of the broadcast storm, it is important to translate these metrics into more meaningful ones (i.e., packet loss ratio and total end-to-end delay). In general, high link load causes high contention at the link layer and hence high packet loss rate. Similarly, low packet penetration also implies long delay. Therefore, in order to create a realistic broadcast storm scenario for collecting these statistics, we resort to the OPNET simulator.

Communication Model and Broadcast Protocol Implementation

In order to mimic the link layer contention of the DSRC device, we configure the wireless node in OPNET to use IEEE 802.11a with 10 MHz bandwidth so that the range is approximately 1 km. AODV is modified to handle a special broadcast packet by adding a node's location in the routing packet header. Upon receiving the broadcast packet, each node accesses its current location and uses one of the broadcast rules described earlier to determine whether or not the packet should be rebroadcast. For example, if weighted p-persistence is chosen, each node will simply calculate the reforwarding probability based on Eq. 1.

Because it is possible to receive multiple broadcast packets with the same ID, each node has to wait for a period of WAIT_TIME to allow for some or all duplicate broadcast packets sent by other relay nodes to arrive. This WAIT_TIME is also a common parameter in both the slotted 1-persistence and slotted p-persistence schemes since each node has to use its relative distance to the nearest node that has previously rebroadcast the packet to determine its forwarding probability or time slot before transmission. Therefore, WAIT_TIME has to be greater than most of the MAC delay experienced by all of the nodes in the network so that each node has a chance to receive most of the duplicate broadcast packets. According to the MAC delay statistics shown in Table 1, the 95th percentile of the MAC delay for the 1-persistence scenario considered earlier is under 5 ms in most scenarios. These statistics suggest that it is sufficient to choose a WAIT_TIME of at most 5 ms if the traffic density is below 100 cars/km/lane. Note that in a scenario with more than 100 cars/km/lane, the broadcast suppression mechanisms can virtually reduce the level of the contention and cause the 95th percentile of the MAC delay to be significantly less than the values presented in Table 1.

Similarly, the estimated 1-hop delay τ has to account for both the WAIT_TIME and propagation delay. Given that nodes have to be within 1 km of one another in order to correctly receive the packet, the propagation delay will be negligible compared to the WAIT_TIME. Hence, it is reasonable to assume that τ = WAIT_TIME.

Simulation Results

In the following, we consider 1000 simulation runs of a 10 km road section with four lanes and random traffic, similar to the scenario considered earlier. The WAIT_TIME is assumed to be 5 ms, and the slot size is approximately 200 m, so there are approximately five slots. The forwarding probability is set to 0.5 in the slotted p-persistence scenarios.

Packet Loss Ratio — Figure 5a shows the broadcast packet loss ratio at four different traffic densities. Without using any of the suppression schemes, the packet loss ratio is 60 percent in the worst case. Note that this packet loss ratio in the scenario considered pertains to the loss of duplicate broadcast packets only; therefore, even if half of the broadcast duplicate packets get lost, each node can still receive the broadcast message since not all of them get lost during the broadcast storm. Hence, the reachability of the broadcast message should be satisfactory in all scenarios; most vehicles should receive the broadcast message with high probability if the network is well connected. However, as discussed earlier, this high packet loss rate could pose serious problems to other applications, because any urgent messages transmitted during the broadcast storm may get lost or delayed due to link layer contention and software/hardware resource limitations. By making use of GPS or RSS information, it is possible to reduce this high loss ratio in the worst case by up to 90 percent; that is, from 60 percent down to about 5 percent if one uses the slotted p-persistence approach. Notice that these results are highly correlated with the link load results presented in Fig. 3a in that among the three schemes proposed, slotted p-persistence yields the best performance while the worst scheme is weighted p-persistence.

Latency — The total end-to-end delay of the proposed schemes, on the other hand, is significantly longer than that in the 1-persistence case, especially in a sparse network. As shown in Fig. 5b, the total delay increases from 15 to 125 ms under light traffic conditions with 10 cars/km/lane when slotted p-persistence is used. The

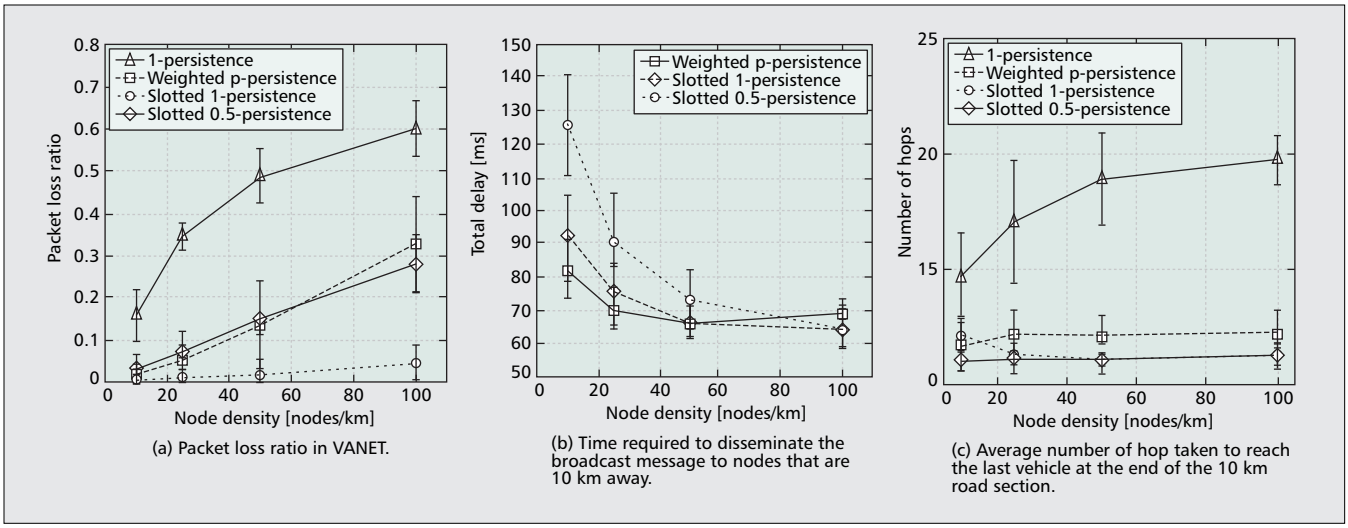


Figure 5. *Broadcast statistics at various traffic densities: a) packet loss ratio in a VANET; b) time required to disseminate the broadcast message to nodes 10 km away; c) average number of hops to reach the last vehicle in the 10 km road section. All results are shown with 95 percent confidence intervals.*

increase in total delay is partly due to the number of hops chosen by the routing protocol, and mainly due to the scheduling and waiting time of 5 ms required before contending with other nodes for retransmission at each hop. Since the proposed schemes give priority to the shortest path route, the number of hops chosen during the route discovery process is almost at the minimum possible value, which is roughly 10 hops for the considered scenario, as shown in Fig. 5c. Observe that traffic density does not have much impact on the number of hops chosen by the routing protocol when one of the broadcast suppression techniques is employed.

Given that the time slot is 5 ms, the total delay is mainly due to the scheduling and waiting time imposed by the broadcast schemes: the transmission delay and propagation delay are much smaller than 5 ms. For example, the transmission delay of a packet of size 250 kbytes is approximately 40 ms, and the per hop propagation delay is at most 2 μs. Observe that when using the slotted scheme, the total waiting time at each hop can be longer than 5 ms in a sparse network because there may not be any nodes in the slot with minimum waiting time. As expected, slotted p-persistence introduces the longest propagation delay due to the uncertainty imposed by the prespecified forwarding probability. In a dense traffic scenario, on the other hand, weighted p-persistence introduces the longest delay among the three schemes due to the longer medium access delay caused by much larger broadcast redundancy. These results also match the packet penetration rate prediction presented in Fig. 3b.

Despite a much longer total delay, however, the message can still propagate 10 km in less than 150 ms under all schemes. Therefore, as long as the delay is within an acceptable range specified by the applications (e.g., active safety applications), the forwarding probability can be decreased or the number of slots can be increased to further improve the packet loss ratio.

CONCLUSIONS

Since most applications in VANETs favor broadcast transmission as opposed to point-to-point routing, routing protocols should be designed to address the broadcast storm problem to avoid unnecessary loss of important safety related packets during a broadcast storm. In this article we have proposed three techniques that depend only on the local positions of the receiver and transmitter nodes. The algorithms are completely distributed and computationally efficient in that they require only minor computations. In the absence of the GPS signal, the proposed algorithms can also be modified to use the RSS of the packet received to determine whether or not the packet should be retransmitted, although this approach is not as efficient as the GPS approach.

The proposed schemes are tested against single-lane and multilane topologies as opposed to generic two-dimensional square or torus topologies. The results show that the proposed slotted 1-persistence and slotted p-persistence schemes can reduce broadcast redundancy and packet loss ratio by up to 70 percent while still offering acceptable end-to-end delay for most multihop VANET applications (e.g., using a roadside unit to inform drivers about detours, construction).

It is worth mentioning here that while the broadcast storm problem can also be tackled at the MAC layer, this article takes the viewpoint that the current DSRC employs a fixed MAC protocol for VANETs specified by the standard [2], and therefore focuses on solving the broadcast storm problem at the network layer via intelligent routing strategies. We consider both of these approaches viable and interesting (and different) ways of solving the same problem. In addition, given that currently active safety applications mainly concern car manufacturers, solving the broadcast storm problem (as well as the routing problem in sparse VANETs [18]) for active safety applications *without* the use of fixed infrastructure (wireless or wired) was considered. With the emergence of new applications

The results show that the proposed slotted 1-persistence and slotted p-persistence schemes can reduce the broadcast redundancy and packet loss ratio by up to 70 percent while they can still offer an acceptable end-to-end delay for most multi-hop VANET applications.

(Internet access, infotainment, social networking, etc.), use of fixed infrastructure will become an attractive option. Further research is needed to address such possibilities.

REFERENCES

[1] O. K. Tonguz and G. Ferrari, *Ad Hoc Wireless Networks: A Communication-Theoretic Perspective*, Wiley, 2006.

[2] ASTM E2213-03, "Standard Specification for Telecom and Information Exchange Between Roadside and Vehicle Systems — 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications," http://www.standards.its.dot.gov/Documents/advisories/dsrc_advisory.htm

[3] M. Torrent-Moreno, D. Jiang, and H. Hartenstein, "Broadcast Reception Rates and Effects of Priority Access in 802.11-Based Vehicular Ad Hoc Networks," *Proc. ACM Int'l. Wksp. Vehicular Ad hoc Networks*, Philadelphia, PA, Oct. 2004.

[4] L. Briesemeister and G. Hommel, "Role-Based Multicast in Highly Mobile but Sparsely Connected Ad Hoc Networks," *Proc. ACM Int'l. Symp. Mobile Ad Hoc Network and Computing*, Boston, MA, Aug. 2000, pp. 45–50.

[5] G. Korkmaz *et al.*, "Urban Multi-Hop Broadcast Protocol for Inter-Vehicle Communication Systems," *Proc. ACM Int'l. Wksp. Vehic. Ad Hoc Networks*, Philadelphia, PA, Oct. 2004.

[6] J. L. Sobrinho and A. S. Krisnakumar, "Distributed Multiple Access Procedures to Provide Voice Communications over IEEE 802.11 Wireless Networks," *IEEE GLOBECOM*, vol. 3, 1996, pp. 1689–94.

[7] G. Korkmaz, E. Ekici, and F. Ozguner, "An Efficient Fully Ad-Hoc Multi-Hop Broadcast Protocol for Inter-Vehicular Communication Systems," *Proc. IEEE ICC*, Istanbul, Turkey, June 2006.

[8] Z. Haas, J. Halpern, and L. Li, "Gossip-Based Ad Hoc Routing," *Proc. IEEE INFOCOM*, vol. 3, New York, NY, June 2002, pp. 1707–16.

[9] S. Ni *et al.*, "The Broadcast Storm Problem in a Mobile Ad Hoc Network," *Proc. ACM Int'l. Conf. Mobile Computing and Networking*, Seattle, WA, 1999, pp. 151–62.

[10] S. Ni, Y. Tseng, and E. Y. Shih, "Adaptive Approaches to Relieving Broadcast Storms in a Wireless Multihop Mobile Ad Hoc Network," *Proc. IEEE 21st Int'l. Conf. Distrib. Comp. Sys.*, 2000, pp. 481–88.

[11] A. Laouiti, A. Qayyum, and L. Viennot, "Multipoint Relaying: An Efficient Technique for Flooding in Mobile Wireless Networks," *IEEE 35th Annual Hawaii Int'l. Conf. Sys. Sci.*, 2001, pp. 3866–75.

[12] C. Hu, Y. Hong, and J. Hou, "On Mitigating the Broadcast Storm Problem with Directional Antennas," *Proc. IEEE ICC*, vol. 1, Seattle, WA, May 2003, pp. 104–10.

[13] J. Lipman, P. Boustead, and J. Chicharo, "Reliable Optimized Flooding in Ad Hoc Networks," *IEEE 6th CAS Symp. Emerging Technologies: Frontiers of Mobile and Wireless Commun.*, vol. 2, Shianghai, China, June 2004, pp. 521–24.

[14] R. Mangharam *et al.*, "GrooveSim: A Topography-Accurate Simulator for Geographic Routing in Vehicular Networks," *Proc. 2nd ACM Int'l. Wksp. Vehic. Ad Hoc Network*, Cologne, Germany, Sept. 2005.

[15] D. B. Johnson, D. A. Maltz, and Y. C. Hu, "Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," IETF Internet draft, Apr. 2003; http://www3.ietf.org/proceedings/04mar/I-D/draft-ietf-manet-dsr-09.txt

[16] C. E. Perkins, E. M. Royer, and S. Das, "Ad Hoc On Demand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.

[17] J. B. Andersenn, T. Rappaport, and S. Yoshida, "Propagation Measurements and Models for Wireless Communications Channel," *IEEE Commun. Mag.*, vol. 99, Jan. 1995, pp. 42–49.

[18] N. Wisitpoughphan *et al.*, "Routing in Sparse Vehicular Ad Hoc Wireless Networks," *IEEE JSAC*, vol. 25, no. 8, Oct. 2007, pp. 1538–56.

BIOGRAPHIES

NAWAPORN WISITPONGPHAN (nawaporn@ece.cmu.edu) received her B.S. and M.S. degrees in electrical and computer engineering from Carnegie Mellon University (CMU), Pittsburgh, Pennsylvania, in 2000 and 2002, respectively. Currently, she is a research assistant working toward a Ph.D. degree in electrical and computer engineering at CMU. Her research interests include traffic modeling, chaos in the Internet, and cross-layer network protocol design for wireless networks.

OZAN K. TONGUZ (tonguz@ece.cmu.edu) is a tenured full professor in the Electrical and Computer Engineering Department of CMU. He currently leads substantial research efforts at CMU in the broad areas of telecommunications and networking. He has published more than 200 papers in IEEE journals and conference proceedings in the areas of wireless networking, optical communications, and the Internet. He is also the author of the 2006 Wiley bestseller *Ad Hoc Wireless Networks: A Communication-Theoretic Perspective*. More information about his research group and research interests can be found at http://www.ece.cmu.edu/~tonguz.

JAY PARIKH (jayendra.s.parikh@gm.com) is currently a staff research engineer at General Motors R&D. He started his career as a research engineer in 1985. He was actively involved in R&D work on a radar-based automotive collision avoidance system including simulation and modeling of 77 GHz radar for automotive applications. Since 1999 his focus has been on R&D of wireless communication for inter- and intravehicular applications. His current interests are applying emerging wireless communication technologies for vehicles ranging from active safety to infotainment to wireless sensors. He received a B.S. in electrical and electronics engineering from L. D. Engineering College, India, in 1976 and an M.S. in computer science from Oklahoma State University in 1980.

PRIYANTHA MUDALIGE [M] (priyantha.mudalige@gm.com) is a chartered professional engineer with 17 years of industry experience. Currently, he is a senior researcher at General Motors R&D, Warren, Michigan. His research interests are vehicle-to-vehicle-communication-based active safety systems, autonomous vehicles, collision avoidance, vision, and embedded software development. He holds a B.Sc.Eng. (Honors) degree from the University of Moratuwa, Sri Lanka, in 1987 and an M.S.Eng. degree from the University of New South Wales, Australia, in 1993.

FAN BAI (fan.bai@gm.com) has been a senior researcher in the Electrical and Control Integration Laboratory, General Motors Corporation, since September 2005. Before joining General Motors, he received a B.S. degree in automation engineering from Tsinghua University, Beijing, China, in 1999, and M.S.. and Ph.D. degrees in electrical engineering from the University of Southern California, Los Angeles, in 2005. His current research is focused on the discovery of fundamental principles and the analysis and design of protocols/systems for next-generation VANETs.

VARSHA SADEKAR (varsha.sadekar@gm.com) received her M.S. degree in CSE in 1989 from the Indian Institute of Technology, Bombay, and her Ph.D. in systems engineering in 1997 from Oakland University, Michigan. She has been with General Motors since 1993 and is currently manager of the Active Safety and Driver Assistance Systems Group at the R&D Center, where she manages several teams involved in the development of applications that provide safety all around the vehicle using combinations of various sensors and algorithms.