On Multi-hop Forwarding over WBSS-based IEEE 802.11(p)/1609 Networks

Shie-Yuan Wang, Chih-Che Lin, Kuang-Che Liu, and Wei-Jyun Hong

Department of Computer Science
National Chiao Tung University
Hsinchu, Taiwan
Email: {shieyuan, linjc, gjliou, wjhong}@cs.nctu.edu.tw

Abstract—**The IEEE 802.11(p)/1609 network is a promising candidate for future vehicular communication networks. Due to the deployment cost consideration, roadside units (RSUs) in such networks are usually installed only at hot spots and intersections, causing the service coverage of RSUs to be discontinuous. To overcome this problem, multihop data forwarding among vehicles can be used to extend the service coverage of RSUs.**

In this paper, we propose a receiver-centric WBSS (Wave Basic Service Set)-creating scheme to support multihop data forwarding in WBSS-based IEEE 802.11(p)/1609 networks and evaluate its performances using simulations. Our simulation results show that this scheme outperforms a typical sender-centric WBSS-creating scheme on end-to-end flow goodputs under different traffic loads.

I. INTRODUCTION

Vehicular networks have obtained great attention in recent years due to the challenges resulting from its extremely dynamic nature. The IEEE 802.11(p) specification [1], which amends the IEEE 802.11-2007 standard [2], is currently under-development for this type of networks. It defines a new MAC-layer operational mode for Wireless Accesses in Vehicular Environments (called the WAVE mode). The WAVE mode so far defines two basic service sets. One is the WAVE Basic Service Set (WBSS), which comprises a provider and several users and is mainly used for Roadside Units (RSUs) [3] to communicate with Onboard Units (OBU) [3]. Data communication is only allowed between a provider and its user. The WBSS defined in the 802.11(p) network is analogous to the infrastructure BSS defined in the traditional 802.11(a/b/g) network. The key difference between them is that after listening to a beacon message of a WBSS, a new user can directly join the WBSS without performing the authentication and association procedures. The details of a WBSS are explained in Section II.

The other type of BSS is the WAVE Independent Basic Service Set (WIBSS), which comprises multiple peer users. Data communication is allowed between any pair of users. The WIBSS in the 802.11(p) network is analogous to the Independent Basic Service Set (IBSS) defined in the traditional 802.11(a/b/g) network. The main difference between them is that the former explicitly excludes the use of beacon messages in its operation while the latter use them to synchronize the clocks of nodes.

The IEEE 802.11(p) specification and the IEEE 1609 standard family [3][4][5][6] co-define a complete protocol suite for vehicular networks (denoted as the IEEE 802.11(p)/1609 network). The IEEE 802.11(p)/1609 network supports the TCP/UDP/IP protocol suite and a new WAVE-mode short message protocol (WSMP). WSMP is used to disseminate small packets that carry emergent safety and traffic information.

The IEEE 802.11(p)/1609 network manages link bandwidth in a combined FDMA/TDMA manner. In this network, the available frequency spectrum is divided into one control channel (CCH) and several service channels (SCH). The CCH is used by nodes to exchange their network control messages while SCHs are used by nodes to exchange their data. WAVE-mode short messages (WSMs) can be transmitted on both CCH and SCHs. The link bandwidth of each of these channels is further divided into transmission cycles on the time axis, each comprising a control frame and a service frame. In a transmission cycle, the control frame must be on CCH whereas the service frame can be on any SCH.

Due to the deployment cost consideration, RSUs are usually installed only at hot spots and intersections. In this condition, an OBU may not be able to directly connect to a RSU at all time. To overcome this discontinuous coverage problem, multihop data forwarding among vehicles is required to help extend the coverage of RSUs. This means that multihop data forwarding is required for a vehicular network that operates in the WBSS mode.

Multihop data forwarding can be achieved over a WIBSS. This approach is very similar to using multihop data forwarding over a traditional IBSS, which has been extensively studied in the literature. In an IBSS/WIBSS, however, normally every node needs to operate on the same channel. As a result, the bandwidth of multiple SCHs cannot be used at the same time unless a complicated protocol is used. Multihop data forwarding can also be achieved by using WSMP, which allows nodes to transmit data using WSMs without forming a basic service set in advance. However, normally WSMP is used for transmitting small packets carrying emergent information rather than for transmitting large normal data packets. Besides, to use WSMP, every node needs to operate on the same channel, which has the same problem with WIBSS.

These observations motivated us to design a solution that

can easily deploy multihop forwarding in WBSS-based networks. Our proposed solution has two objectives: 1) to efficiently deploy multihop data forwarding in WBSS-based networks and 2) to allow nodes to spread their traffic loads over different service channels to increase total network capacity. In this paper, we studied two WBSS-based multihop forwarding schemes. One is the Sender-centric WBSS Forwarding Scheme (called SWFS), which uses a typical sender-centric WBSS-creating scheme, while the other is our proposed Receiver-centric WBSS Forwarding Scheme (called RWFS), which uses a novel receiver-centric WBSS-creating scheme proposed in this paper. We evaluated the performances of SWFS and RWFS using a RSU-aided multihop forwarding scenario explained Section III. To the best of the authors' knowledge, this paper is the first work that studies the issues and performances of deploying multihop data forwarding in WBSS-based vehicular networks.

The rest of this paper is organized as follows. In Section II, we briefly explain the operation of a WBSS. In Section III, we present the details of the RSU-aided multihop forwarding scenario used to evaluate the performances of SWFS and RWFS. We then explain the designs of SWFS and RWFS in Section IV and evaluate their performances in Section V. Finally, we survey related work in Section VI and conclude this paper in Section VII.

II. The Operation of a WBSS

After joining an 802.11(p)/1609 network, a node should first operate on CCH to gather necessary network information. Data packet transmissions are only allowed to occur within a WBSS. A node that creates a WBSS is called a WBSS provider and nodes that join a WBSS are called WBSS users. To establish a WBSS, a WBSS provider needs to broadcast beacon frames that contain a WAVE Service Advertisement (WSA) message for this WBSS on CCH. A WSA message includes the operational information of its WBSS (e.g., the ID of the WBSS and the SCH that the WBSS will use). A node should monitor all WSA messages on CCH to know the existence and the operational information of available WBSSs. After obtaining the operational information of a WBSS, a node can join the WBSS by switching its channel to the SCH used by the WBSS on service frames.

A WBSS user need not perform the authentication and association procedures to join a WBSS. The reason is that in a highly-mobile environment such as a vehicular network, wireless link connectivity among vehicles is very fragile and has very short lifetime. By using this design, a vehicle can quickly utilize the bandwidth of a WBSS after detecting its existence. Because a WBSS provider may change the operational parameters of its WBSS, a WBSS user should switch back to CCH constantly to learn the latest information about its WBSS.

The communication in a WBSS is carried out in a one-hop manner, i.e., data exchanges are only allowed between a WBSS user and the WBSS provider. According to [3], "WAVE devices take the role of either provider or user on a given service; this is determined by the role chosen by the application operating through the device." and "A device may change roles as it participates on different services." These statements mean that *A node cannot simultaneously create its own WBSS and join other node's WBSS on a given service at the same time.* Such a design is required for a multi-channel network such as an 802.11(p)/1609 network. Otherwise, if a node joins a WBSS and creates its own WBSS at the same time for the same service and the SCHs used by these WBSSs are different, then which SCH should it switch to during a service frame to receive packets sent from other nodes to it? The same dilemma may occur when the two WBSSs belong to different services. This dilemma can be solved as different services are associated with different priorities and the node can determine which SCH to switch to based on their priorities. However, if the two WBSSs belong to the same service, such a dilemma cannot be solved based on priority.

Because the standard does not allow a node to join a WBSS (to be a WBSS user) and create a WBSS (to be a WBSS provider) at the same time for the same service and multihop data forwarding certainly is a service to upper-layer applications, supporting multihop data forwarding over WBSS-based vehicular networks is a problem. This is because in a general multihop vehicular network some nodes unavoidably will need to be both a provider and a user at the same time to forward packets.

III. RSU-aided Geographic Multihop Forwarding Scenario

In our multihop forwarding scenario, each RSU is connected to the Internet via wired lines. Each OBU establishes a constant-bit-rate (CBR) UDP flow with a different host in the Internet. To transmit its packets to the end host, each OBU should send packets toward the RSU that is closest to itself. On receiving these packets, the RSU will forward them to the Internet. Each RSU and OBU is equipped with a Global Positioning System (GPS) and thus knows its location at all time.

Each RSU periodically advertises its location information using a scoped-flooding mechanism. On receiving a location-information message of a RSU, an OBU re-broadcasts this message if the number of hops that this message has traversed has not exceeded the maximum allowed hop count. Based on the received location-information messages, each OBU knows the location of the RSU that is closest to itself at present.

As discussed in Section I, due to the deployment cost consideration, RSUs are usually installed only at hot spots and intersections. An OBU, therefore, may not be able to directly connect to a RSU at all time. To overcome this problem, other OBUs on the path from the OBU to its nearest RSU will forward packets to extend the service coverage of a RSU. The forwarding of a packet is accomplished in a geographic forwarding manner. The detailed geographic forwarding design based on SWFS differs from that based on RWFS. This is due to the differences between sender-centric and receiver-centric WBSSs. We explain these details below.
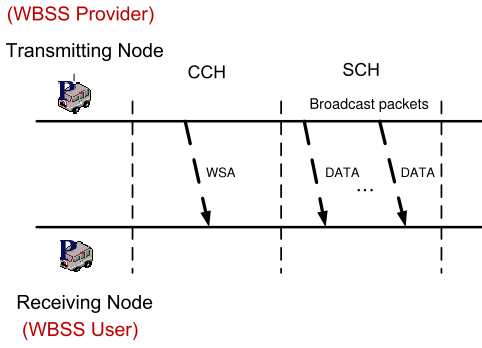
(WBSS Provider)
Transmitting Node

CCH   SCH
                  Broadcast packets

WSA   DATA   DATA
           ...

Receiving Node
(WBSS User)

Fig. 1: The procedure to create a WBSS under SWFS

IV. TWO WBSS-BASED MULTIHOP FORWARDING SCHEMES

A. Geographic Forwarding using the Typical SWFS

Fig. 1 shows the procedure to create a WBSS under a typical SWFS. Using SWFS, a transmitting node should create a WBSS before it transmits its data packets. After broadcasting a WSA message for the WBSS that it creates (on a control frame on CCH), the transmitting node assumes that a receiving node will join its WBSS on the subsequent service frame to receive (and forward) its packets. As presented before, because a new user can directly join a WBSS without performing the authentication and association procedures, a WBSS creator has no clues to know which node will join (or has joined) its WBSS. Thus, it cannot know the exact IP address of the next-hop node. For this reason, the transmitting node simply broadcasts its data packets in its WBSS on the subsequent service frame and assumes that a receiving node exists in its WBSS and will receive these broadcast packets.

If no receiving nodes join this WBSS, the packets broadcast by the transmitting node will be lost. If a receiving node already exists in this WBSS and successfully receives these packets, it should determine whether it is the destination of the received packets. If it is, it delivers the payloads of these packets to upper-layer protocols/applications. If not, it should create a new WBSS and re-broadcast these packets toward the nearest RSU. This process is repeated until these packets arrive at the nearest RSU.

To efficiently utilize the link bandwidth of multiple SCHs, in SWFS each node maintains a channel utilization table based on its received WSA messages on control frames. The channel utilization table is used to record the number of active WBSSs on each SCH. With this information, each node can choose a least-used SCH to create its own WBSS when it needs to broadcast packets. Doing so can spread traffic load across all SCHs to efficiently utilize network bandwidth.

B. Geographic Forwarding using the Proposed RWFS

The operation of SWFS is based on an assumption: *After a WBSS is created, at least one neighboring node will join it*. However, this assumption is not always true. For example, consider an 802.11(p)/1609 network comprising four nodes, A,

B, C, and D, that can listen to each other. Nodes A and B have data to send and thus create their respective WBSSs. Suppose that the WBSSs of nodes A and B use different SCHs for better channel utilization. Other nodes (such as nodes C and D), therefore, cannot simultaneously join these two WBSSs at the same time. Without coordination, nodes C and D may choose the same WBSS (e.g., node A's WBSS) to join. In this condition, no nodes will join node B's WBSS to receive and forward its packets. Worse yet, because under SWFS node B disseminates data using broadcast rather than unicast, without the link-layer ACK mechanism (which is used only for unicast), it cannot detect such packet losses and quickly retransmit them at the MAC layer.

From these observations, we concluded that a sender-centric WBSS-creating scheme cannot efficiently forward data due to two reasons. First, a WBSS provider cannot know whether a WBSS user has joined its WBSS to forward its packets. Second, it may happen that most WBSS users choose to join the same WBSS, causing some WBSSs having no WBSS users to forward their packets. To solve these problems, we propose a receiver-centric WBSS-creating scheme (used by RWFS), which aims to efficiently perform multi-hop forwarding in a WBSS-based vehicular network.

As shown in Fig. 2, using RWFS a WBSS is created by the receiving node rather than the transmitting node. Instead of broadcasting a WSA message, when node i has data to send, it first broadcasts a "forward-req" WSM on a control frame on CCH to probe whether any of its neighboring nodes that are closer to the nearest RSU is willing to forward its packets. The "forward-req" WSM contains the ID of the transmitting node, the ID of the nearest RSU chosen by the transmitting node, and the ID of the SCH that the transmitting node intends to use. Upon receiving node i's "forward-req" WSM, a neighboring node that is closer to the chosen RSU and willing to forward node i's packets should create a WBSS and respond to node i's request by advertising the WSA message of its created WBSS on CCH.

Node i can detect whether there is a node willing to forward its packets by listening to CCH and checking whether a WBSS has been created on the SCH that it indicated in its "forward-req" WSM. (This is accomplished by checking the received WSA messages.) If not, it should rebroadcast its "forward-req" WSM on the next control frame. If yes, node i knows that a receiving node that is closer to the chosen RSU will forward its packets. With this information, node i then joins the WBSS created by this receiving node and transmits data packets to it using unicast. Such a forwarding process repeats until node i's data packets reach the chosen RSU, which then forwards these packets to the destination end host in the Internet. Compared with the SWFS, this receiver-centric design can reduce the number of packet losses caused by inexistence of receiving nodes in WBSSs. It therefore outperforms SWFS on the achieved end-to-end flow goodputs.

RWFS uses a redundant WBSS cancellation mechanism to eliminate WBSSs that are unnecessarily created. We briefly explain this mechanism here. Consider node j that is also
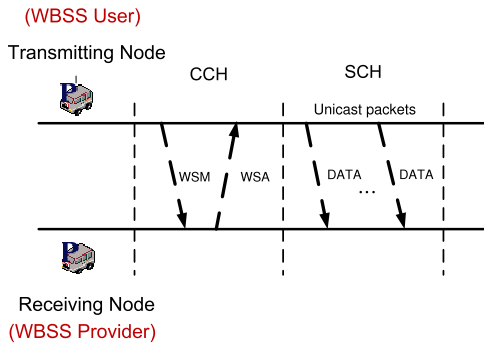
Fig. 2: The procedure to create a WBSS under RWFS

Fig. 3: The road network topology used in simulations

willing to create a WBSS to service node i's "forward-req" WSM. Before broadcasting out its WSA message, if it detects that another WBSS has been created and uses the same SCH as that indicated in the "forward-req" WSM[1], it will destroy its own WBSS and cancel its WSA broadcast. Ideally, this cancellation mechanism will create only one WBSS to forward packets. Even if multiple WBSSs are created due to some reasons such as packet collisions of WSA messages, since the transmitting node will choose only one WBSS to join and use unicast to transmit its packets, link bandwidth will not be wasted by redundant data packet forwarding performed by multiple receiving nodes. Like SWFS, RWFS also uses a channel-load-balancing mechanism to spread traffic load across multiple SCHs.

V. Performance Evaluation

In this section, we use the NCTUns network simulator [7] to evaluate and compare the performances of the typical SWFS and our proposed RWFS in the RSU-aided geographic forwarding scenario presented in Section III. As shown in Fig. 3, the topology is a rectangular road network with a RSU deployed at the center of the road network. Each road segment is 750 meters in length. The RSU is connected to a fixed network that is composed of 20 hosts. Twenty 802.11(p)/1609 OBUs (cars) are randomly deployed on the roads. The transmission range and interference range of each node's radio were set to 250 meters and 550 meters, respectively. The data rate of the radios was set to 27 Mbps, which is a valid rate defined in 802.11(p).

In this scenario, k constant-bit-rate (CBR) UDP flows are activated during simulation, where k is ranged from 5 to 20. Each sender of the flows is run on a different OBU while its corresponding receiver is run on a different host. During simulation, the sender transmits one 1400-byte UDP packet every 0.1 second to its corresponding receiver. The moving behavior (speed, car following, etc.) of each OBU on the roads is controlled by the vehicle movement model proposed in [8]. The simulated time for each run is set to 1,000 seconds.

Two performance metrics are used to evaluate the performances of SWFS and RWFS. One is Aggregate UDP-flow
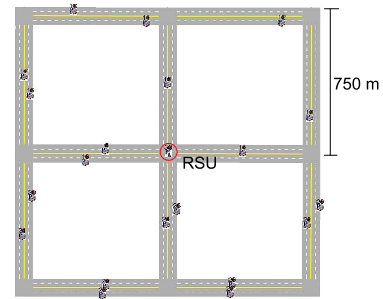
Goodput (AUG) and the other is Average End-to-end Packet Delay (AEPD). The AUG metric is defined as $\sum_{i=1}^{N} t_i$, where t_i is the average goodput obtained by the i-th UDP flow and N denotes the total number of UDP flows in a simulation run. The average goodput obtained by a flow is defined as the number of bytes received at its receiver divided by the simulated time. The AEPD metric is defined as $\frac{\sum_{i=1}^{N} AD_i}{N}$, where AD_i denotes the average packet delay experienced by the i-th UDP flow and N denotes the total number of UDP flows in a simulation run. The average packet delay experienced by a flow is defined as the average of the delays experienced by all of its received packets. Each AUG and AEPD result presented in this paper is the average across ten simulation runs, each using a different random number seed.

Fig. 4 shows the AUG results of the SWFS and RWFS schemes under different number of flows. One sees that the achieved aggregate goodput of RWFS is greater than that of SWFS under different traffic loads and when the traffic load is heavy (i.e., when the number of flows is 20), RWFS significantly outperforms SWFS. There are several reasons to explain the results. First, RWFS uses unicast rather than broadcast to forward packets. As a result, no network bandwidth is wasted due to redundant packet forwardings that may occur in SWFS. (This is possible when multiple receiving nodes decide to forward the packets broadcast by the transmitting node.) Second, in SWFS the transmitting node (the provider) broadcasts packets without knowing whether there is a receiving node (a user) willing to receive and forward the packets. The packets may thus be lost due to no such receivers and this reduces the number of packets that successfully reach the receiver of the UDP flow. Third, both RWFS and SWFS can spread traffic load across multiple SCHs to efficiently utilize network bandwidth. However, RWFS is more effective than SWFS in this operation as it does not have the bandwidth wastage problems with SWFS.

Compared with SWFS, although RWFS needs to broadcast an extra WSM in a control frame, the bandwidth overhead for these WSMs is tiny. This is because a WSM is not broadcast for just one packet to be forwarded but instead for all the packets to be forwarded in the following service frame (which lasts 50 ms). The size of such a WSM is small and one may assume it to be 100 bytes. Given that the rate of the used radios is 27 Mbps, the transmission time for such a WSM is only

---

[1]This detection can be accomplished by monitoring the WSA messages broadcast on control frames on CCH.

(100*8)/27 = 30 us. This means that to forward 50-ms worth of packets in a service frame, one just needs to use 30 us in the preceding control frame. The overhead of transmitting such WSMs is only 30 us/50 ms = 0.6% of the channel bandwidth.

Fig. 5 shows the AEPD results of SWFS and RWFS under different number of flows. One sees that (1) the packets delays in both RWFS and SWFS decrease as the traffic load increases, and (2) the packet delays in RWFS are quite close to those in SWFS and the maximum delay difference between them is only about 50 ms when the traffic load is heavy (i.e., when the number of flows is 20).

For the (1) result, it is because when the number of flows increases, the number of source OBUs used in the simulation increases as well. Because the density of source OBUs on the roads increases, there are more UDP flows with few hop counts to reach the RSU. As a result, the average hop count of all UDP flows decreases as the number of flows increases. Since the hop count of a flow strongly affects the end-to-end packet delays of a flow, it is natural that the packet delays of both RWFS and SWFS decrease as the number of flows increases.

For the (2) result, although RWFS uses a two-phase protocol while SWFS uses a one-phase protocol, in most cases RWFS can forward packets as soon as SWFS does in the service frame following a control frame. This is because before forwarding packets in a service frame, SWFS needs to broadcast a WSA while RWFS needs to finish a WSM-WSA exchange in the preceding control frame. As long as the WSM-WSA exchange can be finished in the same control frame (which is the common case under light traffic load), like SWFS, RWFS can immediately forward packets at the beginning of the following service frame. This explains why when the traffic load is not heavy, the packets delays of SWFS and RWFS are almost the same. On the other hand, when the traffic load is heavy, the WSM-WSA exchange may not be able to finish in the same control frame. For example, the WSM may be broadcast near the end of a control frame. Because the control/service frames need to be switched every 50 ms, the transmission of the WSA may have to be postponed until the next control frame, which causes extra 50 ms delay to the packets to be transmitted. This explains why when the traffic load is heavy, packet delays of RWFS may be larger than those of SWFS by about 50 ms.

VI. RELATED WORK

In [9], the authors proposed a new WBSS-user-oriented WAVE mode for IEEE 802.11(p)/1609 networks. Using this new operational mode, a WBSS provider will transmit data packets to its users only when it receives a "transmission request" control message sent by them.

The WBSS-creating scheme proposed in [9] falls into the sender-centric design category as well because a WBSS is created by the transmitting node. Although this user-initiated polling design can save link bandwidth by reducing unnecessary packet transmissions, it requires each node to periodically join and poll all neighboring WBSSs to know whether there
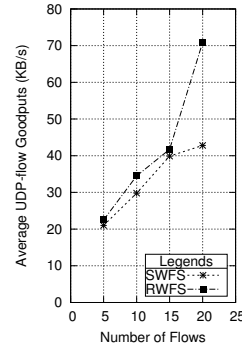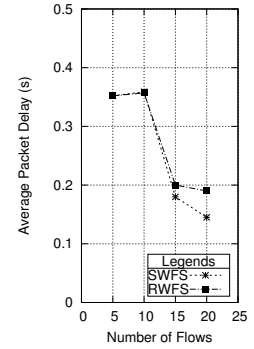

Fig. 4: The AUG results   Fig. 5: The AEPD results

is data destined to it. Compared with our proposed RWFS, such a polling mechanism is more time-consuming to forward packets between two nodes.

VII. CONCLUSION

In this paper, we proposed two schemes for deploying multihop data forwarding in WBSS-based vehicular networks. The first one uses a typical sender-centric WBSS-creating scheme (called SWFS) and the second one uses our proposed receiver-centric WBSS-creating scheme (called RWFS). We evaluated the performances of both SWFS and RWFS in a RSU-aided geographic forwarding scenario. The simulation results show that RWFS outperforms SWFS on end-to-end flow goodputs and incurs almost the same packet delays as SWFS does under different traffic loads. Given the restrictions imposed by the current IEEE 802.11(p)/1609 standards on a WBSS-based network, our proposed RWFS is an effective way to use multihop forwarding to extend the service coverage of RSUs in a WBSS-based 802.11(p)/1609 network.

REFERENCES

[1] *Draft P802.11p/D3.0*, the IEEE 802.11 Working Group of the IEEE 802 Committee, July 2007.
[2] *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)*, June 12, 2007.
[3] *IEEE P1609.0/D0.7 Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Architecture*, the WAVE Working Group of the ITS Committee, January, 2009.
[4] *IEEE 1609.1 Trial-Use Standard for Wireless Accesses in Vehicular Environments (WAVE) - Resource Manager*, IEEE Vehicular Technology Society, October 2007.
[5] *IEEE 1609.3/D1.0 Draft Standard for Wireless Accesses in Vehicular Environments (WAVE) - Networking Services*, the WAVE Working Group of the ITS Committee, December 2008.
[6] *IEEE 1609.4/D1.0 Draft Standard for Wireless Accesses in Vehicular Environments (WAVE) - Multi-channel Operation*, the Dedicated Short Range Communication Working Group of the ITS Committee, December, 2008.
[7] S.Y. Wang et al., *The Design and Implementation of the NCTUns 1.0 Network Simulator*, Computer Networks, Vol. 42, Issue 2, June 2003, pp. 175-197.
[8] S.Y. Wang et al., *A Vehicle Collision Warning System Employing Vehicle-to-Infrastructure Communication*, IEEE Wireless Communications and Networking Conference 2008 (WCNC 2008), March 31-April 3, 2008, Las Vegas, USA.
[9] Choi, N. et al., *A Solicitation-based IEEE 802.11p MAC Protocol for Roadside to Vehicular Networks*, 2007 Mobile Networking for Vehicular Environments Workshop (MOVE 2007), p.p. 91-96, May 11, 2007, Anchorage, Alaska, USA.