A Multi-hop MAC Forwarding Protocol for Inter-Vehicular Communication*

Woosin Lee[1], Hyukjoon Lee[1], Hyun Lee[2], ChangSub Shin[2]

[1]School of Computer Engineering, Kwangwoon University,
447-1 Wolgye-Dong, Nowon-Gu, Seoul 139-701, Korea
wlee@kw.ac.kr, hlee@daisy.kw.ac.kr
[2]Electronics and Telecommunications Research Institute,
161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea
{hyunlee, shincs}@etri.re.kr

Abstract. Conventional topology-based routing protocols such as AODV, DSR and ZRP are not suitable for inter-vehicular communication, where the duration of communication lasts extremely shortly. This paper presents a new inter-vehicular communication protocol called the Multi-hop MAC Forwarding Protocol (MMFP). The MMFP avoids explicit path setup in order to reduce the control overhead associated with it, but instead uses the reachability information towards the destination at each hop. Next-hop nodes are determined on-the-fly by contention based on a priority value. The basic operations of the MMFP are conceptually similar to that of MAC bridges and position-based ad-hoc routing protocols. The MMFP is designed to be integrated with the IEEE 802.11 MAC protocol in order to achieve higher efficiency and accuracy in its time-critical operations. It is shown through simulations that the MMFP outperforms the AODV in a realistic inter-vehicular communication scenario in terms of both the end-to-end delay and packet delivery ratio.

1. Introduction

Inter-vehicular communication based on multi-hop wireless networking is attracting a considerable amount of attention as it can not only extend the coverage of infrastructure-based systems but it can also introduce a new set of services in a robust and cost-efficient manner. In the infrastructure-based systems, the radio coverage of a roadside unit (RSU) can be extended by having a node near the edge of the transmission range forward data to nodes outside the range. Imminent collision warning, rollover warning, work zone warning, platooning, cooperative route planning, and peer-to-peer entertainment are some of the public safety and non-safety related applications that can be enabled by the inter-vehicular communication.

Although there is a large body of work on mobile ad hoc network protocols [1-4], most of them are not suitable for inter-vehicle communication. In general, topology-

* This work was supported by Grant No. R01-2001-00349 from the Korea Science & Engineering Foundation and Research Grant of Kwangwoon University in 2005

based unicast routing protocols — proactive, on-demand or hybrid of the two — such as DSDV, DSR and ZRP set up a path between two nodes before they exchange data. In inter-vehicular communication scenarios, where network topologies change continuously and abruptly, frequent route updates may be necessary. Route update operations, generally based on message flooding, generate an excessive amount of control message overhead which is one of the main sources of large end-to-end delay. The end-to-end delay is one of the most crucial protocol design parameters in the inter-vehicular communication where the duration of communication may be extremely short. Moreover, the control message overhead may cause a significant media contention when communicating nodes are densely populated as in a crowded urban traffic environment [5]. Therefore, a routing protocol with a minimum amount of control overhead in path discovery is desired in inter-vehicular communication.

Position-based routing protocols can forward packets without path discovery or maintenance operation [6-9]. Forwarding decision at each node is made primarily based on the position of the destination and one-hop neighbor nodes. The position information of the destination node is carried in the packet header so that packets can be forwarded by intermediate nodes in the general direction of the destination node. However, unless a separate channel is available for the location service by which the source node to obtain the position of the destination, the position-based routing protocols can suffer from the overhead of location service that scales with $O\left(1/\sqrt{n}\right)$, where n is the number of nodes [6]. This means the overhead of location service has approximately the same complexity as that of path discovery. Furthermore, the inaccuracy of position information caused by node mobility may lead to a significant decrease in terms of packet delivery ratio.

Our goal is to design a new multi-hop routing protocol for inter-vehicular communication that does not perform path discovery or maintenance without using position information. Each node relies on reachability information collected from the packets received previously in making the forwarding decision. This new protocol called MMFP (Multi-hop MAC Forwarding Protocol) is designed as an extension to the IEEE 802.11 MAC layer [10] in order to ensure its functional accuracy in the time-critical operations.

The rest of this paper is organized as follows: In section 2 the MMFP is explained in detail. Simulation results are presented in section 3. Finally, some conclusions are drawn in section 4.

2 Multi-hop MAC Forwarding Protocol

2.1 Main protocol operation

The operation of MMFP follows the principle of a MAC bridge that forwards a frame to a particular LAN segment, if the destination address of a frame has been registered to the filter table, and floods it to all LAN segments otherwise. Specifically, whenever a node receives a packet, the addresses of the transmitter, i.e., a 1-hop neighbor, and the source node are entered in the forward table as reachable nodes.

Two modes of forwarding are defined: (1) *Implicit unicast mode* is used to select a single forwarding node among the 1-hop neighbors by competition based on a priority value. This mode is used when the reachability information is available for the destination node. (2) *Broadcast mode* is used to inform all its 1-hop neighbors to rebroadcast the received packet. This mode is used when the reachability information is not available. A more detailed description on how to maintain the forward table is deferred to the next sub-section. The implicit unicast forwarding process is different from the conventional unicast forwarding process. Whereas each node forwards packets to the next-hop along the predetermined end-to-end path in the conventional unicast, each node broadcasts packets with the destination address specified in the implicit unicast. By allowing only one of the neighbor nodes receiving the broadcast frame to rebroadcast it, an operation similar to the unicast is achieved. This is in principle similar to the forwarding process of position-based routing.

The rebroadcast node is selected based on a priority value, which is determined by the effectiveness of forwarding by each neighbor node. The effective period of a forward table entry, Received Signal Strength Indicator (RSSI), the hop count, or the interface queue length are a few examples of possible metrics that can be used to determine the priority value. The position-based forwarding is achieved if the distance to the destination node is used as the priority value. The selected node sends an ACK so that the semantics of original IEEE 802.11 MAC is preserved. The black-burst method that allows a node sending the longest jamming signal to reserve the medium is used in order to have the highest-priority neighbor node send an ACK frame. Once the destination node receives a frame, it sends an ACK frame immediately after SIFS without sending the black-burst signal. If there are many nodes with the same priority, collisions may occur. The MMFP sends the black-burst signal of a random length once again to resolve the collision. Namely, our black-burst process consists of two black-burst phases; the priority-based first phase and the random backoff-based second phase. A more detailed discussion on the two black-burst phases is presented in section 3.3. The main algorithm of MMFP can be summarized as follows:

```
forward_frame():
    if (new frame is received and destination is another node) then
        lookup forward table;
        if (forward table has destination address) then send_delayed_ack;
            if (send_delayed_ack is successful) then send_implicit_frame;
                        else discard frame;
        else if (frame is flooding frame) then send_flooding_frame;
             else discard frame;
        update forward table;
```

2.2 Maintaining the forward table

The main propose of forward table is to provide information about all reachable nodes. Each entry of the forward table consists of two fields (*destination_address, refresh_timer*), of which *destination_address* represents the address of a node

reachable and the *refresh_timer* indicates the effective period of an entry. An entry is automatically purged when the value of *refresh_timer* becomes zero.

Depending on the type of frames received, the forwarding table should be updated as follows:

1. *When a data frame is received:* Both the source node and transmitter node are reachable along the reverse path assuming all links are bidirectional. Hence, new entries for the source and transmitter nodes should be registered or the *refresh_timer* should be updated if the corresponding entries exist.
2. *When an ACK frame is received:* There are two sub-cases when an ACK frame is received:
   A. The received ACK frame acknowledges the data frame transmitted by the node itself. The destination node is reachable via a neighbor node. If the transmitted data frame is an implicit unicast frame, it means that the existing entry for the destination node is still valid. Hence, the *refresh_timer* should be reset. Otherwise, a new entry for the destination node should be registered.
   B. The received ACK frame acknowledges the data frame transmitted by a neighbor node. The destination of data frame transmitted by the neighbor node is reachable via the node from which the ACK has been received. Hence a new entry for the destination node should be registered.

Fig. 1 shows an example for each case. In Fig. 1 (c), creation of the implicit multipaths is observed. Implicit multipaths S-A-C-D and S-B-C-D between S and D are created as B adds D to the forward table, and the frame, therefore, can continue to be transferred even if either A or B node moves away. As a result, it is possible to reduce overheads significantly, compared to topology-based routing protocol that is subject to the path maintenance process.

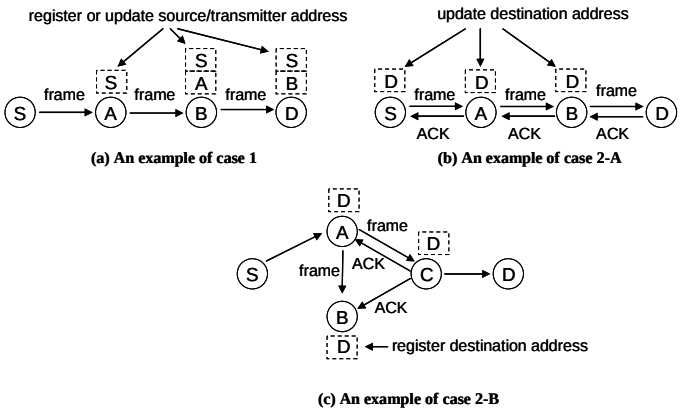

Fig. 1. An example of forward table maintenance

If the destination is not registered in the forward table, a node should broadcast a flooding frame to all 1-hop neighbors. The flooding frames are repeatedly rebroadcasted by subsequent nodes until they reach a node that has a forward table entry for the destination. From then on the frames are forwarded by the implicit unicast. Since the last nodes that rebroadcast a flooding frame receive an ACK from one of their 1-hop neighbor, i.e., case 2 above, they add a new entry for the destination to their forward tables. This type of forward table update is spread from the destination towards the source as more frames are sent by the same source to the same destination. As a result, the area of flooding is reduced quickly as communication between two nodes proceeds. An example is illustrated in Fig. 2, where none of node A and B initially has a forward table entry for destination node D. The flooding frame sent by node S reaches destination node D via node B. Node D broadcasts an ACK which is received by B. Node B then adds a forward table entry for node D as explained above (Fig. 2 (a)). When node B receives the next frame destined for node D from node A, since node B now has a forward table entry for node D, broadcast an ACK and sends an implicit unicast frame to node D. Upon receiving the ACK from node B, node A adds an entry for node D (Fig. 2 (b)). Similar phases are taken when the next frame is sent by node S and now all of nodes S, A and B have an entry for node D (Fig. 2 (c)), hence no more flooding frames are generated. (Fig. 2 (d)).

2.3 Forwarding node selection by contention

As mentioned previously, all neighbor nodes that have the reachability information for the destination compete for a right to send an ACK using the black-burst method. The winner rebroadcast the frame (i.e., implicit unicast) whereas the losers discard the frame (Fig. 3). This prevents uncontrolled rebroadcasting of the same frame. Since this ACK is delayed by black-burst, we call it a delayed_ACK.

Black-burst method was proposed in [11] and [12] in order to provide guaranteed access delays to rate-limited traffic. By allowing each node transmit a data frame only if the medium is free after sending out an energy burst (channel jamming signal) of which the length is determined independently based on a priority value, a node with the highest priority has the exclusive right to transmit the data frame.

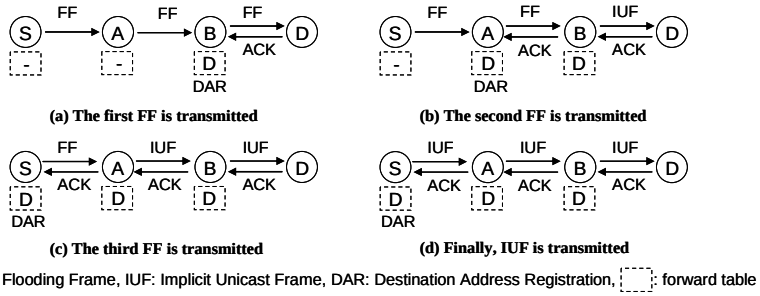

Fig. 2. An example of forward table update process

All contending nodes send the black-bursts after they sense the medium is idle in SIFS+1 slot after receiving a data frame. Since it makes no sense to have the destination node contend with other nodes, the destination node is allowed to send an ACK in SIFS after receiving the frame as specified in the IEEE 802.11 standard. In other words, SIFS+1 slot of waiting by the other nodes ensures the priority access to the medium by the destination node taking into account the propagation delay of the ACK.

The length of black-burst is determined by:

$$\text{The length of black - burst} = \lfloor (priority\_value) \cdot D_r \rfloor \cdot slot\_time, \quad (1)$$

where *priority_value* is number in [0, 1] that increases as the effectiveness of forwarding by a node increases, D_r is the maximum number of slots allocated to the first phase black-burst, and *slot_time* is the length of a slot (i.e., 9 microseconds).

In our work, we use the value of refresh timer and RSSI in calculating the priority value. The value of refresh timer can be regarded as the validity of reachability information. The RSSI can be used to determine the distance between two communicating nodes based on the path-loss radio propagation model, namely, the ratio of the received signal strength P_{RX} at distance d from the transmitter, to the transmitted signal strength P_{TX}, is given by:

$$\frac{P_{RX}}{P_{TX}} = Cd^{-\alpha}, \quad (2)$$

where C is a constant that depends on the antenna gains, the wavelengths, and the antenna heights, α is the path loss factor ranging from 2 to 4 [13]. Using the distance, the farthest away node from the forwarding node among its contending neighbor nodes becomes the winner. Therefore, it is more likely that the closest nodes to the destination become the intermediate nodes in the forwarding path.

It is possible that more than one contending node have the same priority value and hence the same black-burst length. In this case, ACK's sent by these nodes can collide. In order to resolve the problem of colliding ACK's, all winning nodes perform the second phase black-burst one slot after the first-phase black-burst taking into account the propagation delay of the first-phase black-bursts. The length of the second phase black-burst is determined randomly from the range of allowed slots. Note that the per-hop transmission overhead generated by the two-phase black-burst would not be a significant loss compared to the overhead generated by the transmission of RTS/CTS pair that takes 13 slots in IEEE 802.11 a/g.

In Fig. 3 an example of the selection process of a forwarding node based on two-phase black-burst is illustrated. Three contending nodes (A, B and C) send the first phase black-bursts. In this example, node A and B send the black-bursts of the same length, and node C send a shorter black-burst since node A and B have the same priority values that is higher than node C. In the second-phase black-burst, node A sends a longer black-burst than B as determined randomly. Since A senses the idle channel for SIFS, it proceeds to send a delayed_ACK and rebroadcast the implicit unicast frame, and node B and C discard the frame.

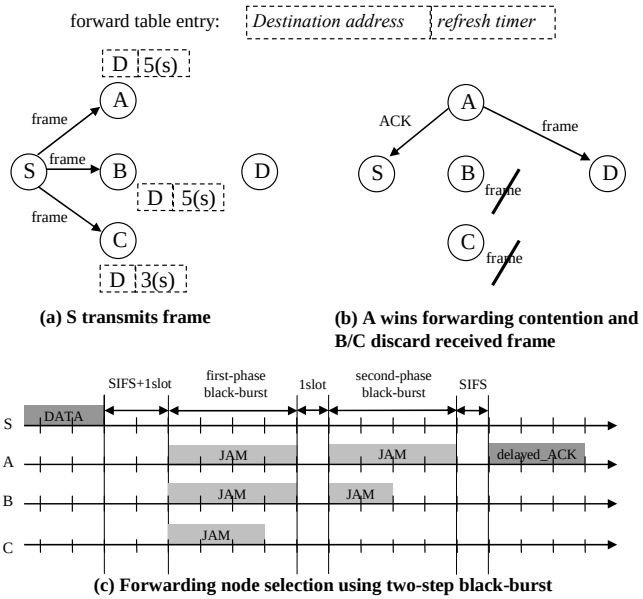

Fig. 3. An example of contention-based forwarding node selection using two-phase black-burst

2.4 Maintaining the sequence number table

In the MMFP, the routing loop is prevented by using the sequence number defined in the IEEE 802.11 MAC specification. The sequence number table consists of four fields including *source_address, sequence_number, forwarding_flag* and *refresh_timer.* When a node receives a frame whose source address matches that of a sequence number table entry with a sequence number equal to or smaller than the *sequence_number,* it discards the frame.

The *forwarding_flag* is used to resolve forward table errors due to the collision of delayed_ACK's that may occur because the two-phase black-burst works with a limited number of slots. If two forwarding nodes send the delayed_ACK's at the same time, as shown in Fig. 4, a collision occurs and the sender retransmits the frame for a specified number of times or until it finally receives an ACK. Because the sequence number of all retransmitted frames is the same, the forwarding nodes determine them as duplicate frames and discard them. In this case, the sender, deluding himself that the retransmission has failed, erroneously purges the corresponding entry. The default value of *forwarding_flag* is 0, and it is set to 1 if the frame is forwarded. If the value of *retry field* in the header of duplicated frame and *forwarding_flag* are both 1, the forwarding node recognizes that there has been a collision in sending the previous delayed_ACK, and it retransmits a delayed_ACK.

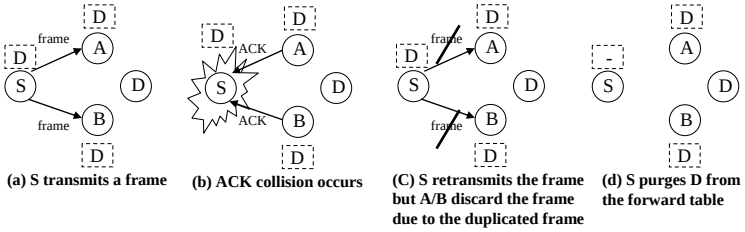

Fig. 4. An example of forward table error

2.5 An extension to IEEE 802.11 MAC protocol

The MMFP uses the four address fields i.e., Address 1 to 4, of IEEE 802.11 MAC frame headers to specify the addresses of the receiver, transmitter, destination and source nodes, respectively. The broadcast address is specified in the receiver address since both the implicit unicast and flooding frames are broadcasted. Because both unicast and broadcast frames are transmitted by using the same broadcast address as the receiver address, the MMFP distinguishes the implicit unicast frames (type: 10, subtype: 1000) and flooding frames (type: 10, subtype: 1001) from each other by using the unused bits of type/subtype fields in the 802.11 MAC header. As opposed to the IEEE 802.11 MAC standard which specifies all broadcast frames are transmitted at the basic rate to minimize the transmission errors of control frames, both the implicit unicast and flooding frames should be transmitted at a data rate.

The MMFP does not use RTS/CTS because all frames are broadcasted, and it resolves the frame loss due to the hidden/exposed terminal problem through retransmission of the unicast frame.

3 Simulation

In order to analyze the performance of MMFP, we performed the simulation using ns-2. The MMFP was implemented in a sublayer between the network and IEEE 802.11 MAC layer. The AODV was also implemented in the sublayer for a fair comparison. We set the values of *active_route_timeout* and *max_rreq_timeout* to 10 seconds, *local_repair_wait_time* to 0.15 seconds, and *rreq_retry* to 3 times as recommended by [14]. The physical layer of IEEE 802.11b was modified to operate as 802.11g by specifying the system parameters for the ERP-OFDM as shown in Table 1. The two-way ground model was chosen as the path-loss radio propagation model. A simulation scenario was designed to reflect the realistic inter-vehicle communication by 180 cars running on a one-way straight-line highway of two lanes with the occasional occurrences of entrances and exits (Fig. 5). Each node periodically makes random transitions with the probability varied from 0.0 to 0.4 between two states, i.e., ‘on’ and ‘off’ states, which represent entering and exiting the highway, respectively. Table 1 lists some of the simulation parameters.

Table 1. Simulation parameters

Parameter	Value
Frequency (GHz)	2.4
CWMin (slots)	15
SlotTime (microseconds)	9
Preamble length (bits)	120
PLCP Header Length (bits)	24
PLCP Data Rate (Mbps)	6
Data rate (Mbps)	54
Transmission range (m)	200
Carrier sensing range (m)	1000
Traffic pattern	CBR
UDP payload size (bytes)	1024

The data rate was set to 54 Mbps with the transmission range of 200 meters. The distance between two nodes in the outer and inner lane was set to 90 and 89.3 meters, respectively. Two adjacent nodes in different lanes were initially separated by 5 meters. All nodes in each lane move at the same speed and the difference in speed between two (passing and driving) lanes is 10 m/s. Scenarios for two cars communicating while moving in opposite directions are left out for further investigation in the future. Each node has nine 1-hop neighbor nodes within its transmission range. Each of the 10 randomly selected nodes sends data traffic at 10 pkts/s for 20 seconds to a destination node that is selected to be a specific distance apart at the beginning of a simulation session. Both the source and destination nodes remain in 'on' state during an entire simulation session. Half of the cars are randomly selected to be initially in 'on' state and the other half in 'off' state such that the network topology changes frequently. A series of simulations were run while changing the values of the distance between the source and destination nodes (360, 720, 1080, 1440, 1800 m) and the on/off probability (0.0, 0.1, 0.2, 0.3, 0.4). Each simulation was repeated 30 times with different seed values for random numbers.

The performance of MMFP was measured with two priority values, based on the refresh timer (MMFP-RT) and RSSI (MMFP-RSSI). Fig. 6 and 7 illustrate the performance of MMFP and AODV in terms of the end-to-end delay and delivery ratio, respectively, against the varying on/off probability values. Here, the distance between the source and destination nodes is fixed at 1440 m. Fig. 6 shows the end-to-end delay of MMFP is consistently lower than that of AODV regardless of the values of on/off probability: 14 ms and 13 ms for the MMFP-RSSI, 50 ms and 48 ms for the MMFP-RT and 128 ms and 238 ms for the AODV when the values of on/off probability are 0.1 and 0.4, respectively. We observed the AODV suffer from the frequent local repair of routes which increased the queuing delay and hence the end-to-end delay. By contrast, because the MMFP is able to forward the frames without the route repair via the implicit multi-paths, the end-to-end delay remains almost constant. In particular, the MMFP-RSSI outperforms the MMFP-RT in terms of the mean number of hops from the source node to the destination node, for example, 9.1 hops versus 10.2 hops with on/off probability 0.4. Furthermore, a smaller number of

ties in priority values among the contending neighbor nodes occur when RSSI is used to calculate the length of the black-bursts.

In Fig. 7, we can see that the MMFP-RSSI outperform both the MMFP-RT and AODV. However, the AODV achieves a higher delivery ratio (93 %) than the MMFP-RT (88 %) when the on/off probability is 0.1. This is because the MMFP-RT loses more frames due to the reset of queue as well as the hidden terminal problem when a node switches to the 'off' state from the 'on' state than the AODV. However, the amount of frame losses due to the collision decreases quickly enough for both the MMFP-RT and MMFP-RSSI that they outperform the AODV (89% and 95% versus 84% when the on/off probability is 0.4).

Fig. 8 and 9 show the performance of MMFP and AODV in terms of the end-to-end delay and delivery ratio, respectively, against the different values of distance between the source and destination nodes with the fixed value of on/off probability (0.3). In Fig. 8, it is shown the end-to-end delay of MMFP-RT and MMFP-RSSI is lower than that of AODV in all regions of the distance values except at 360 m (2.2 ms for the MMFP-RSSI, 13.5 ms for the MMFP-RT and 12.8 ms for the AODV). When the distance increases to 1800 m, the end-to-end delay becomes 16.9 ms for the MMFP-RSSI, 53 ms for the MMFP-RT and 302 ms for the AODV. The steep increase in the end-to-end delay of AODV is due to the increase in queuing delay caused by the route repairs as the probability of route failure increases with the distance. By contrast, for the MMFP, the end-to-end delay increases slowly as the queuing delay is barely affected by the increased distance. Again, the MMFP-RSSI outperforms both the MMFP-RT and AODV. As shown in Fig. 9, the delivery ratios of MMFP and AODV both drops as the communication distance increase: from 99% to 91% for the MMFP-RSSI, from 98 % to 84 % for the MMFP-RT and from 95 % to 83 % for the AODV, respectively, as the distance increase from 360 m to 1800 m.

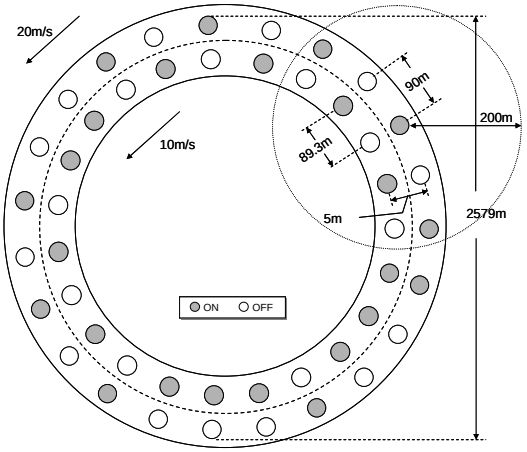

Fig. 5. Circular scenario

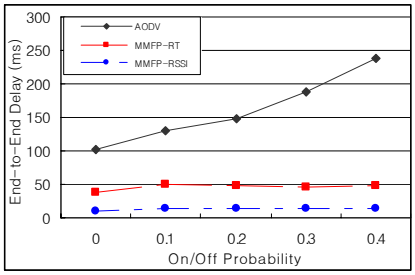

Fig. 6. End-to-end delay vs. on/off probability

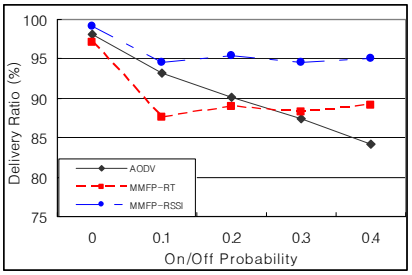

Fig. 7. Delivery ratio vs. on/off probability

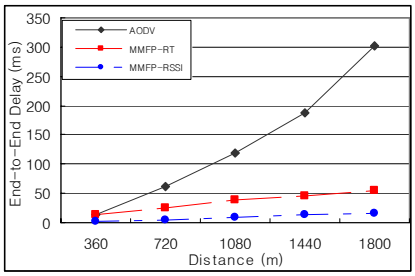

Fig. 8. End-to-end delay vs. inter-vehicular distance

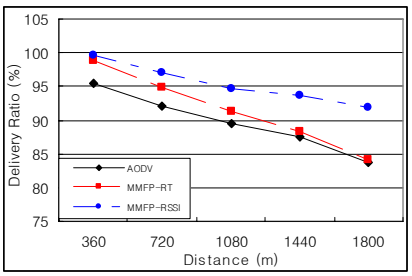

Fig. 9. Delivery ratio vs. inter-vehicular distance

4 Conclusions

In this paper, we propose a new multi-hop routing protocol for inter-vehicular communication. The proposed protocol, MMFP, does not perform path discovery or use the position information of communicating nodes. Since no path discovery or maintenance is performed, the communicating nodes experience shorter delay which is critical in the high-mobility scenarios of inter-vehicular communication. The fact that the MMFP is implemented as an extension to IEEE 802.11 MAC is a significant advantage in terms of reliable performance and rapid deployment. Additional simulations are being set out to evaluate the performance of MMFP in more realistic situations such as a two-way highway with multiple lanes in each direction and a blind intersection. Further investigations are also underway to improve the performance of the MMFP by integrating position information into the forward node selection procedure and by containing flooding frames within the general direction of the destination node.

References

1. Perkins, C.E., Bhagwat, P.: Highly Dynamic Destination Sequenced Distance-Vector Routing (DSDV) for Mobile Computers, In Proc. of ACM SIGCOMM'94 (1994) 234–244
2. Johnson, D.B., Maltz, D.A.: Dynamic source routing in ad hoc wireless networks in Mobile Computing, Imielinski, T. and Korth, H. Eds. Norwell, MA: Kluwer Ch. 5. (1996) 153-181
3. Perkins, C., Royer, E.: Ad-hoc On-Demand Distance Vector Routing, In IEEE Workshop on Mobile Computing Systems and Applications (1999) 90-100
4. Perlman, M.R., Haas, Z. J.: Determining the optimal configuration for the zone routing protocol, IEEE Journal on Selected Areas in Communications (1999) 1395–1414
5. Zhu, J., Roy, S.: MAC for Dedicated Short Range Communications in Intelligent Transport System, IEEE Communications Magazine (2003) 61-67
6. Mauve, M., Widmer, J., Hartenstein, H.: A survey on position-based routing in mobile ad hoc networks, IEEE Network, Vol. 15 No. 6. (2001)
7. Karp, B., Kung, H. T.: GPSR: Greedy Perimeter Stateless Routing for Wireless Networks, MobiCom '00, Boston Massachusetts (2000) 243–254
8. Basagni, S. *et al*.: A Distance Routing Effect Algorithm for Mobility (DREAM), MOBICOM '98, Dallas TX USA (1998) 76−84
9. Blazevic, L. *et al*.: Self-organization in mobile ad-hoc networks: the approach of terminodes, IEEE Communication Magazine (2001)
10. ANSI/IEEE: 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (1999)
11. Sobrinho, J.L., Krishnakumar, A.S.: Distributed multiple access procedures to provide voice communications over IEEE 802.11 wireless networks, GLOBECOM'96 Communications: The Key to Global Prosperity, Vol. 3. (1996) 1689 – 1694
12. Jacob, L., Xiang, Li, Luying, Zhou: A MAC protocol with QoS guarantees for real-time traffics in wireless LANs, ICICS-PCM 2003, Vol. 3. (2003) 1962 – 1966
13. Rappaport, T. S.: Wireless communications. principles and practice., Prentice Hall (1996)
14. The Network Simulator(ns-2), http://www.isi.edu/nsnam/ns/