Highway Multihop Broadcast Protocols for Vehicular Networks

[1]Mohssin Barradi, [1]Abdelhakim S. Hafid, [2]Sultan Aljahdali
[1]Network Research Laboratory, University of Montreal, Canada
{mbarradi, ahafid}@iro.umontreal.ca
[2]College of Computers and Information Technology, Taif University, Saudi Arabia
aljahdali@tu.edu.sa

Abstract — IEEE 802.11p Wireless Access in the Vehicular Environment (WAVE) standard is being developed, in order to support Intelligent Transportation System (ITS) applications including safety applications. This includes data exchange between vehicles (V2V), and between vehicles and infrastructure (V2I). Safety applications, e.g., collision and other safety warnings, rely on broadcast communication. Unfortunately, 802.11p does not allow mechanisms such as sending RTS/CTS and acknowledgements for broadcast communication. Therefore, several collisions can be caused by hidden nodes/vehicles. Moreover, the possibility of using the binary exponential back-off technique to reduce congestion is not supported due to the lack of acknowledgements. In this paper, we propose a new 802.11 based Vehicular Multi-hop Broadcast protocol, called Highway Multihop Broadcast (HMB) that addresses the broadcast storm, hidden node, and reliability problems of multi-hop broadcast in VANET. HMB selects the farthest vehicle, with the least speed deviation with respect to the source, to forward and acknowledge broadcast frames. Simulation results show that HMB has a very high success rate in delivering safety messages, and efficient channel utilization when compared with existing broadcast based protocols

Keywords — WAVE *vehicular networks, IEEE 802.11p, Multihop broadcast, IEEE 802.11p, hidden nodes, and storm.*

I. Introduction

The transportation system has a significant impact on the economy and safety of society. Safe, timely and low-cost transportation of people and goods is important for the well-being of commerce, industry, government, educational centers, families, etc. To this end a special electronic device will be placed inside each vehicle which will provide Ad-Hoc Network connectivity for the passengers. Each vehicle equipped with Vehicular Ad-hoc Network (VANET) device will be a node in the Ad-hoc network and can receive and relay messages through the wireless network. Collision warnings, road sign alarms and in-place traffic view will give the driver essential tools to decide the best route to take to his destination.

Because of its size, complexity, and large number of components, the transportation system is extremely difficult to manage and supervise. The need for the development of intelligent systems able to enhance the transportation infrastructure in terms of safety, comfort and efficiency, was understood quite a long time ago. One way to do this is creating a wireless communications network accessible by vehicles on the move, and able to provide them with safety-critical information as well as with a gateway to the global Internet.

In 1999, the FCC allocated 75 MHz of bandwidth in the 5.9 GHz band to create a nationwide VANET. This set of frequencies is known as the Dedicated Short-Range Communications (DSRC) band. Its purpose is to provide vehicle-to-roadside (V2I) as well as vehicle-to-vehicle (V2V) wireless communications; thus, stations on the roadside (roadside units - RSU) and mobile radio units located on board vehicles (on board units - OBU) can share information related to road and traffic conditions and use it to improve the safety and efficiency of the transportation system. The resulting technology is known as WAVE (Wireless Access in Vehicular Environments), which recently has attracted considerable attention from the research community and automotive industry. Many protocols and devices have been proposed for purposes of safety, comfortable driving, and entertainment. The concept includes seven radio channels within the DSRC band. One of them is known as the Control Channel (CCH) and the remaining six are known as Service Channels (SCH). The CCH is the channel that road safety relies on, since all safety-related messages are exchanged using it. Service channels, on the other hand, are reserved for non-safety-related connections (e.g. to look for nearby hotels, to download a map or to check e-mail) and their goal is to allow people in vehicles to maintain access to the Internet.

In WAVE, safety messages are broadcasted on the CCH. A CCH classifier is in charge of sorting packets into four access categories AC[i] ($0 \leq i \leq 3$), each having a separate queue identified by their indexes. The authors in [1] present an example of each access category in the CCH: (1) AC[3] concerns emergency information from the Road Side Unit (RSU) (i.e. accidents, obstacles, slippery conditions or missing traffic signs, etc.) and information generated by cars (vehicle with malfunctioning brakes, or speeding over a certain limit, etc.); (2) AC[2] concerns presence and speed information advertised by vehicles; (3) AC[1] concerns information sent by vehicles asking for help when they pose no risk to other vehicles (e.g. when they overheat or run out of gas); and (4) AC[0] concerns information aimed at establishing new non-safety-related connections over the service channels. All these messages are broadcasted through the control channel (CCH). The MAC protocol currently adopted for vehicular networks, namely Enhanced Distributed Channel Access (EDCA), described in the IEEE 802.11 standard, does not implement a strict priority for safety messages on CCH, but only enforces service differentiation among the different types of messages.

To propagate safety messages beyond the transmission range, a vehicular network uses Multihop Broadcast protocols. Unfortunately, few of the proposed multi-hop broadcast protocols give a complete solution to Multihop broadcast communication problems, such as interference, packet collisions, reliability, and hidden node problem, which can stop the message dissemination during multi-hop broadcast. Moreover, some of the proposed multi-hop broadcast protocols (e.g., simple-flooding, probabilistic rebroadcast [3], Clustering-based Multihop broadcast [4], MCDS-based broadcast [5], Area–based Multihop broadcast [6] and Distance–based Multihop broadcast [7]) are very harmful for wireless resources, because of unnecessary retransmissions, and thus overload the network. These facts increase the need for a novel Multihop broadcast protocol based on MAC layer design for efficient and reliable broadcast dissemination, especially on highways where the speeds are very high and the density can be very low. We can conclude that vehicular networks suffer from the lack of a MAC protocol with the capabilities to (1) establish a strict priority, needed for adequate support of safety messages; (2) prevent hidden node problem and solve the problem of collisions in wireless communication; (3) acknowledge safety messages that are broadcasted on CCH with free overhead in order to make the use of binary-exponential back-off technique possible; and (4) minimise the redundancy in order to gain in terms of time and resources needed by emergency messages.

In this paper, we propose a novel Multihop broadcast protocol for ad-hoc vehicular networks, called HMB. Based on IEEE 802.11, HMB establishes a strict priority for safety messages, and provides a complete solution to multi-hop broadcast communication problems, such as broadcast storm, hidden node, and reliability problems. HMB makes use of a mechanism similar to RTS-CTS (Figure 1) to prevent hidden node problem, and passive acknowledgements to support reliability while minimizing overhead. In HMB, vehicles make their own decision to forward and acknowledge received packets without the need of any topology information. The decision to forward or not is based on the distance from the source, received signal strength indicator (RSSI) of received messages, the speed deviation between sender and forwarder, and the priority of received messages. The performance of HMB is analyzed through simulation

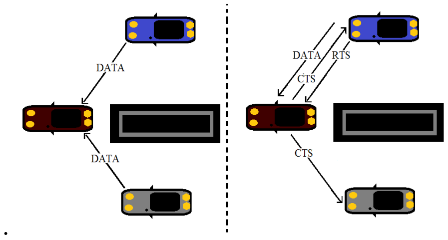

Figure 1. RTS CTS handshake.

The remainder of this paper is organized as follows: Section 2 describes details of the proposed Multihop broadcast protocol (HMB). Section 3 evaluates HMB via simulations. Finally, Section 4 concludes the paper.

II. PROTOCOL DESCRIPTION

HMB aims at supporting QoS for timely delivery of safety messages over V2V and V2I-based VANET. It supports high reliability and strict priority for safety messages broadcasted in CCH and prevents collisions due to hidden node problem while avoiding storm problems and minimizing overhead.

FSD	Direction
00	South
01	North
10	East
11	West

Table I. Direction Converter

V’: speed	V: speed (Km/h)
0	0-60
1	60-80
2	80-100
3	100-+

Table II. Speed Converter

HMB is composed of four rounds: Initial Clear-To-Broadcast, Forwarded-Clear-To-Broadcast, sending data, and forwarding data; Figure 2 shows the HMB rounds. When OBU1 wants to broadcast a safety message (priority i), it generates Initial Clear to Broadcast (ICTB); OBU2 responds with Forwarded Clear to Broadcast (FCTB); after receiving FCTB, OBU1 starts sending data, and OBU3 must stop broadcasting all messages with priority smaller than i until receiving data; when OBU2 receives data, it forwards it. OBU can request permission to send a message of priority higher than i, by sending ICTB. In this case, OBU2 must start another round according to the last priority. We assume that each vehicle is equipped with an electronic map, has a unique MAC-ID, and every frame has an ID chosen randomly. We propose to add four bits in the MAC sub-layer header of all outgoing frames; two bits to represent Frame Sender State (FSS) and the two last bits are for Frame Sender Direction (FSD); see Table I. Thus, each received frame includes an I.D, the original sender I.D. (i.e., frame source id), the state, the direction, the speed (V’) according to Table II, and the position of the last sender.

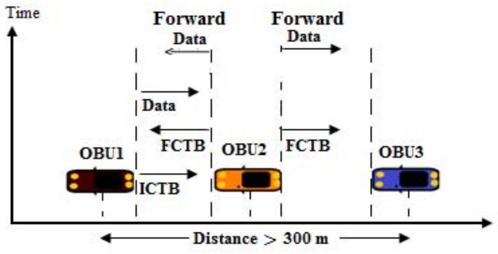

Figure 2. HMB

A. DIRECTIONAL FORWARD AND PASSIVE FORWARDER SELECTION

In this subsection, we describe the approach used by HMB, to select a forwarder without the knowledge of the network topology. OBU x processes only frames sent by another OBU or RSU in front of it and moving in the same direction. A vehicle can be in the four states: Master Repeater (MR), Repeater Ready (RR), Repeater (RP), or Ordinary vehicle (OV). FSS takes the value 00 if the frame is sent by an OV, 01 if the frame is sent by a RP and 10 if the frame is sent by a MR. A MR is the farthest vehicle that can still receive frames from an OV or a RP. A RP is a vehicle that can communicate with multiple MRs. An OV is a vehicle that is neither a MR nor a RP. A RR is a vehicle that has not heard from MRs or RPs, and is ready to forward a received message; these last two states are temporary.

The basic idea behind Passive Forwarder Selection Technique (PFST) is to divide the transmission range into n areas Ai ($1 \leq i \leq n$) according to the distance d from the frame sender. In this paper, n assumes 6 (see Figure 3); the impact of the value of n on the performance of HMB is planned for future work. Nodes in area Ai have the same probability to be MR. PFST allows all vehicles in transmission range of the frame sender to be ready as forwarders. When receiving a frame for the first time, an OV becomes a RR, and starts a timer (T); when T expires, RR forwards the frame. In the case where there are no MRs and no RPs already present in the coverage area of the frame sender, the first RR in $A1 \leq i \leq 6$ that successfully forwards the frame becomes a MR; thus, there is no need to restart the process of selection; this allows gaining precious time for safety messages/applications. The operation of PFST takes into account the distance between the frame sender and neighbours in the coverage area, the received signal strength indicator (RSSI) of the received frame, the priority of the received frame, the speed deviation between the frame sender and the frame receivers, and the direction of the frame sender.

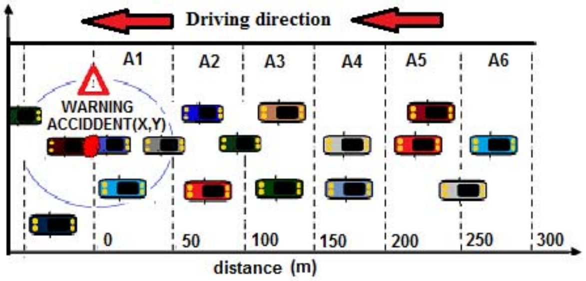

Figure 3. Area classification according to the distance

Vehicles in area Ai, with the same RSSI and speed deviation, have the privilege to start retransmission before the vehicles in A_{i-1}. When receiving a frame for the first time, an OV changes its state to RR, saves the frame, and starts a timer T; when the timer expires, RR forwards the frame. T is defined as follows:

$$\mathbf{T = T1 + T2 + T3 + T4} \qquad (1)$$

$$\mathbf{T1 = MAX\left(0, \left(6 - \left\lfloor \frac{d}{50} \right\rfloor\right)\right) * SlotTime} \qquad (2)$$

$$\mathbf{T2 = \left\lfloor \frac{RSSI}{CSThresh} - 1 \right\rfloor * SlotTime} \qquad (3)$$

$$\mathbf{T3 = |\, V's - V'r \,| \;\; * SlotTime} \qquad (4)$$

$$\mathbf{T4 \;=\; (3 - PRIO) * SlotTime} \qquad (5)$$

where Slot Time is the length of one slot, T1 (see Equation (2)) is a waiting time that is a function of the distance between the current node and last frame sender; T2 (see Equation (3)) is a waiting time that is a function of the received signal strength indicator of the received message; CSThresh is the minimum acceptable RSSI; T3 (see Equation (4)) represents the speed deviation (ΔV') between frame senders and the current node; T4 (see Equation (5)) is a waiting time that is a function of the priority of the received message (i.e., *PRIO* (AC[i]) $_{0 \leq i \leq 3}$ = i). Note that T4 allows for high priority messages to be forwarded before lower ones. MRs must wait, before forwarding, only for T4 after receiving frames (i.e. $T_{MR} = T_4$). Distance and RSSI, are strongly correlated; however, considering both of them in Equation (1) minimizes the probability of simultaneous forward and enhances the chance of MR and RP to forward first.

B. HANDSHAKE AND PASSIVE ACKNOWLEGEMENT

In the 802.11, RTS/CTS handshake is the widely used technique to prevent hidden node problem in wireless communications to achieve high throughput. The sender can send an RTS message to ask whether the receiver is not involved in any another communication. If the receiver is listening, it will answer with a CTS message telling nodes in its communication range that it is waiting for data from the requesting node. This will result in other prospective senders being informed that this node will get data from another node. This mechanism is not feasible in broadcast communications since broadcasted frame have more than one destination. Some protocols [8] use the topology information to directly select the nodes which will send CTS and ACK frames. However, in VANETs, the large number of nodes and high mobility make such pro-active approaches impractical. Thus, the 802.11 Medium Access Control (MAC) provides no means to solve hidden node problem.

To avoid hidden node problem and maximize the reliability of safety messages, while preventing storm problem, we propose that the sender engages in handshake. Only MRs and RPs can respond, forward, or acknowledge the received frame; the other vehicles can overhear the transmission as well. To select MRs and RPs, the protocol divides the road portion inside the transmission range of the frame sender into segments without any knowledge of the network topology. PFST allows an OBU to decide whether it must forward received messages or not according to its state (MRs or RPs) as explained in Section II-A.

Before broadcasting a safety frame, OBU x must broadcast an ICTB frame with a Time To Live (TTL) equal to two; the ICTB frame must include the frame information (I.D., Priority, Original MAC ID) and last frame sender information (FSS, FSD, coordinates, speed). When receiving

ICTB frame, the MR or PR which is located in the coverage area behind x, and traveling in the same direction of x, updates the last sender information of this frame (FSS, FSD, coordinates, speed) and forwards it to all neighbours. After receiving FCTB frame, all OBUs except x must stop broadcasting, and x can start sending the data frame(s). If collision occurs among ICTB frames, retransmissions are performed with an extra random time (between 1 to 4 Slot Time) to prevent the same collision situation. Figure 4 shows the sequence of ICTB and FCTB handshake frames.

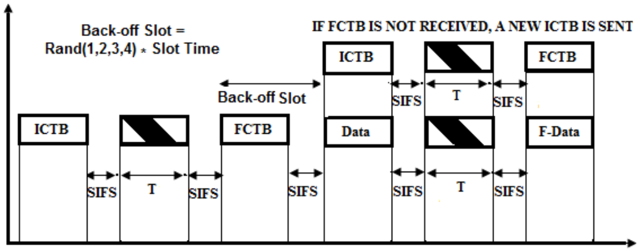

Figure 4. Sequence of ICTB FCTB handshake.

The use of acknowledgement (ACK) in 802.11 allows a frame sender to know about the successful reception of its frame, and gives it the possibility to retransmit when it fails. Unfortunately, this mechanism is not feasible in broadcasting systems, since broadcast frames have more than one destination, and acknowledging broadcasted data can be very harmful to the network and leads to what we call storm problem around the source. Indeed, 802.11 MAC provides no reliability for broadcast traffic; in this paper, we propose a very simple and effective solution, called passive acknowledgment, to overcome this limitation. As mentioned above, every frame is triple-identified by its I.D., original MAC I.D., and the last sender I.D. When forwarding, MRs and RPs update only last-sender information in forwarded frames. Therefore, there is no need to send an ACK frame since the frame sender is in the coverage area of the MR or RP (that forwards the frame). Indeed, the forwarded frame is also heard by the sender; this is represents an implicit acknowledgement since the frame sent by the sender and the frame forwarded by MR/PR have the same ID. If the frame sender does not hear/receive the forwarded frame (i.e. a collusion happened) , it increments its back-off counter and try to send again.

III. SIMULATIONS AND RESULTS

A. *SIMULATION ENVIRONMENT*

The simulations were carried out using ns-2.34. Each simulation lasts for 100 seconds, and is repeated thirty times. We generated a scenario of a highway in a grid of 4000m × 100m, with up to 400 vehicles turning around the grid as shown in Figure 5 (100 vehicles moving at 60km/h, 140 vehicles at 80km/h, and 160 vehicles moving at 100km/h). All vehicles use the setting of 802.11a at 6Mbps for the physical layer. We built our implementation based on the last draft of 802.11p. We compared the performance of HMB protocol to probabilistic rebroadcast protocol, and UMB which is the same in the highway scenario as distance-based 802.11 [2]. We choose randomly 10% of nodes to generate frames of high priority (AC[3] frames), and 90% of nodes to generate low priority frames(AC[i] 1≤i≤2 frames). We vary the average frame generation rate of each vehicle (λ) from 10 to 200 (frame/s).

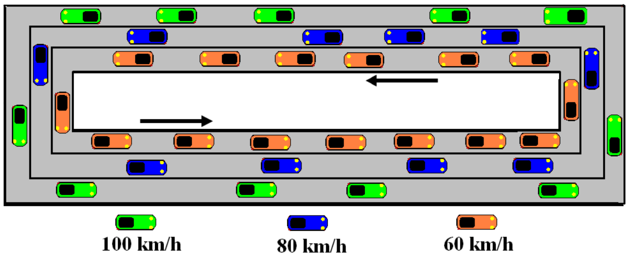

Figure 5. Simulation topology

B. *Simulation Metrics*

In our simulations, we consider the following metrics:

- Redundancy Factor: the ratio between the number of nodes that forwarded a frame, and the total number of nodes that received this frame. This metric is considered to show the improvement that HMB achieves regarding the broadcast storm problem.
- Reliability Factor: the ratio between the number of nodes that received the broadcasted frame and the total number of nodes in the observed area. This metric is considered to show the improvement that HMB achieves regarding the successful delivery of safety frames

C. *RESULTS*

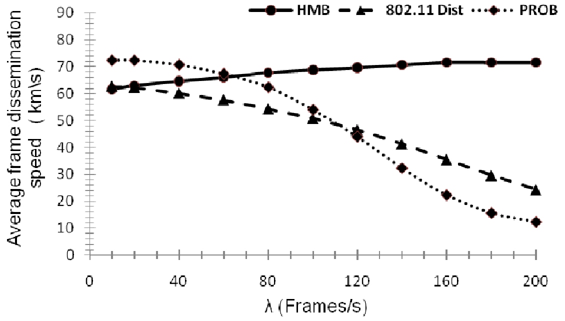

Figure 6. Frame dissemination speed of higher priority frames (AC[3]).

Figure 6 shows that with probabilistic and distance-based 802.11 protocol [2] the frame dissemination speed of highest-priority (AC[3]) frames decreases when the average frame generation rate increases; however, with HMB the frame dissemination speed of highest-priority frames increases with the traffic load. This can be explained by the fact that in high traffic load, exchanges of frames increase and thus MRs and RPs become more stable; this stability allows decreasing the total amount of time required to forward frames. It is important to mention that HMB provides highest priority frames a higher speed delivery even in high traffic load.

Figure 6 shows also that the probabilistic broadcast protocol provides slightly high dissemination speed when the traffic load is light (smaller than 60 frames per second); this can be explained by the fact that the number of collisions is small (light traffic load) and that OBUs, using probabilistic broadcast protocol, forward received frames without any waiting time (in opposition to the two other protocols)

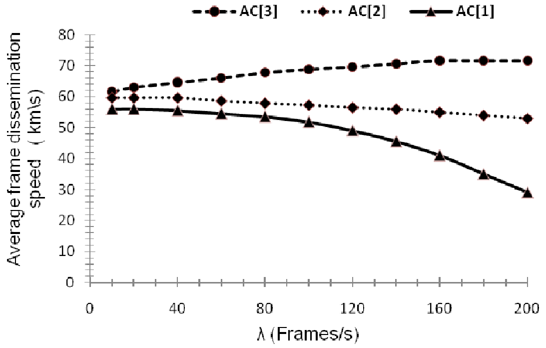

Figure 7. Frame dissemination speed, using HMB, of different priority frames.

Figure 7 shows that the dissemination speed, using HMB, of AC[3] frames increases (and becomes stable) with traffic load. On the other hand, we observe that the dissemination speed of AC[2] and AC[1] frames decreases when traffic load increases, especially for AC[1] frames. This decrease is the price paid in order to allow high-priority frames to reach destinations quickly; we believe it is a small price to pay to guarantee a speedy delivery of critical safety messages; lower priority frames can tolerate longer delays since they are not related to emergency situations.

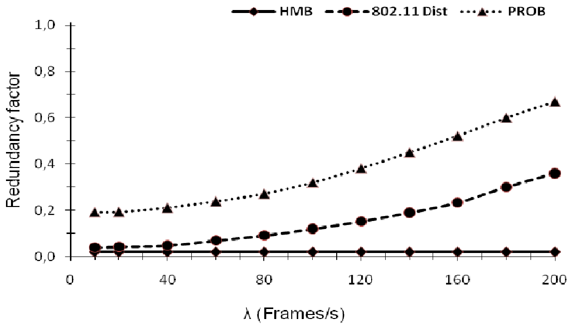

Figure 8. Redundancy factor.

Figure 8 shows that the Redundancy Factor, when using HMB, remains low even in the case of high traffic load. We can say that HMB generates a minimum overhead allowing a high delivery of safety frames and efficient use of the network. This is the result of using a directional broadcast and passively selecting forwarders.

Figure 9 shows that, in high mobility and traffic load, the reliability of safety frames is very low when using probabilistic or 802.11-based distance protocols; the reliability decreases severely when traffic load increases. In opposition, we observe that HMB provides high reliability independently from the traffic load; this is key requirement, in vehicular networks, to support emergency/safety applications. The high degree of reliability achieved by HMB can be explained by the fact that hidden nodes and redundancy (eliminated by HMB) cause many collisions, especially in the case of high mobility and traffic load.; the passive acknowledgement allows HMB to retransmit only the frames that are lost without any extra overhead.

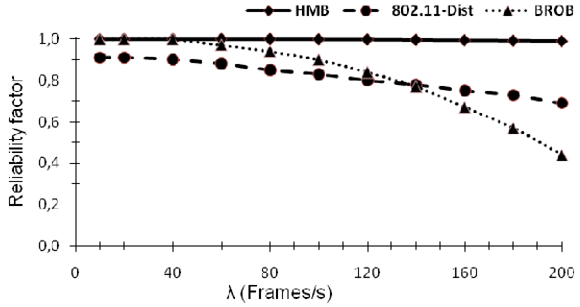

Figure 9. Reliability factor .

IV. CONCLUSION

We propose a novel multi-hop broadcast protocol that is very simple to implement on top of 802.11p; it provides solutions to (1) hidden node problem by introducing ICTB FCTB handshake; (2) storm problem by passive forwarder selection; and (3) reliability by using passive acknowledgement; this allows a sender to know whether the frame it did send, was successfully received and, if not, to retransmit the frame using the binary exponential back-off technique, thus increasing the probability of success. Our simulation results show the effectiveness of the proposed HMB in reducing redundancy, enhancing the delivery delay (in a differentiated way based on the priority of the frame) and increasing the reliability for safety messages even in the case of high-traffic load.

References

[1] M. Barradi, A. Hafid and J.R. Gallardo, “Establishing Strict Priorities in IEEE 802.11p WAVE Vehicular Networks,” IEEE Globecom, 2010

[2] L. Briesemeister and G. Hommel, “Role-based multicast in highly mobile but sparsely connected ad hoc networks,” IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), 2000.

[3] S. Ni, Y. Tseng, Y. Chen, J. Sheu, “The broadcast storm problem in a mobile ad hoc network,” ACM/IEEE MOBICOM, 1999..

[4] J.Y. Yu and P.H.J. Chong, “A survey of clustering schemes for mobile ad hoc networks,” IEEE Communication Survey and Tutorial, vol. 7, no. 1, pp. 32–48, January 2005.

[5] A. Zanella and G. Pierobon and S. Merlin, “On the limiting performance of broadcast algorithms over unidimensional ad-hoc radio networks,” WPMC’04, 2004.

[6] J L. Briesemeister, L. Schäfers, and G. Hommel, “Disseminating messages among highly mobile hosts based on inter-vehicle communication,” IEEE Intelligent Vehicles Symposium, 2000.

[7] G. Korkmaz, E. Ekici, F. Ozguner, and U. Ozguner, “Urban multi-hop broadcast protocol for inter–vehicle communication systems,” ACM workshop on Vehicular ad hoc networks, 2004.

[8] M.-T. Sun, L. Huang, A. Arora, and T.-H. Lai, “Reliable MAC layer multicast in IEEE 802.11 wireless networks," International Conference on Parallel Processing, 2002.