IPv6 Neighbor Discovery with Multi-hop Communication for IP-Based Vehicular Networks

Zhong Xiang*, Yiwen (Chris) Shen*, and Jaehoon (Paul) Jeong‡
* Department of Electrical & Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea
‡ Department of Interaction Science, Sungkyunkwan University, Suwon, Republic of Korea
Email: {xz618, chrisshen, pauljeong}@skku.edu

***Abstract*—This paper presents a Vehicular Neighbor Discovery (VND) as an extension of IPv6 Neighbor Discovery (ND) for IP-based vehicular networks. An optimized Address Registration and a multihop Duplicate Address Detection (DAD) mechanism are specified to eliminate the frequent address reconfigurations of vehicles when passing between Rode-Side-Units (RSUs) in a Mobility Anchor (MA) domain for operation efficiency and vehicle energy saving. Furthermore, multi-hop communication for a vehicle outside the coverage of an RSU via relay vehicles is proposed to support communication between a vehicle and an RSU out of one-hop wireless communication range, which can extend the serving coverage of the RSU and improve network performance. Through performance evaluation, it is shown that our VND outperforms the legacy ND by greatly reducing DAD in vehicular networks, leading to the efficient IP address autoconfiguration operation.**

***Index Terms*—Vehicular Neighbor Discovery, Address Registration, Duplicate Address Detection, Multi-hop Communication**

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANET) have been explored to provide safe and efficient driving as well as entertainment in Intelligent Transportation Systems (ITS). IEEE 802.11p [1] based on the Dedicated Short-Range Communications (DSRC) has been specified for a low-latency wireless communication, considering the high-speed mobility of vehicular environments and was re-specified as IEEE 802.11 Outside the Context of a Basic Service Set (OCB) in 2012 [2]. In addition, IEEE has standardized Wireless Access in Vehicular Environments (WAVE) [3] which is considered as a key component in ITS. Furthermore, IP Wireless Access in Vehicular Environments (IPWAVE) working group in IETF is working for IP-based vehicular networking using vehicle-to-infrastructure (V2I), vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) [4].

VANET features asymmetric connections and moderate power constraint in mobile devices (e.g., electric cars and unmanned aerial vehicles) due to high-mobility dynamics in continuously changing radio environments. However, the classical Neighbor Discovery (ND) in IPv6 [5] assumed that nodes are always power-on and reachable in stable networks (e.g., Ethernet). Thus, the relatively time-consuming ND operations are not desirable in VANET scenarios.

To enhance the interaction between a vehicle and an RSU (V2I) or between vehicles (V2V), this paper specifies an extension of IPv6 ND called Vehicular ND (VND) for optimization of Duplicate Address Detection (DAD) and Address Registration in vehicular networks. Note that our preliminary idea of this paper is proposed in our IETF Internet draft [6]. The main contributions of this paper are listed as follows:

- An improved Router Discovery (RD) procedure by removing the periodic or unsolicited multicast Router Advertisement (RA) messages;
- An Address Registration mechanism by maintaining all registered vehicles in both RSUs and a Mobility Anchor (MA);
- A multihop DAD procedure by two new types of ICMPv6 messages to eliminate multicast storms and frequent address reconfigurations when passing by RSUs;

The remainder of this paper is composed as follows: Section II summarizes the related work of neighbor discovery. Section III describes our network architecture and design of IPv6 VND for Address Registration and optimized multihop DAD. The performance evaluation is presented in Section IV. In Section V, we conclude this paper along with future work.

II. RELATED WORK

VANET supports a variety of applications such as one-hop communication and multi-hop information dissemination via V2V or V2I. The work in [7] points out that for opportunistic networks (e.g., vehicular networks), challenges such as the recognition of the presence of neighbors, extended lifetime, and communication ranges are quite important for effective neighbor discovery, especially considering mobility features.

IPv6 ND [5] gives definition to several important mechanisms such as prefix discovery, router discovery, DAD, address resolution, etc. The classical ND demonstrates DAD as follows [8]; each node joins the solicited-node multicast address corresponding to the IPv6 address to be configured in its network interface card and multicasts Neighbor Solicitation (NS) messages to the link to which the network interface card belongs. If a duplicate address is discovered in this process, the node using the same IPv6 address replies a Neighbor Advertisement (NA) message to indicate that the IPv6 address has already been used by the node sending the NA message. An IPv6 address can be considered as unique only after sending three NS messages with certain intervals. The original DAD is relatively feasible in stable networks such as Ethernet where nodes are supposed to be power-on and reachable most of the time. However, it is not suitable and inefficient to perform this time-consuming DAD in vehicular networks since VANET features high-mobility dynamics, and asymmetric lossy connections.

In the optimized IPv6 ND for IPv6 Low-Power Wireless Personal Area Network (6LoWPAN) [9], connections among nodes are assumed to be asymmetric and unidirectional because of continuously changing radio environments and lossy signals. The authors proposed an improved IPv6 ND which greatly eliminates link-scope multicast to save energy by constructing new IPv6 options and a new scheme for address configurations. Furthermore, an efficient multihop DAD mechanism is provided for 6LoWPAN. Vehicular environments hold many common characteristics with 6LoWPAN such as asymmetric connections and restrict powers. This paper takes advantage of the optimized ND in 6LoWPAN and proposes an improved IPv6 VND to eliminate an inefficient link-scope-multicast-based DAD in vehicular networks, and use an efficient network-wide multihop DAD.

In [10], a new framework called VIP-WAVE is proposed for extended and non-extended IP-based services in vehicular networks as well as a mobility management scheme using Proxy Mobile IPv6 over WAVE to improve network performance and demonstrate the feasibility of IP-based WAVE standard. To guarantee seamless communications for Mobile Nodes (MNs), a per-MN-Prefix model is presented by assigning a unique IPv6 prefix to every mobile node. However, this per-MN-Prefix model causes the waste of IP prefix assignments and prevents all vehicles holding the same IP prefix from communicating directly with each other without intermediate routers. Thus, this paper proposed a Shared-Prefix model which refers to an addressing model where the prefix(es) are shared by more than one node. That is, the same prefix is assigned to multiple vehicles attached to a common RSU and the IP address uniqueness is guaranteed with a multihop DAD mechanism.

III. Vehicular Neighbor Discovery

A. Vehicular Network Architecture

Fig. 1 illustrates an example of vehicular network architecture for V2I and V2V. Three RSUs are deployed along roadsides and are connected to an MA through wired links (e.g., Ethernet). The MA maintains integrated information reported from each RSU including IP addresses and mobility information of vehicles driving within the communication coverage of RSUs in the vehicular networks. Vehicles are wirelessly connected to RSUs by IEEE 802.11-OCB standard, that is, V_2 is wirelessly connected to RSU_1 while V_3 and V_4 are connected to RSU_2 and RSU_3, respectively. Vehicles can directly communicate with each other via V2V connection (e.g., the link between V_2 and V_3) to share driving information. In addition, vehicles out of the range of any RSU may connect with an RSU through multi-hop connection via relay vehicles (e.g., V_1 can communicate with RSU_1 via V_2) for DAD and TCP connections. Vehicles are assumed to establish the connection with an RSU as soon as they enter the coverage of the RSU.

This paper recommends a multi-link network involving multiple RSUs and vehicles as explained above. This recommendation targets at the extension of the service range of the infrastructure (e.g., RSUs) and the reduction of frequency address reconfigurations of vehicles during handover between two adjacent RSUs. The uniqueness of global addresses is the fundamental prerequisite and critical task of constructing this multi-link network. Unlike proposed in [11] to use a per-MN-Prefix model which may result in redundant prefix waste, a Shared-Prefix model for efficient prefix utilization is presented in this paper. That is, vehicles attached to the same RSU should hold the same prefix for their global IP addresses and multihop DAD is conducted to guarantee their uniqueness in this MA domain. When they pass through RSUs in the same MA domain, vehicles do not need to perform the Address Registration and DAD again but can maintain their current IP addresses in wireless coverage of other RSUs. On the other hand, if vehicles enter the wireless coverage of an RSU belonging to another MA domain, they must repeat the Address Registration and DAD procedure to update their IP addresses with the new prefix.

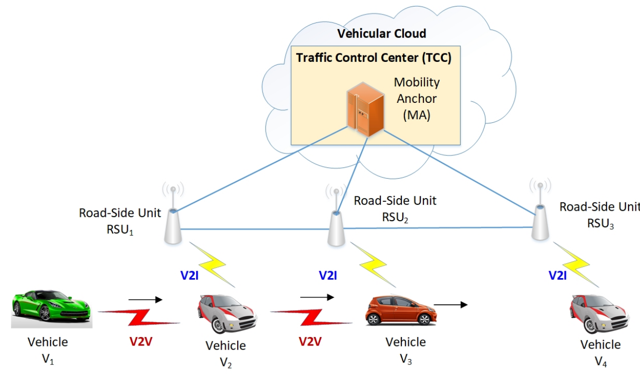

Fig. 1. Vehicular Network Architecture

B. Address Registration

A new Address Registration and multihop DAD mechanism is specified in this paper for avoiding link-scope multicast floods and saving energy in a large-scale vehicular network. The host-initiated RD removes the necessity for RSUs to frequently multicast unsolicited RA messages to accommodate vehicles. Neighbor Unreachability Detection (NUD) is replaced by Address Registration which removes the bandwidth-consuming neighborhood test that a vehicle checks periodically the reachability of its neighbor vehicles. If an RSU inspects any vehicle with expired registration time, it will directly delete it without NUD.

In multi-link vehicular networks, three practicable scenarios may happen according to our Address Registration scheme:

1) Vehicles enter this MA domain for the first time where the current RSU belongs to another MA domain: Vehicles are required to perform multihop DAD along with Address Registration as described in Section III-C.
2) The new RSU is located in the same MA domain as the precedent RSU where a vehicle has already held a non-tentative global IPv6 address with the obtained prefix:

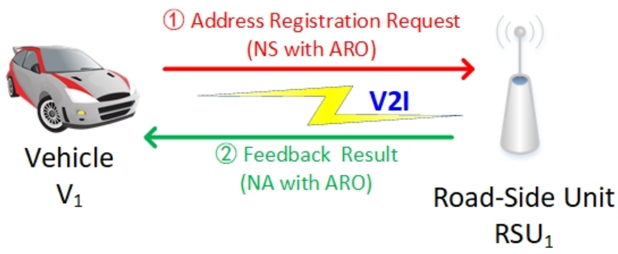

Fig. 2. Address Registration

TABLE I
PARAMETERS IN NEIGHBOR CACHE ENTRY

Field	Description
Interface ID	Neighbor's registered interface identifier
IPv6 Address	IPv6 link-local address of the registered interface
MAC Address	Link layer address of the registered interface
Reachability State	Neighbor's reachability state
Registered Lifetime	Registered time during which neighbor is reachable
Relay Address	Address of intermediate neighbor for this interface
isRouter	Determine if the node is a router (RSU)
Router Expire Time	Indicate valid lifetime of a router (RSU)

The vehicle does not need to repeat the multihop DAD again but just registers its address with the new RSU since the global address has been proved to be unique in this MA domain.

3) Vehicles are out of the coverage of any RSUs but find a neighbor which already registered with its serving RSU: A new relay scenario via V2V communication for vehicles out of the serving range of RSUs is introduced in this paper. If a user vehicle become disconnected from an RSU, it initiates to search for a neighbor vehicle which can provide relay service and share its global prefix achieved from its serving RSU. A relay vehicle is expected to forward DAD messages for a user vehicle. Note that in this paper, at most one intermediate vehicle is allowed.

After autoconfiguring its global IPv6 address with the obtained global prefix, a vehicle initiates to register its address with the serving RSU through multihop DAD. Address Registration is performed by appending Address Registration Option (ARO) in NS and NA messages to indicate registration time and registration status. Its format is defined in [9]. ARO is always initiated by vehicles. Information such as registration time and registration status carried by ARO is also included in Duplicate Address Request (DAR) and Duplicate Address Confirmation (DAC) messages transmitted between RSU and MA in multihop DAD, but ARO is not directly used in these two messages. The detailed formats of DAR and DAC are specified in [9].

Fig. 2 provides an example message transfer scheme of Address Registration. The detailed procedure is together described with the DAD mechanism in Section III-C since Address Registration is implemented simultaneously with multihop DAD. After DAD succeeds, vehicles need to periodically repeat the Address Registration to maintain its registration to its serving RSU before its lifetime expires.

C. Multihop Duplicate Address Detection

A vehicle must process DAD to determine whether its address is unique or already in use by another vehicle before exchanging information with other vehicles with this address. In the legacy IPv6 ND [5], nodes multicast NS messages to all links in a solicited-node multicast address and wait for a certain period to detect if a duplicate address exists. Instead of this time-consuming process, an optimized multihop

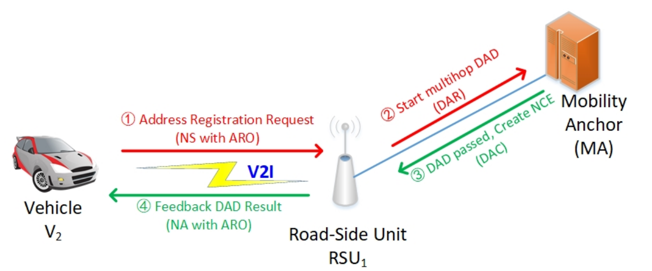

Fig. 3. Multihop DAD Procedure

DAD is designed in this paper to decrease frequent multicast messages for energy-saving. Neighbor Cache Entries (NCEs) are maintained by each RSU and MA in DAD Tables to inspect address duplication during the multihop DAD process. That is, each RSU preserves NCEs for all on-link vehicles (i.e., reachable vehicles) in its DAD Table. Similarly, MA stores an integrated DAD Table for NCEs reported by all RSUs in its domain. The parameters in NCEs are listed in Table I.

A vehicle can avoid redundant DAD with multihop DAD whenever it enters the coverage of another RSU in the same MA domain, leading to the reduction of traffic overhead in vehicular wireless links. Two new ICMPv6 messages such as DAR and DAC are applied for multihop DAD. Information carried from ARO is copied into these two messages and transmitted to MA.

Fig. 3 presents an example procedure for Address Registration and multihop DAD. Note that these steps are based on the assumption that this vehicle has successfully finished the RD and its link-local address autoconfiguration as specified in [8].

The multihop DAD procedure along with Address Registration is explained as follows:

1) A vehicle unicasts an NS message including ARO to the serving RSU to register its address.
2) The RSU inspects its DAD Table first to check whether the address already exists or not after receiving the NS message. If no duplicate NCE exists, a tentative NCE is created for this address, and then the RSU unicasts DAR to MA to start multihop DAD.
3) When MA receives DAR from an RSU, it checks whether the register-requested address exists in its DAD Table or not. If an entry with the same address exists in the

DAD Table, which means the address is duplicate, MA returns a DAC message to RSU with registration status to notify the address duplication. On the other hand, if no entry with the same address exists in the DAD Table, an entry for the address is created, then MA replies a DAC message to the RSU to confirm the uniqueness of the register-requested address.

4) If notified with the address duplication from MA, the RSU deletes the tentative NCE and sends back NA to notify the address-registration vehicle of the registration failure. Otherwise, the RSU changes the tentative NCE into a registered NCE in its DAD Table to indicate the vehicle is reachable, and then send back NA to the vehicle to inform the registration success.

Thus, the multihop DAD is processed simultaneously with the Address Registration. Note that the tentative address are not considered to be assigned to any vehicle until MA confirms the uniqueness of the register-requested address by multihop DAD.

D. Multihop DAD via One Intermediate Vehicle

If a vehicle fails to register its IP address with a direct serving RSU, it triggers neighbor discovery to look for neighbor vehicles which can provide relay services via multi-hop communications. It is assumed that a vehicle triggers a relay request only if its RD fails. On the other hand, at most one intermediate vehicle is permitted to act as a relay for another vehicle to communicate with the RSU.

Note that not all the vehicles have the ability to provide relay services. Vehicles should determine if they are available to serve as relay vehicles by checking its own registration status and current processing relay requests. Only vehicles which can act as temporary relays will take action when they receive relay requests. The user vehicle can process its global IP address configuration, Address Registration, and DAD through a relay vehicle. Fig. 4 demonstrates an example scenario for relay services. When a user vehicle fails to directly register its IP address with an RSU, it multicasts NS messages to initiate neighbor discovery through V2V communication. If a neighbor can provide relay service, it creates an NCE for the user vehicle, setting its own address as a relay address, and sends back NA with prefix information received from RSU.

In the case where several neighbors reply, a nearest neighbor selection mechanism is required to select the neighbor closest to an RSU. After multicasting NS messages, the vehicle waits for 1 second to receive all replies and keep them in a tentative router list, including global prefixes and hop distances in Prefix Information Option. Then the user vehicle chooses another vehicle with the least hop distances as its relay neighbor.

After determining its relay neighbor, the vehicle configures its global address with the received global prefix and initiates the Address Registration along with DAD process via its relay vehicle. NS message is configured as described in Section III-C but indicates the relay vehicle's address as next-hop address to reach the RSU. In such a case, the relay vehicle will forward those relay-request messages received from the user vehicle to its serving RSU. The registration and multihop DAD procedure is the same as the normal one except that the RSU will include the intermediate neighbor's address as a relay address in NCE to indicate that it is not a directly attached vehicle at this moment and set the relay address as the next-hop address.

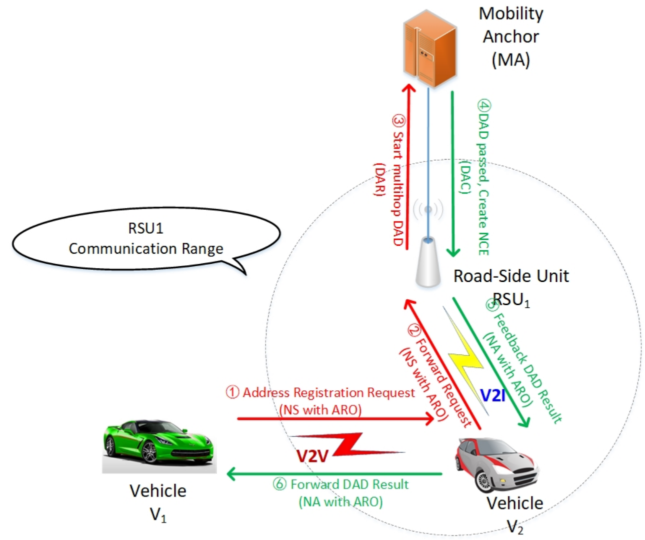

Fig. 4. V2V Multihop Communication

TABLE II
SIMULATION PARAMETERS

Parameters	Values
Road network size	1400m * 700m
Communication range of nodes	200m
Maximum speed limit	5-30m/s
PHY/MAC Layer	IEEE 802.11-OCB
Minimum gap between two vehicles	2.5m
Vehicle acceleration	$2.6m/s^2$
Vehicle deceleration	$4.5m/s^2$
Tx Power RSU	20mW
Tx Power Vehicle	10mW

IV. Performance Evaluation

The implementation of our model is carried out in simulator OMNeT++ [12] and SUMO [13]. We constructed our VND model based on INET and Veins Frameworks. Fig. 5 illustrates our main simulation scenarios. The major implementation is achieved by appending new options in ND messages such as NS and NA. Also, two new ICMPv6 messages such as DAR and DAC are implemented to construct multihop DAD. Table II shows detailed simulation parameters in our implementation.

For performance evaluation, we compare two kinds of DAD mechanism defined in classical IPv6 ND and VND proposed in this paper. The comparison evaluates the average processing time of DAD without intermediate relays as well as End-to-End (E2E) delay under multiple hop distances in VND along with different vehicle numbers.

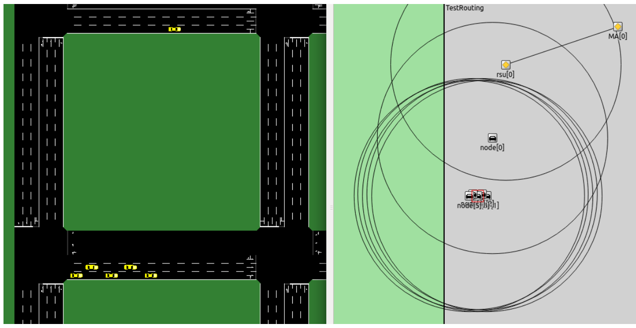

Fig. 5. Simulation Interface

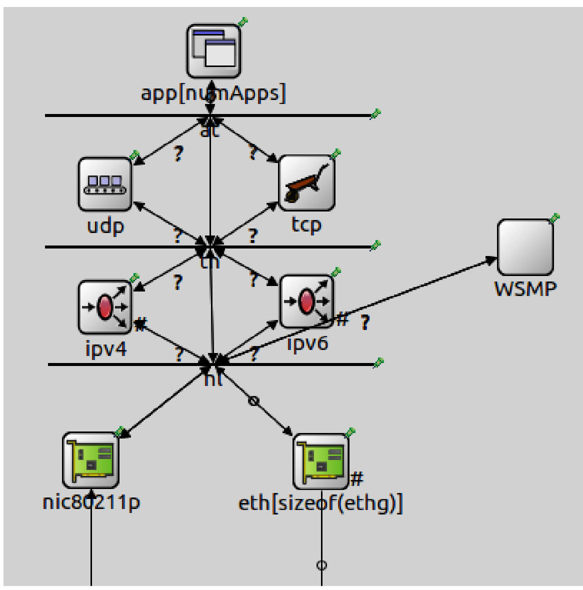

Fig. 6. Node Structure

A. IEEE 802.11-OCB

In this paper, a novel framework of IP communications in vehicular networks is presented. To support the IEEE 802.11-OCB in IP-based network, we established new Vehicle and RSU models based on Veins and INET projects by attaching the PHY/MAC layer which defines IEEE 802.11-OCB to the original IPv6 node architecture determined in INET. Also, we modified the MAC layer in IEEE 802.11-OCB to accept IP packets from the network layer as well as to deliver the received IP packets to upper layers. The node structure is as shown in Fig. 6.

B. Comparison of legacy DAD and multihop DAD

The evaluation results of two kinds of DAD in the legacy ND and VND without intermediate relays are presented in Table III. It is obvious that the average DAD processing time is greatly reduced in VND by unicasting multihop ND messages to its serving RSU and MA instead of broadcasting and waiting for a reply from the duplicate address in the legacy ND. Furthermore, the average processing time in VND is stable with a small variance with increased vehicles since the whole process takes less than 0.001s and is not based on multicast.

TABLE III
DAD PROCESSING TIME IN THE LEGACY ND AND VND

#Vehicle	Legacy ND (s)	VND (s)
5	1.665790753	0.000846651
10	1.614267702	0.000867451
15	1.622217908	0.000863119
20	1.593333245	0.000844052
25	1.631985633	0.000839892
30	1.661594873	0.000844486

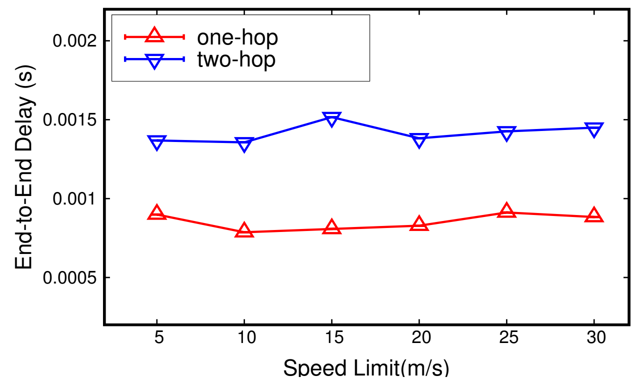

Fig. 7. E2E delay of multihop DAD under different velocity

C. Multihop DAD with Different Hops

a) The impact of speed limit: To figure out the impact of vehicle velocity to DAD process, we assume a fixed number of vehicles run forward with different speed limits and specific acceleration and deceleration. The speed limit varies from 5 m/s (18 km/h) to 30 m/s (108 km/h) with a step of 5 m/s. Fig. 7 shows the E2E delay of multihop DAD in VND along with increasing velocity and different hop distances. Note that hop distance indicates hop count between a vehicle and its serving RSU. Here we consider multihop DAD without an intermediate vehicle as "one-hop" and multihop DAD with an intermediate vehicle as "two-hop",

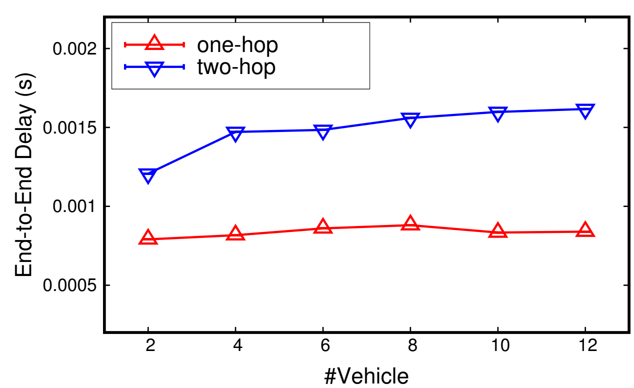

Fig. 8. E2E delay of multihop DAD under different vehicle numbers

respectively. Vehicles are distributed with the same separation distance. For multihop DAD with relay services, one vehicle in the coverage of the serving RSU acts as a relay neighbor for other vehicles in uncovered areas. It is observed that E2E delay with one intermediate vehicle is 150% of E2E delay without one intermediate vehicle since the communication distance increased. On the other hand, DAD processing time is slightly influenced by speed since the process takes less than 0.002 second.

b) The impact of vehicle number: Fig. 8 shows the E2E delay of multihop DAD with various numbers of vehicles. It is assumed that each vehicle can provide relay service to at most 12 vehicles at the same time. It can be observed that for multihop DAD without relay vehicles (one-hop), E2E delay maintains a stable value when the vehicle number increases. On the other hand, E2E delay for multihop DAD with a relay vehicle (two-hop) gradually increases along with more vehicles. The main influence factor is that vehicles may fail to register the nearest neighbor as its relay vehicle when the number of neighbors increases, leading to more message conflicts because they send or receive multiple packets at the same time.

V. Conclusion

In this paper, we provide a new Vehicular Neighbor Discovery (VND) for vehicular networks. A multihop DAD and Address Registration mechanism enhances the legacy IPv6 ND to speed up the DAD process for highly dynamic road traffic. Moreover, our VND facilitates multihop communications between remote vehicles and RSUs via V2V and V2I by extending the service coverage of transportation infrastructures. As future work, we plan to demonstrate a mobility management for the seamless communication of vehicles moving between the RSUs in a proactive fashion by using the trajectories of vehicles in vehicular networks.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2017R1D1A1B03035885). This research was supported in part by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2018-2017-0-01633) supervised by the IITP (Institute for Information & communications Technology Promotion). Note that Jaehoon (Paul) Jeong is the corresponding author.

References

[1] IEEE, "IEEE Draft Standard for Information Technology-Telecommunications and information exchange between systems-Local and Metropolitan networks-Specific requirements-Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications-Amendment 8: IEEE 802.11 Wireless Network Management," *P802.11v/D12.0, June 2010*, pp. 1–392, Jul. 2010.

[2] IEEE, "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2016*, pp. 1–3534, Dec. 2016.

[3] Y. L. Morgan, "Notes on DSRC & WAVE Standards Suite: Its Architecture, Design, and Characteristics," *IEEE Communications Surveys Tutorials*, vol. 12, no. 4, pp. 504–518, Fourth 2010.

[4] J. P. Jeong, "IP Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases," Internet Engineering Task Force, Internet-Draft draft-ietf-ipwave-vehicular-networking-11, Jul. 2019, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-ipwave-vehicular-networking-11

[5] W. A. Simpson, D. T. Narten, E. Nordmark, and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)," RFC 4861, Sep. 2007. [Online]. Available: https://rfc-editor.org/rfc/rfc4861.txt

[6] J. P. Jeong, Y. C. Shen, and Z. Xiang, "Vehicular Neighbor Discovery for IP-Based Vehicular Networks," Internet Engineering Task Force, Internet-Draft draft-jeong-ipwave-vehicular-neighbor-discovery-07, Jul. 2019, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-jeong-ipwave-vehicular-neighbor-discovery-07

[7] R. Pozza, M. Nati, S. Georgoulas, K. Moessner, and A. Gluhak, "Neighbor Discovery for Opportunistic Networking in Internet of Things Scenarios: A Survey," *IEEE Access*, vol. 3, pp. 1101–1131, 2015.

[8] D. T. Narten, T. Jinmei, and D. S. Thomson, "IPv6 Stateless Address Autoconfiguration," RFC 4862, Sep. 2007. [Online]. Available: https://rfc-editor.org/rfc/rfc4862.txt

[9] C. Bormann, Z. Shelby, S. Chakrabarti, and E. Nordmark, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)," RFC 6775, Nov. 2012. [Online]. Available: https://rfc-editor.org/rfc/rfc6775.txt

[10] S. Cespedes, N. Lu, and X. Shen, "VIP-WAVE: On the Feasibility of IP Communications in 802.11p Vehicular Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 1, pp. 82–97, Mar. 2013.

[11] K. Chowdhury, K. Leung, B. Patil, V. Devarapalli, and S. Gundavelli, "Proxy Mobile IPv6," RFC 5213, Aug. 2008. [Online]. Available: https://rfc-editor.org/rfc/rfc5213.txt

[12] "OMNeT++: Discrete Event Simulator." [Online]. Available: https://omnetpp.org/

[13] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, "Recent Development and Applications of SUMO - Simulation of Urban MObility," *International Journal On Advances in Systems and Measurements*, vol. 5, no. 3&4, pp. 128–138, Dec. 2012. [Online]. Available: http://elib.dlr.de/80483/