A Contention-Free Broadcast Protocol for Periodic Safety Messages in Vehicular Ad-Hoc Networks

Ahmed Ahizoune, Abdelhakim Hafid, Racha Ben Ali
Network Research Lab, University of Montreal, Canada
{ahizouna, ahafid, benalira}@iro.umontreal.ca

Abstract—Ad-hoc multi-hop broadcast protocols are usually used in vehicular networks to provide safety services. However, these protocols face several issues, namely broadcast storms, hidden nodes, and message delivery failures, that prevent safety applications from guaranteeing their required high message delivery ratio and low delays. In this paper, we tackle these issues using a novel cluster-based contention-free broadcast protocol. Particularly, we propose an efficient time slot reservation protocol, centralized in stable cluster heads that continuously adapts to vehicles dynamics. Thus, using a centralized protocol, we ensure an efficient utilization of the time slots for the exact number of active vehicles including hidden nodes; our protocol also ensures a bounded delay for safety applications to access communication channel. We reduce the overhead of our reservation protocol using a directed broadcast propagation and a single reservation request for a periodic medium access during a vehicle’s cluster session. During the recurrent service interval, a contention-based period follows the efficiently-used contention free period; it is dynamically adjusted to improve throughput-sensitive non-safety applications. Extensive simulation results show that the proposed scheme can significantly improve the periodic safety application performance in terms of safety message delivery ratio and delay.

Index-terms: VANET, Periodic Safety Messages, broadcast protocols, contention-free.

I. INTRODUCTION

New wireless technologies have the potential to enable inter-vehicle communications with the purpose of crash avoidance and transportation system efficiency improvement. Consequently, the Federal Communications Commission (FCC) of the U.S. approved the 75MHz bandwidth at 5.850-5.925GHz band, in year 1999, for Intelligent Transportation System (ITS). This wireless spectrum is commonly known as the Dedicated Short-Range Communication (DSRC) allocated by the regulator to be used exclusively for vehicle to vehicle (V2V) and vehicle to roadside (V2R) communications [12]. The DSRC spectrum is divided into seven channels: one control channel generally restricted to safety communications; two channels reserved for future accident avoidance applications and high-powered public safety usages; and four service channels available for both safety and non-safety usage. An IEEE 802.11p Task Group was created to standardize DSRC. It is commonly called WAVE (Wireless Access for Vehicular Environments). This IEEE 802.11p is typically a customized variant of IEEE 802.11a PHY layer specially adapted to provide low-overhead operation in the DSRC spectrum. It combines parts from the original standard together with the MAC amendment 802.11e for QoS support. For more details, authors in [1] introduces the concepts, applications and performance characteristics behind these technologies used for V2V communications. DSRC will support safety critical communications, such as collision warnings, as well as other valuable Intelligent Transportation System applications, such as Electronic Toll Collection (ETC) and real-time traffic advisories, digital map update. The versatility of DSRC greatly enhances the likelihood of its deployment by various industries and adoption by consumers. Broadcast protocols will play a major role in the success of Vehicular Ad Hoc Networks (VANETs) since they will support a large variety of new safety applications. Some of the uses of broadcast protocols are: sending emergency warning messages, transmitting state information to other vehicles, broadcasting aggregate data, address resolution, and determining routes.

However, existing broadcast protocols suffer from several issues not totally resolved in the literature. In fact, due to the specific characteristics of the vehicular network in establishing multi-hop communications over a limited number of channels and commonly using a single radio interface per vehicle, interference related problems occur. Broadcast storms, hidden nodes and reliable delivery of critical messages are the main issues specific to broadcast safety services; these issues that cannot be resolved by the existing IEEE 802.11p broadcast protocol derived from IEEE 802.11.

Our contributions in this paper can be summarized as follows: (1) An improved virtual carrier sense (VCS) mechanism for periodic broadcast messages in which a single Request-To-Broadcast (RTB) is used to reserve periodic time slots for a contention free broadcast during a stability period. RTB and Clear-To-Broadcast (CTB) confirmations are sent during a contention period for each service period. During contention free, emergency messages are prioritized over periodic Safety messages by using a shorter inter-frame space (AIFS1); (2) A time slot scheduling algorithm, implemented by cluster-head vehicles (we assume a clustered structure of the vehicular network), that allocates periodic broadcast time slots to requesting vehicles which minimizes the effects of the hidden station problem; and (3) A dynamic CFP channel operation algorithm, in opposition to the static one used in IEEE 802.11p; it maximizes the throughput on the service channel while guaranteeing low delays and high delivery rates on the control channel.

The remainder of this paper is organized as follows. In Section II, we present related work. Section III presents definitions and assumptions. In section IV, we describe the protocol architecture. In section V, we present the protocol operation analysis. Section VI presents simulation and performance analysis. Section VII concludes the paper.
II. RELATED WORK

Broadcast protocols will play a larger role than unicast messages in vehicular networks since they are designed to communicate important safety messages to all surrounding vehicles in the area.

Because of the broadcast and multi-hop inherent characteristics of VANETs, flooding is generally used in VANETs to disseminate messages to all vehicles several hops away from the source. Broadcasting in VANETs using local information has been widely studied in the literature. Most of these contributions [1, 2 and 3] reduce broadcasting load and improve performance in terms of packet delivery ratio.

Due to the well known broadcast storm problem, broadcasting protocols in VANETs usually include an efficient flooding protocol. Most of these protocols use the vehicles positions information to limit the number of nodes relaying the broadcast messages. Multi-hop Broadcast protocol (UMB) [4] introduces a new RTB and CTB handshake for IEEE 802.11. UMB tackles the problem of hidden node problem which is more accentuated in broadcast mode compared to the unicast mode. It selects the farthest vehicle from a transmitter to retransmit the message. UMB uses repeaters at street intersections to rebroadcast packets in all directions. Authors show that UMB improves the delivery ratio and the bandwidth utilization compared to the standard IEEE 802.11. However, packet dissemination speed is slower for small packets and is relatively worse at higher transmission rates.

The multi-hop vehicular broadcast (MHVB) [5] efficiently broadcasts local information for safety services, such as positions and velocities, in VANETs. It includes a congestion detection algorithm that avoids unnecessary broadcasts in congestion situations and a backfire algorithm that selects the broadcast relaying nodes based on the distance. Authors show that MHVB improves the performance of broadcast services in VANETs. The same authors improve this protocol in [6] by altering the backfire area from a circular shape to a sectoral shape. Furthermore, they introduce a dynamic priority scheduling algorithm based on the "processing" of the received messages. Particularly, this improved MHVB make vehicles that are at a distance farther than 200m re-transmitting the received information earlier than all the other nodes in the network. Thus, emergency information is forwarded more quickly over longer distances.

The mobility-centric approach for data dissemination (MDDV) in VANETs [7] is designed to exploit mobility for message broadcasting. It combines opportunistic forwarding, trajectory based forwarding and geographical forwarding. MDDV determines a forwarding path to a destination region, and its closest vehicles within the path to participate in group forwarding.

Palazzi et al. [8] propose a Fast multi-hop Broadcast protocol (FB) to quickly propagate broadcast messages by adapting to transmission range variations when minimizing the number of relaying hops. Particularly, FB allows each vehicle to estimate its current transmission range and transmit it to other vehicles. Receiving vehicles use these estimations to determine their relative positions and assign to themselves priorities in becoming next forwarders of broadcasted messages.

Although these broadcast protocols improve the performance of VANETs by reducing the message delivery delay and/or the message delivery success rate, they assume a contention based medium access. This latter requires complex mechanisms, (to resolve broadcast contentions) that struggle to maintain good performance in very high load conditions and especially to satisfy real-time constraints of safety applications. In fact, since standard VCS mechanism, i.e. RTS/CTS, cannot be used to prevent hidden nodes collisions when broadcasting safety messages, frequent collisions in larger hidden node areas are experienced in this broadcast environment compared to a unicast one. Moreover, the mechanisms used in RTB/CTB schemes, such as in UMB [4] for instance, cannot guarantee a collision free reception of the CTB. Furthermore, the reservation RTB/CTB for each broadcast transmission adds a considerable and unnecessary overhead for periodic safety message broadcast. Rather than relying on a contention-based MAC protocol, we propose a novel reservation based protocol especially customized for periodic broadcast applications. By this protocol, we aim to: (1) efficiently reduce the reservation signalling overhead using a stable-cluster-based centralized (at the cluster head) reservation protocol that manages an efficient schedule of contention free periods with less signalling overhead; (2) guarantee a deterministic access for the delay-sensitive applications with a high delivery ratio; and (3) maximize the throughput for other applications by an adaptive adjustment of contention free period (CFP) and contention period (CP).

III. DEFINITIONS AND ASSUMPTIONS

In this section we present the definitions of key terms and assumptions used in this paper.

As shown in Figure 1 we identify three basic states/roles of a node:

Cluster Head (CH): A cluster head serves as a local coordinator for its cluster, performing inter-cluster routing, data forwarding and so on. In our protocol, each CH maintains two groups of vehicles: the Back Group (BG) and the Front Group (FG).

Back Group (BG): Contains every cluster member whose position \( X_i \) is smaller than \( X \) where \( X \) is the position determined by CH in order to avoid interferences (see Section V). In this paper, we assume that the coordinates of a node correspond to its projection on a reference axis (x-axis) for which an origin is defined, according to a given direction. Only one coordinate, \( X \), is thus sufficient to define the position of a car.

Front Group (FG): Contains every cluster member whose position \( X_i \) is bigger than \( X \) where \( X \) is the position determined by CH in order to avoid interferences.

Cluster Gateway (CG): A cluster gateway is not a CH with inter-cluster links; thus, it can access directly (1-hop communication) neighboring clusters and forward information between clusters. In our proposed scheme, the election of CG is based on the distance \( D \) between two neighbouring CHs. If \( D \) is 2-hops (Figure 1-(b)), then the node part of the shortest path between the two CHs is elected as CG. If \( D \) is bigger than 2-hops then, as shown in Figure 1-(a), \( CH_m \) and \( CH_n \) elect \( CG_m \) and \( CG_n \) according to the following rule: \( CG_m \) belongs to BG of \( U_m (Um_{BG}) \) and is the farthest from \( CH_m \) and \( CG_n \) belongs to FG of \( U_n (Un_{BG}) \) and is the
farthest from CH $n$. The cluster-head keeps updating these lists according to topology changes.

**Cluster Member (CM):** A cluster member is a node that is neither a CH nor a CG.

Sometimes, an additional state called Undecided State (US) is used for the initial state of a node.

We call forward CG the selected forwarder in the forward direction of cluster vehicles movement. Similarly, we call backward CG the selected forwarder in the backward direction of cluster vehicles movement.

In this paper, we assume that vehicles positions and timing information are provided using GPS (Global Positioning System) timing information. All vehicles have the same transmission power and thus the same transmission range $r$ and the same interference range $R (R = 1.78 \times r [15])$.

Also, we assume that time is partitioned into periodic, regulated intervals, called the Repetition Period (RP). RP is of length $T$. Each RP is shared between service and control channels and divided into two periods, CFP and CP.

**IV. PROPOSED PROTOCOL**

IEEE 802.11 broadcast transmission is not reliable. Vehicle safety applications need to be designed to tolerate some broadcast message delivery failures. Nevertheless, it is important, when designing a safety application protocol for VANETs, to consider reducing the number of broadcasts that generate bad receptions. A node in a VANET is able to detect collisions and congestion by simply analyzing the sequence numbers of packets it has recently received [16]. Each node will periodically broadcast its status, e.g., relevant information about its location, speed, and acceleration to its neighbours. While a node does not know whether the packets it sent are correctly delivered, it knows the exact percentage of packets sent to it, from its neighbours that are successfully received if a feedback mechanism is implemented. Based on this feedback, a node is able to dynamically adjust the parameters it uses, such as contention window (CW) size, transmission rate, and transmission power, to improve the delivery rate of broadcast messages. The probability of transmission collisions can be reduced and the packet delivery rate can be improved if the size of the CW used to send broadcast messages is able to adapt based on the network conditions.

Rather than relying on feedback messages, for each broadcast message sent by the source, that increase interferences and collision probability on the shared wireless medium, we propose to allow the transmission of feedback messages only in two situations (a) occurrence of congestion and (b) or other message delivery problems (e.g. hidden node problem).

In fact, due to the specific periodicity of safety messages, we do not need, as in the standard 802.11 protocol, to exchange a RTB/CTB each time a message needs to be broadcasted. Therefore, we propose to synchronize the nodes using GPS timing information and include 802.11 transmission opportunity periodicities in the RTB message. Consequently, each node will establish periodic Network Allocation Vector (NAV) periods during which it is not allowed to transmit since these periods are reserved for transmissions of other nodes; this will considerably reduce interferences and collisions. Furthermore, by adding a congestion notification field in CTB messages, the local node, upon receipt of these messages, can be aware of its participation to a remote congestion along the broadcast forwarding path. Thus, it can adjust its broadcast rate $f$ based on the level of measured congestion. We assume that the periodic safety application adjusts its message broadcast rate $f$ based on lower layer congestion.

**Broadcast forwarders (multi-point relaying) selection:** In most cases, safety messages do not need to be flooded over all directions. Indeed, several nodes, such as vehicles upward a sudden traffic jam may not be interested in the information it encapsulates. Therefore, in our proposed protocol we add a field in the RTB message specifying one of the four possible broadcast forwarding directions (eastbound, westbound, northbound or southbound). This will prevent unnecessary safety message broadcasts to participate in increasing the congestion level. The forwarder is selected among the $n$ nodes in the broadcast range quadrant of the specified direction that reports the $n$ lowest signal strengths. These nodes correspond to the $n$ farthest vehicles from the CH within the broadcast range quadrant. This simple forwarder selection process will ensure that a minimal number of hops will be used to forward the broadcast message; other more dynamic forwarder selection mechanisms, such as the mechanism reported in [9], may also be used.

In opposition to the RTB/CTB message exchanges used in [4] (where these exchanges are repeated for each packet broadcast), in our proposed protocol it is performed only once during a cluster join session. This being said, the verification of the availability of the forwarder is performed for each packet transmission using timeout ACK.

**SCH/CCH channel switching algorithm:** In the DSRC standard, the radio interface of the vehicle has to switch between the control channel (CCH) on which safety messages are broadcasted and the service channels (SCH) on which other unicast data communications are transmitted. Since safety and non-safety applications can not transmit on different channels at the same time using a single radio, CCH/SCH switching has to be performed where a pre-emptive priority is given to transmit the emergency safety messages. Indeed, if a safety application generates an emergency message while a non-safety application is transmitting on the SCH, this latter has to be pre-empted, i.e. temporarily suspended. This is done in order to allow the safety application to switch the single radio interface to CCH on which the urgent message will be transmitted. However, due to the overhead latency of the channel switching process, broadcast safety messages could be lost while the radio is busy switching channels, and therefore, retransmissions are usually needed to ensure reliable delivery. In addition to this pre-emptive switching used for instance in the PeerCast protocol [1], a periodic switching is performed to balance between periodic safety message transmission over the CCH and applications over the SCH.

The DSRC standard uses static time intervals during which the radio is assigned to CCH and SCH channels. In our protocol, we propose to dynamically maximize the time interval for throughput-sensitive applications over SCH channel while guaranteeing a deterministic collision-free access for delay-sensitive safety applications over SCH/CCH channel. The minimal time interval duration for CCH can be
computed by cumulating periodicity information in the RTB messages and taking into account different congestion and wireless medium factors (e.g. AIFS, CW, beacons, etc.).

In this paper, the design of our protocol is motivated by the fact that DSRC spectrum at 5.9-GHz band is divided into seven channels, including Ch172, Ch174, Ch176, Ch178, Ch180, Ch182, and Ch184, each spanning 10 MHz. One of these seven channels is identified as a control channel Ch178; it can be used for Inter-cluster management, delivering safety messages and announcements between CMs and their CH, and between neighboring CHs via CGs. The remaining six channels are called service channels; they are used for Intra-cluster management and safety message delivery within the cluster. In addition, CMs can use service channels to exchange non-safety data with one another and with members of neighboring clusters.

![Figure 1. Highway scenario](image)

Our proposed scheme aims to provide low latency and high message delivery ratio of real-time data safety messages and increasing the throughput for the non-safety data over the V2V-based VANETs. The key idea behind our proposed scheme is to integrate the clustering algorithm with both the contention-free and contention-based MAC protocols under the DSRC architecture.

TDMA-based (Time Division Multiple Access) MAC protocols are usually used to achieve collision-free transmission of data over the shared wireless medium. In these protocols, a central node such as the access point, assigns the different time slots to data sources. However, since VANETs do not rely on a centralized node in a fixed infrastructure, we need to elect a vehicle that will act as a central node for time slot scheduling and management. Therefore, our proposed protocol uses a CH election algorithm to select the central node.

A. Cluster Formation algorithm

In VANET, vehicles moving in platoons share similar traffic patterns like the average speed, the average acceleration, and the direction of motion. This group of vehicles can be united together to form a new entity called a cluster. Clustering schemes [10-12] can be used to reduce data congestion and increase the probability of safety and non-safety data delivery. There are many techniques for cluster formation (e.g. [12, 13, 14 and 17]). In this paper, we adopt a mobility-based clustering scheme for Vehicle Ad hoc Networks, [17], that uses the Affinity Propagation algorithm in a distributed manner. This algorithm determines clusters that minimize both relative mobility and distance from each CH to its CMs. The resulting clusters are stable and exhibit long average CM duration, long average CH duration, and low average rate of CH changes.

B. Repetition period

The CFP is divided into time slots. Each time slot can be owned by only one CM on service channel. The time slots are grouped into virtual frames VF=F1 + F2. F1 contains time slots of vehicles in the range of the forward CG node whereas time slots in F2 are allocated for vehicles in the range of the backward gateway node. During its assigned time slot, a vehicle can transmit its safety messages while all others must remain silent but they can receive or overhear others’ transmissions. The time slot size is related to the transmission latency of the longest safety message packet. The time slot duration of a packet with a maximum size S is denoted by $T_{Slot} = \frac{S}{R}$, where, R is the channel data rate.

CP follows CFP in the RP, T, as illustrated in Figure 2. CH responds to requests from vehicles joining the cluster, updates the list of CMs and elects the backward and the forward CGs. A CM keeps listening to the service channel until the end of CP, or switches to the control channel if it loses contact with its CH.

C. Slot management

Vehicles act as mobile nodes with different speeds in VANETs. A vehicle knows that it is in the range of a given CH when it receives an advertisement message from it. Each vehicle broadcasts, during CP, a Hello message that includes information about its speed and position. If it needs to send a safety message, the vehicle will send a slot request RTB during CP. Due to the specific periodicity of safety messages, each CM does not need, as in IEEE 802.11, to exchange RTB each time a safety message needs to be broadcasted; it requests to reserve a periodic time slot for CFP allocation by a single RTB during a stability period. In this paper, we define a stability period as the period during which CMs remain in the same cluster and the CH does not change its state. When a CH gets a RTB for CFP allocation, it checks the current state of CFP allocation and the list of vehicles in the cluster. Then, CH adds the CM identifier to BG or FG and assigns the corresponding CFP time slots to the CM by replying with CTB containing the slot identifier. The CH, maintains a slot schedule as illustrated in Figure 2-(b). In the same way, deallocating CFP slots are performed by the CH after a CM resigns (i.e., requests leaving the cluster) or a CM’s dead time interval expires elapses (i.e., a hello reception timeout). In other words, if the CH does not receive any message from a given CM after a specific time period, it declares the vehicle in an out of transmission range and therefore, the vehicle is no longer a member of the cluster.
V. PROTOCOL OPERATION ANALYSIS

A. Intra-cluster communication

According to our protocol, access to the wireless medium for intra-cluster and inter-cluster communication is divided into CFP and CP. The periodicity of Safety message within a cluster is defined within CFP. Thus, time slots in CFP are assigned to vehicles in order that each vehicle can broadcast its Safety message in a dedicated and predictable duration.

Time slot scheduling protocol: In order to avoid interference among CMs and, thus, avoid the hidden-terminal problem, we propose a novel time slot scheduling protocol to be executed by CHs; the protocol allocates periodic broadcast time slots to a requesting vehicle based on the position of its neighbouring CHs and the number CMs (per neighbouring CH).

Let us consider clusters \( U_n \) and \( U_m \) of \( N, M \) vehicles (see Figure 1):

\[
U_n = \{V_1, \ldots, V_n\} \quad \text{and} \quad U_m = \{V_1, \ldots, V_m\};
\]

\[
PQ = (X_m - X_n, Y_m - Y_n)\]

is the velocity vector where \( P(X_n, Y_n), Q(X_m, Y_m) \) are the positions of the CHs (\( CH_n \) and \( CH_m \)) of \( U_n \) and \( U_m \) respectively.

As shown in figure 1, \( U_n BG \) contains every cluster member \( CM_i \) whose position \( X_i \) is smaller than \((r + \sqrt{r} + X_M)\); \( U_n FG \) contains every cluster member \( CM_i \) whose position is bigger than \((X_M - 2.78 \cdot r)\). In order to know which slot is assigned to which vehicle, \( CH_m \) and \( CH_n \) transmit a Start Frame SF to their CMs that contains a map with the time slots allocation of the virtual frame \( VF = F1 + F2 \). As shown in Figure 2-(a), \( U_B, U_A \) in \( F1, F2 \) contain the Time slot of vehicles in BG, FG groups respectively. Newly arriving mobile vehicles in a cluster negotiate the allocation of CFP slots in the CP period on control channel.

B. Inter-cluster communication

After receiving safety messages, CHs use data fusion techniques (e.g. [12]) to consolidate the safety information and send it to elected CGs on CCH. The CG uses its time slot during CFP period on CCH to forward backward the safety information, to the neighboring CH (see Figure 2-(b), or neighboring forward CG in case the current CG is out of neighboring CH range. The CH keeps receiving safety messages from neighboring clusters via CG. Note that, during CP, CMs can exchange data with one another and also with neighboring clusters via service channels. The CH transmits a Start Frame (SF), which is very similar to a beacon frame. This SF contains the mapping information between CMs and VF time slots. It is broadcasted at the beginning of the service interval to all CMs.
C. Dynamic CFP channel operation algorithm

If node=CM:
1. Listen on CCH channel and wait for SF.
2. Extract its reserved time slot information from SF and switch listening to SCH.
3. Activate the NAV until its reserved time slot occurrence.
4. Transmit its broadcast periodic safety message after waiting an arbitrary AIFS2, which is longer than AIFS1 used to broadcast emergency safety messages.
5. Wait for the end of dynamic CFP.
6. Transmit its unicast non-safety messages on SCH or switch to CCH if emergency safety messages need to be transmitted and switch back to SCH.
7. Go to 1.

If node=CG:
1. Listen on CCH channel and wait for SF.
2. Extract its reserved time slot information from SF.
3. Activate the NAV until its reserved time slot occurrence.
4. Listen for safety messages from neighbors cluster’s CH and forward it to its own CH during its first reserved time slot.
5. Switch to SCH and transmit its broadcast periodic safety message during its second reserved time slot.
6. Wait for the end of dynamic CFP.
7. Transmit its unicast non-safety messages on SCH or switch to CCH if emergency safety messages need to be transmitted and switch back to SCH.
8. Go to 1.

If node=CH:
1. Compute its own reserved set of time slots (based on the number of CMs) in addition to its CMs reserved time slots and transmit this information in SF on CCH channel.
2. Forward safety messages to neighboring CHs via CGs during its reserved time slots.
3. Switch to SCH and transmit its broadcast periodic safety message.
4. Wait for the end of dynamic CFP.
5. Transmit its unicast non-safety messages on SCH or switch to CCH if emergency safety messages need to be transmitted and switch back to SCH.
6. Go to 1.

VI. SIMULATION RESULTS

In this section, we present our simulation and analysis to evaluate the proposed protocol.

A. Simulator Setup

All simulations are run using NS-2 version 2.33. Table I lists the various IEEE 802.11p parameters settings configured in the simulator.

Based on a transmission rate of \( R = 6 \text{ Mbps} \), and a packet size of \( S = 200 \text{ bytes} \), including 25 bytes of header, the lowest theoretical transmission delay is \( T_{\text{Slot}} = 0.3 \text{ ms} \). Considering that collision warning messages should have a maximum delay of 100 ms to be able to provide a reliable service, therefore, we set \( RP(T) \) to 100 ms, and the max length of a TDMA frame \( T_{\text{ch}} = 70 \text{ ms} \).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>6 \text{ dBm}</td>
</tr>
<tr>
<td>Frequency</td>
<td>5.9 \text{ GHz}</td>
</tr>
<tr>
<td>Data Rate</td>
<td>6 \text{ Mbps}</td>
</tr>
<tr>
<td>RxTh</td>
<td>-87.88 \text{ dBm}</td>
</tr>
<tr>
<td>CsTh</td>
<td>-91 \text{ dBm}</td>
</tr>
<tr>
<td>CpTh</td>
<td>4 \text{ dB}</td>
</tr>
<tr>
<td>Slot Time</td>
<td>9 \mu \text{s}</td>
</tr>
<tr>
<td>SIFS Time</td>
<td>16 \mu \text{s}</td>
</tr>
<tr>
<td>Preamble Length</td>
<td>60 \text{ bits}</td>
</tr>
</tbody>
</table>

Figure 3. The probability of safety-message delivery failure vs. the density of vehicles

Figure 4. The average Safety message Link delay vs. the densities of vehicles

B. Scenario description

The mobility model used in the simulations is the freeway mobility model with four highway lanes, all in the same direction. When vehicles arrive at the end of the highway, they wrap around from the beginning position of the same lane of the highway. The scenario setup is shown in Figure 1. Each node in the simulation is restricted to only travel within its lane. The velocity of each node is temporally restricted based on the nodes previous velocity. A safety distance is maintained so that a node cannot exceed the velocity of the node in front of it if they are within the safety distance.

We consider the following metrics to evaluate our proposed scheme (1) Average safety message delivery delay:

\[
\bar{D} = \frac{1}{n} \sum_{i=1}^{n} d_i
\]

53
Where \( n \) is the total number of vehicles, \( d_i \) is the time taken to send and receive a data packet; (2) Probability of safety message delivery failure:

\[
P = 1 - \frac{1}{n} \sum_{i=1}^{n} P(S_i) \quad P(S) = \frac{1}{x} \sum_{i=1}^{m} y_i
\]

Where \( n \) is the total number of vehicles in our simulation, \( x \) is the packet generation rate, \( m \) is number of neighbors of node S, \( y_i \) is the number of packets unsuccessfully received from sender S and (3) The non-safety message throughput: the average rate of successful message delivery over the whole target region in the network.

A velocity range is specified for the nodes; the acceleration of the vehicles is set to 10% of the maximum velocity. To determine the effectiveness of our proposed broadcast algorithm, described in Section IV, a number of simulations were carried out. In these simulations, we compare the performance of the standard 802.11p protocol against our proposed adaptive and reservation based protocol. We consider the results for three different cases in terms of densities of vehicles, including low density, medium density, and high density. The vehicle density cases that were considered are on average 100 (low density), 200 (medium density) and 300 (high density) vehicles/km/4 lanes. For each traffic density, the average preferred speed of vehicles varies uniformly between 15 and 55 m/s. We use Constant Bit Rate (CBR) traffic of 10 packets per seconds to simulate the safety message application packet generator in each vehicle.

Figure 3 presents the probability of safety-message delivery failure when we increase the number of vehicles and the average speed. Figure 4 shows the safety message delivery delay for different densities of vehicles and average preferred speeds. Using our proposed scheme, we observe that the probability of safety-message delivery failure does not increase with the increase of the number of vehicles and does not exceed 0.05% in the worst case versus 9.5% for the standard scheme. We also observe that our proposed scheme, compared to the standard one, can achieve a low and stable safety-message delivery probability as well as a low average safety message delay under different traffic scenarios (Figure 4). This is due to the proposed time slot scheduling protocol implemented with the clustering techniques (CMs of a cluster exchange safety messages without contention, leading to the timely safety-message delivery), which can significantly decrease the packet collisions and increase the successful broadcast rate. Figure 5 also shows that unlike the standard scheme, all nodes are not trying to simultaneously access the channel, and therefore the access delay remains short. Furthermore, since the packets are transmitted during their reserved time slot in the service interval no later than 100 ms on each hop, our protocol provides a bounded constant delay in average.

Figure 6 shows the gains in non-safety message throughput for a dynamic and a static CFP channel operation algorithm when static CFP period is 70ms against the densities of vehicles.

We can observe that for low and medium densities of vehicles (100 and 200), the proposed dynamic CFP channel operation algorithm can provide higher throughput on the SCH compared to the static CFP channel operation algorithm while guaranteeing low delays and high delivery rates on CCH. However, when the vehicle density is high (300), the dynamic and static CFP channel operation algorithms provide the same throughput. This is due to the saturation of the total number of time slots that can be used in dynamic CFP.

**VII. CONCLUSION**

In this paper, we proposed a new contention-free broadcast protocol for periodic safety messages in vehicular networks. It is based on a dynamic time slot reservation schedule managed by stable CHs that continually adjust to vehicle dynamics. It provides an efficient utilization of the time slots for the exact number of active vehicles including hidden nodes. Moreover, the overhead is reduced using single reservation request for a periodic medium access during a vehicle’s cluster session. The simulation results show that the proposed protocol can significantly improve the delivery ratio of periodic safety messages while providing a bounded access delay. We also show that a dynamic CFP used in combination with our protocol provides a higher throughput compared to a static CFP. As a future work, a comparison with other existing broadcast protocols other than the standard 802.11p will be performed. Furthermore, an anticipation of time slot reservations for vehicles joining/leaving a cluster can be investigated, since vehicles movements in a highway are predictable to some extent. For instance, the Efficient Neighborhood Prediction Protocol [11] is one of the good examples of prediction protocols that can be used for that purpose.
REFERENCES


