An Enhanced Multi-channel MAC for Vehicular Ad Hoc Networks

Duc Ngoc Minh Dang*, Hanh Ngoc Dang†, Cuong The Do* and Choong Seon Hong*
*Department of Computer Engineering, Kyung Hee University, 446-701, Korea
†Department of Telecommunications Engineering, Ho Chi Minh City University of Technology, Vietnam
dnmduc@khu.ac.kr, hanhdn@hcmut.edu.vn, dtcuong@khu.ac.kr and cshong@khu.ac.kr

***Abstract*—The IEEE 1609.4 [1] is a MAC extension of IEEE 802.11p [2] to support multi-channel operations. However, the IEEE 1609.4 does not allow nodes to exchange non-safety messages during the CCH interval. This paper proposes a Vehicular Enhanced Multi-channel MAC protocol (VEMMAC) for Vehicular Ad hoc Networks (VANETs). The VEMMAC adopts the IEEE 1609.4 with alternating sequences of the Control Channel (CCH) interval and the Service Channel (SCH) interval. Different from the IEEE 1609.4, the VEMMAC allows nodes to transmit non-safety messages during CCH interval and broadcast safety messages twice with each in the CCH and SCH interval. Our proposal can utilize the channel resources more efficiently than the IEEE 1609.4. The simulation results show that the proposed VEMMAC protocol achieves higher throughput for service data and is more reliable for safety messages broadcast than other protocols.**

***Index Terms*—Multi-channel, MAC protocol, Vehicular Ad Hoc Networks, VANETs.**

I. Introduction

Vehicular ad hoc networks (VANETs) have been considered to be an important part of the Intelligent Transportation System (ITS). The VANETs focus on Vehicle-to-Vehicle (V2V) communications and Vehicle-to-Infrastructure (V2I) communications. The US Federal Communication Commission allocated 75 MHz of the spectrum in the 5.9 GHz band for Dedicated Short Range Communication (DSRC). As shown in Fig. 1, the overall bandwidth is divided into seven frequency channels. One control channel (CCH), i.e. CH 178, can only be used to send safety relevant applications, system control and management with high priorities. The other six service channels (SCHs) are mainly used to support non-safety relevant applications.

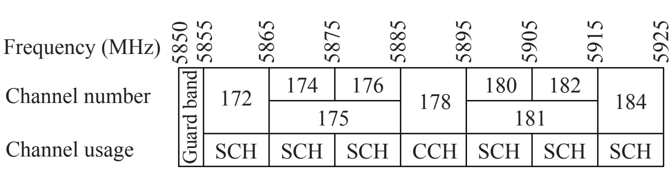

Fig. 1. Channel access scheme for WAVE system.

The applications of VANETs fall into two categories, namely safety applications and non-safety applications. Safety applications, providing drivers information about critical situation in advance, have strict requirements on communication reliability and delay. On the other hand, non-safety applications are used for improving driving comfort and the efficiency of transportation system which are more throughput-sensitive instead of delay-sensitive. Safety messages have higher priority than non-safety messages. The requirements for different applications are shown in Table. I.

Different multi-channel MAC protocols have been proposed for wireless ad hoc networks. In Dynamic Channel Access (DCA)[4], nodes have two transceivers: one is on the control channel, and another can switch to any other data channels. This scheme does not require the time synchronization, but it may suffer the bottleneck on the control channel if the ratio of the control message transmission duration and the data transmission duration is not chosen properly. Multi-channel MAC (MMAC) [5] and Hybrid Multi-channel MAC (H-MMAC) [6] adopt the Power Saving Mechanism of IEEE 802.11 (IEEE 802.11 PSM) in which time is divided into beacons. Each beacon has an Ad hoc Traffic Indication Message (ATIM) window followed by a data window. Nodes exchange control messages during the ATIM window, and switch to agreed data channels for data transmissions. The data transmission duration is extended to the next ATIM window in H-MMAC protocol in order to fully utilize the data channel resources.

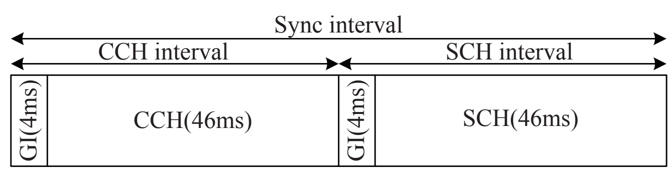

Fig. 2. Frequency channel layout of a 5.9 GHz WAVE system.

Wireless Access in Vehicular Environment (WAVE) is designed for an ITS on 5.9 GHz frequency with the IEEE 802.11p and IEEE 1609 standard family. The IEEE 802.11p standard is set for both the physical and the medium access control layer of DSRC. The IEEE 1609.4 is the standard of the multi-channel operation for WAVE MAC. As shown in Fig. 2, the channel access time is divided into sync interval of 100 ms. Each 100 ms sync interval allocates 50 ms for the CCH interval and 50 ms for the SCH interval, including 4 ms guard interval (GI) for switching between CCH and SCH. All nodes have to tune to CCH during the CCH interval for exchanging safety messages and other control messages. During the SCH

TABLE I
DSRC APPLICATION REQUIREMENTS [3]

Applications	Packet size/Bandwidth	Latency (ms)	Network Data Type	Application Range (m)	Priority
Intersection Collision Warning/Avoidance	100 bytes	100	Event	300	Safety of life
Cooperation Collision Warning	100 bytes/10 Kbps	100	Periodic	50-300	Safety of life
Work Zone Warning	100 bytes/1 Kbps	1000	Periodic	300	Safety
Transit Vehicle Signal Priority	100 bytes	1000	Event	300-1000	Safety
Toll Collections	100 bytes	50	Event	15	Non-Safety
Service Announcements	100 bytes/2 Kbps	500	Periodic	0-90	Non-safety
Movie Download (2 hours of MPEG 1)	>20Mbps	NA	NA	0-90	Non-Safety

interval, nodes can optionally switch to SCHs to exchange non-safety application data. This channel access scheme has the high contention during the CCH interval, and the service channels cannot be utilized during this interval. That means a half of channel resources is wasted in the CCH interval.

The variable CCH interval (VCI) multi-channel MAC scheme, which can dynamically adjust the duration of the CCH interval, is proposed in [7]. The CCH interval is further divided into the safety interval and WAVE Service Announcement (WSA) interval. Nodes broadcast safety messages and VCI packets during the safety interval. During the WSA interval, service providers and service users exchange WSA/Acknowledgement(ACK) or Request for Service(RFS)/ACK. After the end of the CCH interval, nodes switch to certain SCHs to transmit service packets. This scheme tries to improve the saturation throughput of service data and to provide the reliable transmission for safety messages. However, the service channel resources are still wasted during the CCH interval.

Different from above synchronous schemes, an Asynchronous Multi-channel MAC (AMCMAC) is proposed in [8]. Nodes make rendezvous with their receivers or broadcast safety messages on the control channel while the other nodes are exchanging non-safety messages on the service channels. Like DCA, AMCMAC may have the congestion on the control channel when the network load is high. AMCMAC is improved by applying the distributed TDMA (DTDMA) mechanism in [9]. DTDMA reduces the high contention level on the control channel and enhances the service differentiation.

Dedicated Multi-channel MAC (DMMAC) [10] employs the hybrid channel access to provide collision-free and delay-bounded transmission for safety messages. A clustering-based multi-channel MAC protocol is proposed in [11]. Each node has two transceivers which can operate simultaneously on different channels. The cluster head uses one transceiver to collect and deliver emergency messages and control messages within its cluster, and uses another transceiver to exchange consolidated safety messages among cluster head. A proposal in [12] is a VANET Multi-channel MAC (VMMAC) with using directional antenna to improve the spatial reuse.

The multi-channel MAC design for VANET is not only ensure the reliability of safety message transmission, but also provide the high throughput for non-safety data transmission. The Enhanced Multi-channel MAC, named VEMMAC, is proposed to improve the saturation throughput while guaranteeing the safety message broadcast reliability. Similar to the H-MMAC [6] which is proposed for wireless ad hoc network, the VEMMAC allows nodes to extend their non-safety message transmissions to the upcoming CCH interval according to the network load. And the safety message is retransmitted in the next interval for some nodes which are on the service channels in current interval. This helps to increase the broadcast efficiency of safety message transmissions.

The rest of this paper is organized as follows. In section II, our proposed protocol is described in details. Section III presents simulation results. Finally, we conclude this paper in section IV.

II. THE PROPOSED VEMMAC PROTOCOL

First, we assume that a node is equipped with a half-duplex transceiver which is capable of switching the channel dynamically. It can either transmit or listen but cannot do both simultaneously. Like the IEEE 1609.4, all nodes are time-synchronized. Time is divided into sync interval with the CCH interval and the SCH interval. Nodes have two transmission modes: Normal Transmission (N-Tx) which is the transmission performed within the SCH interval and Extended Transmission (E-Tx) which is the transmission performed in SCH interval and the upcoming CCH interval. There is only N-Tx mode for nodes which selected the control channel to exchange their data packets during SCH interval.

Fig. 3 shows the operation of VEMMAC protocol. For the non-safety message transmissions, nodes tries to access the control channel to reserve one of service channels by exchanging SCH-REQ/SCH-ACK/SCH-RES messages (the SCH messages for short) only during the CCH interval. For the safety messages, whenever a node wants to broadcast, it has to switch to the CCH channel and contends the control channel to broadcast a safety message in the current interval (CCH or SCH interval). Then, it attempts to broadcast the safety message again in the next interval because some nodes, which use E-Tx transmission mode, cannot receive the safety message before. In the Fig. 3, some nodes exchange the SCH messages to reserve service channels in the first sync interval. Nodes A and B use N-Tx mode while nodes C and D use E-Tx mode. In the second sync interval, assume that node X broadcasts a safety message (SMsg1). However, only nodes which are on the control channel can receive this safety message successfully. The others like nodes C, D, E and F miss this safety message. After the CCH interval, nodes C, D, E and F are on the control channel. So, node X has to broadcast the safety message again in the SCH interval if this safety

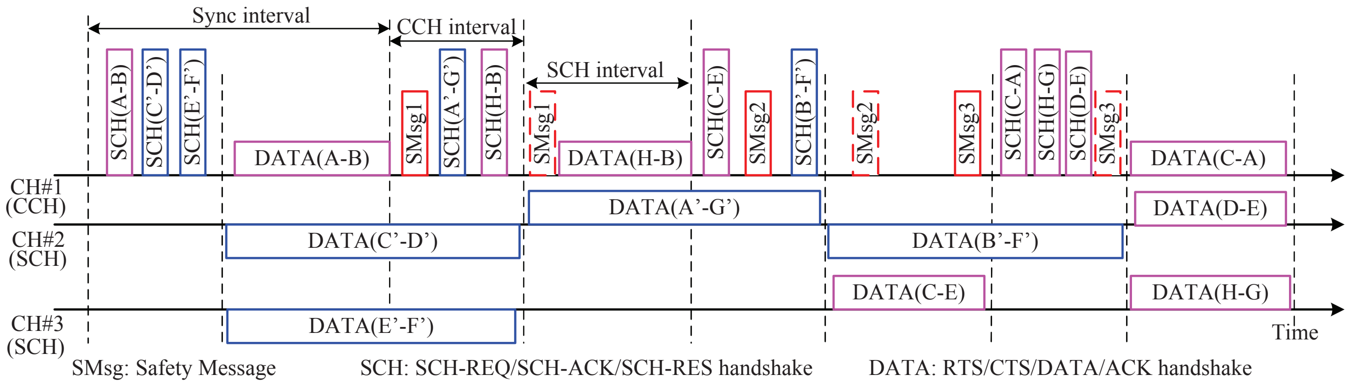

Fig. 3. The operation of VEMMAC protocol.

message is still valid. Similarly, if a node broadcasts a safety message (SMsg3) in the SCH interval, it has to broadcast the safety message again in the next CCH interval.

Since every safety message is broadcast twice, the number of channel contention for safety message broadcast is doubled compared to the IEEE 1609.4. However, in the dense network, node has to contend with all nodes during the CCH interval to broadcast a safety message in the IEEE 1609.4. In VEMMAC, during the CCH or SCH interval, not all nodes are on the control channel, the successful probability of broadcasting safety message is higher than that of IEEE 1609.4. Moreover, each safety message is broadcast twice, it increases the reliability of safety message transmission. Another benefit of VEMMAC is that it utilizes all channels during the CCH interval, the throughput is increased significantly compared to the IEEE 1609.4. Next, in order to keep track the status of neighbor nodes and channels, we define two data structures named Neighbor Information List and Channel Usage List.

TABLE II
NODE A'S NIL

Node	Channel	Tx_mode	Next_CCH
B	1	N-Tx	1
C	2	E-Tx	2
D	2	E-Tx	2
E	3	E-Tx	2
...	...	...	...

A. Neighbor Information List (NIL)

The NIL maintains the information of the neighbor nodes as shown in Table II. The channel indicates which channel the node uses to exchange non-safety messages. Channel 0 means that node does not have any non-safety message to send, and this node will be on the control channel during the SCH interval. Tx_mode has either N-Tx or E-Tx mode. Next_CCH means after how many sync intervals the corresponding node will be on the control channel. The node which uses the N-Tx will be on the control channel after 1 sync interval while the node which uses E-Tx will be on the control channel after 2 sync intervals. The Next_CCH is updated with value of 1 for N-Tx mode or 2 for E-Tx mode.

Each node has to keep the NIL updated in order to exchange data. At the beginning of each sync interval, it decreases the Next_CCH value by 1 in its NIL. If a node is on service channel for data transmissions, it will miss all messages exchanged in the current CCH interval on the control channel. Therefore, it assumes that the nodes are on the control channel will use E-Tx mode and updates the zero Next_CCH to 2 in its NIL. Whenever node overhears SCH messages on the control channel during the CCH interval, it updates its NIL.

B. Channel Usage List (CUL)

The CUL stores the information of channel as shown in Table III. For simplicity, we number the channel from 1 to 7 for a control channel and six service channels. The State of each channel in the CUL is either in the Selected or Not_Selected state. The Selected channel means that this service channel has already been chosen by the node for use in the current sync interval; otherwise, it is a Not_Selected channel, so at most one channel can be Selected at each node for each sync interval. The counter of a channel shows how many node pairs have already reserved that channel.

TABLE III
NODE A'S CUL

Channel	State	Counter
1	Not_Selected	1
2	Selected	1
3	Not_Selected	0
...	...	...

When a node has non-safety massages to send, it has to negotiate with its receiver which channel the data transmission will be taken place. They try to select the ”best” service channel for their data transmissions by Algorithm 1. The ”best” channel is the channel which has the least counter.

We already defined two transmission modes, and now we discuss the criterion which node used to trigger the E-Tx mode. When the network load is low and node uses the E-Tx mode, it can only start its transmission after 2 sync intervals. That means the delay will be high. In case of high network load, nodes have to use the E-Tx mode obviously. The network

Algorithm 1 Algorithm to select the "best" channel

if There is a Selected channel in the receiver's CUL **then**
  This channel is selected.
else if There is a Selected channel in the sender's CUL **then**
  This channel is selected.
else
  The channel with the least counter value is selected.
end if

traffic load depends on the number of nodes that want to exchange data and the number of data packets that they are going to exchange. The number of nodes that use E-Tx mode should be limited.

C. The operation of VEMMAC protocol

The node and its receiver must be on the control channel in order to exchange the SCH messages to reserve the service channel for their non-safety message transmissions.

1) Whenever a node has a safety message to broadcast, it contends the control channel to broadcast in the current CCH or SCH interval. Then, it tries to broadcast again in the next SCH or CCH interval.
2) When a node has non-safety messages to send, it checks the receiver's Next_CCH value in its NIL. If the receiver's Next_CCH is not zero, it has to wait for the next sync interval and try again.
3) The sender checks the receiver's channel in its NIL and its channel from its CUL. If the receiver's channel in NIL and the Selected channels of the sender in CUL (if any) are different, the sender also has to wait for the next sync interval.
4) Based on the traffic load, the sender decides which transmission mode is going to be used.
5) The sender attaches its CUL and transmission mode to the SCH-REQ packet and sends it to the receiver.
6) Upon receiving the SCH-REQ, the receiver selects the "best" channel from its CUL and the sender's CUL by using Algorithm 1. Then, the receiver sends SCH-ACK indicating the selected channel to the sender.
7) The sender sends SCH-RES to confirm the service channel selected by the receiver.
8) Neighbor nodes, which overhear SCH-ACK or SCH-RES messages, update their NILs and CULs.
9) After the CCH interval, the sender and receiver switch to the agreed service channel and start their data transmissions.

III. Performance Evaluation

In this section, we perform the simulations of the IEEE 1609.4 [1], AMCMAC [9] and our proposed VEMMAC protocol on our developed packet-level simulation tool in Matlab.

Each node can have a random location, and can be a source or a destination. There are 10 nodes where each node generates the safety messages (SMsg) with the constant packet arrival rate of 20 packets/second. And there are 40 nodes which generate and transmit non-safety traffic. Since the safety message has the strict delay, we consider the highest priority safety message with 100 byte packet size and 100 ms latency (Table I) in our simulations. That means we set 100 ms time-out for the safety message. When the safety message is generated, node has to contend the control channel and broadcast the safety message within 100 ms, otherwise this safety message is dropped. The other simulation parameters in our simulations are listed in Table IV. Each simulation was performed for 10 seconds, and the simulation results are the average of 20 runs.

TABLE IV
Simulation Parameters

Parameters	Value
Number of nodes	10 + 40 nodes
Data rate	6 Mbps
Safety / Non-safety packet size	100 bytes / 1024 bytes
Safety message time-out	100 ms
AIFS[Safety]/AIFS[Non-safety]	2 / 9
Safety: CW(min:max)	(3:7) time slots
Non-safety: CW(min:max)	(7:1023) time slots
SIFS / DIFS / Slot time	16 μs / 34 μs / 9 μs
SCH-REQ / SCH-ACK / SCH-RES	27 bytes / 16 bytes /16 bytes
Retry limit	7

In the simulation, we use the following metrics to evaluate the performance

1) The aggregate throughput (Mbps) of non-safety traffic.
2) The average delay (msec) of non-safety traffic.
3) The safety message broadcast efficiency (nodes/SMsg): the average number of nodes can receive a safety message successfully.

Fig. 4 shows the performance comparisons of different protocols as the packet arrival rate of non-safety message increases. Since the IEEE 1609.4 allows nodes to exchange non-safety messages only during the SCH interval (a half of sync interval), six service channels are not utilized during the CCH interval. Therefore, the aggregate throughput is lower than that of others as shown in Fig. 4(a). Less non-safety message transmissions leads to high average delay when the packet arrival rate increases. The AMCMAC uses one control channel for broadcasting safety messages and doing RTS-CTS handshake. The other six service channels are used to transmit non-safety messages. Although, the AMCMAC has a higher aggregate throughput than the IEEE 1609.4, it suffers the congestion on the control channel. The service channel utilization of AMCMAC depends on the combination of data rates for CCH and SCH. Different from the IEEE 1609.4, the VEMMAC fully utilizes all service channels during both the CCH and SCH interval. The 50 ms CCH interval is long enough for nodes to negotiate all the service channels for non-safety message transmissions. The aggregate throughput of the VEMMAC is almost twice as high as that of the IEEE 1609.4. In both the IEEE 1609.4 and AMCMAC, when the network goes near saturation, the average delay increases suddenly. In the VEMMAC, we limit the number nodes which can transmit

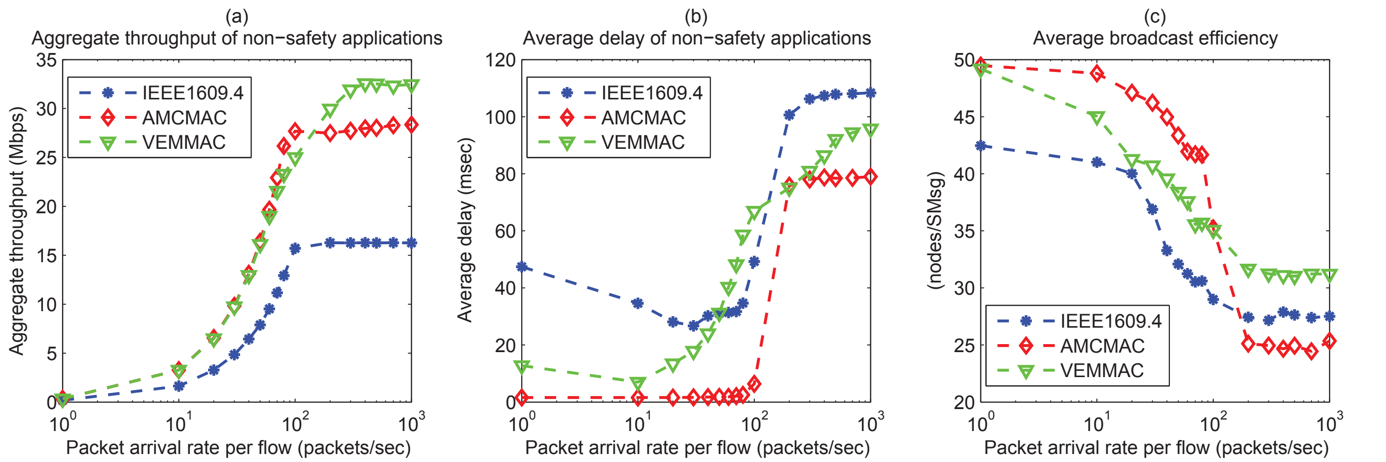

Fig. 4. Performance comparisons of different protocols.

non-safety messages on the control channel during the SCH interval to give more chance for nodes to broadcast safety messages. So, a node just has to contend the control channel if a node has a safety messages to send. On the other hand, if nodes, which are on the control channel during the SCH interval, have non-safety messages to send, they may wait for the next CCH interval to negotiate the service channel for their non-safety message transmissions. That is why the average delay of the VEMMAC is little bit higher than that of the AMCMAC.

Fig. 4(c) shows the safety message broadcast efficiency of different protocols. The safety message is broadcast twice in the VEMMAC. Moreover, when the network load is high, there are some nodes on the service channels, the probability of successful control channel access is higher compared to the IEEE 1609.4. Hence, the safety message broadcast in the VEMMAC is more reliable than the IEEE 1609.4. When the network load is low, the VEMMAC has double safety messages to send compared to the AMCMAC. There are more collisions in the VEMMAC, and the broadcast efficiency is lower than the AMCMAC. However, when the network is saturated, the control channel becomes a bottleneck in the AMCMAC. The number of successful RTS-CTS handshake and safety message broadcast decreases. Broadcast twice and high successful control channel access probability make the VEMMAC have more nodes which receive a safety message successfully than the AMCMAC. In other words, the VEMMAC has higher safety message broadcast efficiency than the AMCMAC.

IV. Conclusions and Future work

This paper proposed the enhanced multi-channel MAC for VANETs which allows nodes to exchange non-safety messages during the CCH interval. By broadcasting safety messages twice, the broadcast efficiency of the VEMMAC is also increased significantly. The simulation results has been presented to show that the VEMMAC protocol outperforms the IEEE 1609.4 in terms of aggregate throughput, average delay and safety message broadcasting efficiency.

Acknowledgment

This research was supported by Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2012-0006421). Dr. CS Hong is the corresponding author.

References

[1] IEEE Standard for Wireless Access in Vehicular Environments (WAVE) Multi-Channel Operation, IEEE Std. 1609.4, Sep. 2010.

[2] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 6: Wireless Access in Vehicular Environments, 2010.

[3] Qing Xu , Tony Mak , Jeff Ko and Raja Sengupta. *Vehicle to Vehicle Safety Messaging in DSRC*, Proceedings of VANET 2004, USA.

[4] Shih-Lin Wu, Chih-Yu Lin, Yu-Chee Tseng, Jang-Laing Sheu. *A new multi-channel MAC protocol with on-demand channel assignment for multi-hop mobile ad hoc networks*, Proceedings. International Symposium on Parallel Architectures, Algorithms and Networks, 2000. I-SPAN 2000.

[5] Jungmin So, Nitin H. Vaidya. *Multi-Channel MAC for Ad hoc Networks: Handling Multi-channel Hidden Terminals Using A Single Transceiver*, MobiHoc '04 Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing *(Mobihoc'04)*, 2004.

[6] Duc Ngoc Minh Dang and Choong Seon Hong. *H-MMAC: A Hybrid Multi-channel MAC Protocol for Wireless Ad hoc Networks*, ICC'12 WS - SaCoNet-III, Canada, Jun. 2012.

[7] Qing Wang, Supeng Leng, Huirong Fu and Yan Zhang *An IEEE 802.11p-based Multi-channel MAC Scheme with Channel Coordination for Vehicular Ad Hoc Networks*, IEEE Transactions on Intelligent Transportation Systems (ITS), 2011.

[8] Chong Han, Dianati, M., Tafazolli, R., Kernchen, R. *Asynchronous Multi-Channel MAC for Vehicular Ad Hoc Networks*, Vehicular Networking Conference (VNC), 2011.

[9] C. Han, M. Dianati, R. Tafazolli, X. Liu and X. Shen. *A Novel Distributed Asynchronous Multi-Channel MAC Scheme for Large-Scale Vehicular Ad Hoc Networks*, IEEE Trans. on Vehicular Technology, vol. 61, p. 3125 - 3138, 2012.

[10] Ning Lu, Yusheng Ji, Fuqiang Liu and Xinhong Wang. *A Dedicated Multi-Channel MAC Protocol Design for VANET with Adaptive Broadcasting* WCNC 2010.

[11] Hang Su and Xi Zhang. *Clustering-Based Multichannel MAC Protocols for QoS Provisionings Over Vehicular Ad Hoc Networks*, IEEE Transactions on Vehicular Technology, 2007.

[12] Xu Xie, Furong Wang, Kewei Li, Peng Zhang and Hao Wang. *Improvement of Multi-channel MAC protocol for dense VANET with Directional Antennas*, IEEE WCNC 2009.