IPv6 Neighbor Discovery for Vehicular Networks

Danilo Moreira[1,2], Kelly Wagemann[1,3], and Sandra Céspedes[1,2]

[1] NIC Chile Research Labs
[2] Department of Electrical Engineering, Universidad de Chile, Santiago, Chile
[3] Department of Computer Science, Universidad de Chile, Santiago, Chile

Abstract. Vehicular Communication Networks (VCN) are critical enabling technologies that contribute to the advancement of Intelligent Transportation Systems. Although initially VCN were thought with a focus on safety, there is a myriad of IP-based applications for information and entertainment systems to be deployed in vehicular scenarios. To support IP-based applications, standard protocol stacks, including IEEE WAVE and the recent 3GPP C-V2X architectures, define the transport of IPv6 and related protocols on top of the specific wireless access technologies. One of the fundamental protocols for the use of IPv6 is Neighbor Discovery (ND), defined in RFC 4861. In this work, we evaluate the performance of the standard ND protocol and compare it to recent works, including several IETF Internet-drafts, that propose enhancements for the IP registration and duplicate detection processes in the dynamic environment of VCN.

Keywords: IPv6 · Neighbor Discovery · Vehicular Networks · Wireless Networks · IEEE 802.11p

1 Introduction

Neighbor Discovery (ND) is a protocol that allows IPv6 nodes on the same link to discover each other's presence, determine each other's link-layer addresses, find routers, and maintain reachability information about the paths to active neighbors [9].

It has been argued in the past that the ND protocol may not be suitable for vehicular communication networks based on 802.11 connectivity, because of the short-lived links that are present and the highly dynamic conditions on these networks [4, 7, 10]. The objective of this project is to evaluate how the standard Neighbor Discovery (ND) in IPv6 performs in a vehicular environment. We study previous works, including IETF Internet-drafts, that propose modifications or extensions to the ND protocol and provide a qualitative and quantitative comparative evaluation of the standard ND with recent proposals designed for vehicular environments.

The remainder of this document is organized as follows: In section 2, we survey related works that review the ND protocol shortcomings and address the drawbacks of ND in highly mobile scenarios. In section 3, we present a qualitative comparison of the different approaches and select the work to be implemented in

a simulation environment. In section 4, we present the simulation scenario, the metrics for quantitative analysis, and the resulting data from the simulations. In section 5, we discuss and analyze the data obtained from the simulations and compare the performance of Neighbor Discovery protocols. Finally, in section 6 we conclude the work.

2 Related work

The works surveyed in this section were selected according to the following criteria: i) to select works that identify and discuss the shortcomings of Neighbor Discovery in vehicular networks and wireless networks in general; and ii) to present recent alternative proposals, including work items at the IETF, to perform neighbor discovery. The chosen proposals were Neighbor Discovery protocols designed for both vehicular networks and other types of wireless networks and are discussed as follows.

2.1 IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases

This work describes the problems of Neighbor Discovery Protocol in Vehicular Environments [7]. In order to specify protocols for Vehicular Ad-hoc Networks (VANETs), the ND protocol needs to be adapted to overcome certain challenging aspects of vehicular networking, such as protocol exchanges that need to be completed in a short time, nodes moving at high speed, asymmetry in the connectivity among neighboring interfaces, and frequent partitioning and merging of VANETs. The main limitations and requirements identified with ND in vehicular networks are:

In legacy Neighbor Discovery, vehicles have to configure a link-local IPv6 address or a global IPv6 address and run IPv6 ND before they can start exchanging application layer messages with each other. However, vehicles move fast within the communication coverage of any particular vehicle or IP-RSU. This limits the lifetime of the links and creates a necessity for a fast start of communications between nodes. ND time-related parameters, such as router lifetime and Neighbor Advertisement (NA) interval, need to be adjusted for vehicular speeds and vehicular densities.

On VANETs, two IPv6 addresses may conflict with each other after a network merging even if they were unique before. The partitioning of a VANET may make vehicles with the same prefix be physically unreachable. Therefore, ND Stateless Address Autoconfiguration (SLAAC) needs to prevent IPv6 address duplication due to the merging of VANETs. A vehicular link model should consider the frequent partitioning and merge of VANETs due to vehicular mobility.

This draft only states the problem and necessities of Vehicular Environments. Therefore, there is no proposed implementation to solve these problems in the document.

2.2 IPv6 Neighbor Discovery on Wireless Networks

Wireless Neighbor Discovery (WiND) is an Internet-draft that proposes two changes to the legacy ND: the proactive addressing registration by hosts to their attachment routers and the routing to host routes within the subnets [10]. Proactive address registration is performed with a new option of NS/NA messages: the Extended Address Registration Option (EARO), which is defined in RFC8505 [11]. This allows the routers to prepare and maintain the hosts' routes and avoids NS Lookup.

The hosts register their addresses to the serving routers with EARO. Routers have complete knowledge of the hosts they serve and hosts gain routing services in return. EARO allows abstraction of the routing protocol, so routing can take multiple forms. This is done by providing information to the router that is independent of the routing protocol.

The draft doesn't provide details of specific use cases. Instead, it abstracts the architecture to a general case, so it may need adaptation for a VANET scenario. The use case that reflects the unique prefix in a Roadside Unit (RSU) and On-board Unit (OBU) infrastructure corresponds with the Hub-and-Spoke configuration of the protocol. The Hub-and-Spoke configuration only requires that link-local addresses be unique from the perspective of every communicating pair, which, in this case, are the pairs of each OBU with the RSU. The OBUs register all their IPv6 addresses by sending an NS with EARO to the RSU.

2.3 Hierarchical SAA in MANETs

This proposal considers a hierarchical model for ND in mobile ad-hoc networks (MANETs) [12]. In MANETs, every node acts both as a host and as a router. Therefore, IPv6 SAA can be employed. The scheme works as follows: every node defines a broadcast link, which will be called *scope*, as the group of nodes that are less or equal than rs hops away to it. The hierarchy is established by assigning a state to each node. These states are Leader, Candidate, and Host. The Leader must act as the router of the subnetwork and it configures a group of nodes by issuing Router Advertisements.

The protocol introduces a new NS message, which is the legacy NS message with a new section called the MANET option. The objective of this section is to include information to build the hierarchy on the subnet. It also contains a Random Source ID field to help distinguish messages with the same tentative link-local address while doing DAD. Nodes have a cache to keep the RS-ID of each message received for a certain amount of time and only forward ND messages with RS-IDs that are not on the cache. This measure reduces the number of collisions in the network.

When a mobile node joins the network, it first generates a tentative link-local address. Then, it needs to perform DAD, so the node sends the modified NS message containing this tentative link-local address and a particular hop limit of rs. The hop limit limits the message to the scope of the node, which forms an abstraction of a LAN broadcast link. When a node receives an ND message, it

decreases the hop limit and then forwards it. Forwarding only is done if the hop limit is greater than 0. If the DAD succeeds, the address is considered valid only for a certain period t_s. Link-local addresses are guaranteed to be unique only within the scope of each node, not the entire ad-hoc network.

The proposal leaves some aspects of the implementation open. For example, it is unclear when the Candidate state is set and what conditions are needed in terms of the parameters of the network. There are also some characteristics of the protocol like optimizations and solutions to merge problems that are left open and not specified.

2.4 Performance evaluation of Neighbor Discovery++ protocol for the provisioning of self-configuration services in IPv6 mobile ad hoc networks

This work presents the ND++ protocol and the simulation results verifying the ND++ behavior in the NS-3 simulation environment [5].

The authors argue that an important aspect in IPv6 Mobile Ad-Hoc Networks (MANETs) is to be able to make configurations that are automated and without the need for supervision. At the moment, IPv6 Neighbor Discovery Protocol makes use of stateless address autoconfiguration (SAA), but this feature is not sufficient to provide complete support to a MANET.

ND++ is proposed as an extended version of ND, designed to perform efficient DAD in MANETs. It is designed to deal with changing topologies, node mobility, and large-scale networks. It takes into account that networks can be merged and divided, allowing address verification over a wide range and minimizing overhead. Also, it fully obeys IPv6 standards and is independent of the routing protocol. Is important to note that ND++ is not aiming at dealing with the address assignment problem itself, but provides the means of efficient detection of duplicate addresses once they are assigned.

The way ND++ performs duplicate address detection is called DAD++. It is divided into two phases. In phase 1, DAD is performed in the standard way, on the neighborhood reached by 1 hop. In phase 2, named n-DAD, an additional DAD is performed using NS multihop messages (mNS) covering an extended range of n hops. To minimize overhead, Multipoint Relay (MPR) based flooding is incorporated.

ND++ simulations and experiments are carried out to evaluate the performance of the protocol. Channel propagation loss is configured so that a node receives a signal with either maximum or null power when it is out of range. The chosen topologies are Grid, Cross-Grid, and 1 Uniform Disc. Experiments are carried out with different amounts of nodes. Experiment 1 consists of the evaluation of ND++ and DAD++ behavior. In general, the results are as expected, but some anomalies are found. In some of the topologies, there is a considerable amount of packet drops. This problem is addressed by introducing a random delay when a node forwards an mNS message.

Experiment 2 consists of the evaluation of the ND++ overhead. Carrying out this experiment shows that the overhead of MPR-based flooding generates

less overhead than exhaustive flooding. How beneficial is the use of MPR-based flooding depends on the MANET topology. In denser networks, higher overhead is expected.

The authors also indicate that the ND++ hop limit parameter specifies the ND++ range. It must be large enough to detect duplicates in (almost) the entire MANET network, but small enough not to generate too much traffic. In general, the optimal value of the Hop Limit parameter is between one to two times the expected diameter of the network.

2.5 VIP-WAVE: On the Feasibility of IP Communications in 802.11p Vehicular Networks

This work aims to solve the problem of IP-based I2V/V2I communications in 802.11p/WAVE networks [4]. For this, the Vehicular IP framework in WAVE (VIP-WAVE) is provided. Scenarios composed of RSUs and OBUs are studied. VIPWAVE defines three main components that interact with the standard IPv6 protocol: i) the IP addressing and mobility block: assignment of global IPv6 prefixes to vehicles and guaranteeing mobility for extended network services. (RSU); ii) On-demand Neighbor Discovery block: corresponds to a light adaptation of ND; iii) Routing block: allows relay selection for multi-hop communications, in case a user cannot consume an IP service directly from the RSU.

In the VIP-WAVE framework, IP services are advertised in a Wave Service Advertisement (WSA) framework. The types of services provided can be extended and non-extended. An extended service is continuously advertised by all RSUs on the network. A non-extended service depends on location. They are provided only by some RSUs.

An RSU announcing a service transmits a WSA frame on the CCH. OBUs monitor the CCH. An OBU that is one hop away from the RSU can receive the WSA. If the OBU wants to consume an extended service, it tunes the radio to the SCH specified in the WSA. If the OBU does not have a global IP address to initiate communication with the hosting server, it sends an RS unicast message. The RSU exchanges PBU/PBA messages with the LMA for prefix assignment, using the Proxy Mobile IPv6 protocol. The RSU sends an RA message to the OBU with the information necessary to configure its IP. The OBU receives the RA, generates its global IP, and may start exchanging packets with the hosting server. A DAD mechanism is not necessary after configuring the global IP of the OBU since the uniqueness of the IP address is guaranteed by the LMA's assignment of unique prefixes to each OBUs.

If the OBU wants to consume a non-extended service, it uses the IP prefix announced in the WRA to generate a global IP. After configuring the IP, it tunes to the specified SCH. Before packets can be transferred, DAD is performed, since the IP prefix used by the OBU is shared by other consumers. The DAD mechanism is centralized, controlled by the RSU. It is only activated upon the first request for IP data transmission from an OBU. The RSU maintains a list of active OBUs and their IP addresses, to detect duplicates. Upon completion of DAD, the OBU may start exchanging packets with the hosting server. The

IP configuration of an OBU for a non-extended service is valid only within the coverage area of the RSU that provides the service. Thus, the uniqueness of the IP can only be guaranteed in this area.

2.6 Vehicular Neighbor Discovery for IP-Based Vehicular Networks

This work is an Internet-draft that specifies a Vehicular Neighbor Discovery (VND) protocol as an extension of ND [8]. An optimized Address Registration and a multihop Duplicate Address Detection (DAD) mechanism are performed. Also, three new ND options for prefix discovery, service discovery, and mobility information report are defined. VND takes advantage of the optimized ND for 6LoWPAN, where connections among nodes are assumed to be asymmetric and unidirectional.

In VND, there are V2V, V2I, and I2V communications. Vehicles that are not in the range of any RSU may connect with it in a multi-hop connection via relay vehicle. Vehicles are assumed to start a connection to an RSU when they enter the coverage of the RSU. A Shared-Prefix model is proposed. For RSUs in the same subnet, the interfaces responsible for prefix assignment for vehicles should hold the same prefix in their global address. Prefix discovery enables hosts to distinguish destinations on the same link from those only reachable via RSUs. Nodes belonging to the same IP prefix domain can communicate with each other directly.

For address autoconfiguration, a vehicle sends an RS message to an RSU. The RSU sends back a RA message containing prefix information. The vehicle generates its global address by combining the prefix for its current link and its link-layer address. After its IP tentative address autoconfiguration, a vehicle starts to register its IP address to the serving RSU along with doing multihop DAD. Address Register Option (ARO) is used. There are three scenarios feasible in the Address Registration scheme:

1. In the first scenario, if a vehicle enters the subnet for the first time or the current RSU belongs to another subnet the vehicle performs the Address Registration and multihop DAD.
2. In the scenario the vehicle has already configured its IP addresses with a prefix obtained from the previous RSU, and the current RSU is located in the same subnet, given that both RSUs have the same prefix, Address Registration and multihop DAD do not need to be performed.
3. In this scenario, a vehicle is not in the coverage of the RSU but has a neighbor registered with the RSU. The vehicle then starts looking for adjacent vehicle neighbors which can work as a relay neighbor to share the prefix obtained from RSU and undertake DAD of the user vehicle by forwarding DAD messages to RSU.

In VND, DAD is performed in a slightly different way than in the legacy protocol.

- If the vehicle is one hop from the RSU, it sends a unicast NS message to the RSU. The RSU receives the NS and inspects its Neighbor Cache to check if it's a duplicate or not. If it's not in the cache, the RSU creates a tentative NCE for the address and forwards the NS to a Mobility Anchor, containing a table of existing addresses. If the MA checks the table and the address is not there, the MA registers the new address and sends a NA message of registration success to the RSU, which then forwards the NA to the vehicle. The RSU changes the tentative NCE into a registered NCE.
- If the vehicle is two hops from the RSU, it initiates ND to detect vehicle neighbors via V2V communication. The vehicle sends NS messages to connect with neighbors in some range. If a neighbor can provide a relay, it creates an NCE for the vehicle, setting its address as relay address, and sends back a NA with prefix information received from the RSU. When NA is received, the vehicle configures its global address. After this, the vehicle starts Address registration and DAD via the relay vehicle. When performing DAD, if the address is not duplicate, MA will include the relay vehicle's address as relay address in NCE to indicate that the vehicle performing DAD is not directly attached to the RSU at the moment.
- If the vehicle is n-hops from the RSU, a new routing mechanism (DSDV) is specified to select a route of vehicles by which communication is going to be made. Multiple vehicles will act as relay vehicles. Each vehicle that acts as a relay vehicle for this remote vehicle will make records in its Neighbor Routing Table. This way it can be ensured that packets from a source vehicle can be successfully transmitted to an RSU as well as the reverse packet path exists from the RSU to the source vehicle.

3 Qualitative Evaluation

The decision matrix of table 1 was used to compare the standard ND protocol and the proposals surveyed in section 2. The focus is to establish the feasibility of implementing the proposals in a simulation environment for a performance evaluation. Aspects considered in the evaluation are the configuration of the network (unique prefix service, distinct prefix service, or ad-hoc architecture), year of last revision, code availability, level of specification by the author, and the types of networks addressed by the proposal. The code availability characteristic considers the state of the protocol in terms of the publicly available code available for simulations.

Based on these criteria, the WiND and the Hierarchical SAA approaches were discarded for the implementation with simulations. WiND does not have a base implementation to work with, it is not very specific to the scenario and was born in 6LoWPAN networks, without the considerations of VANET. On the other hand, Hierarchical SAA was discarded because of its year of revision and its concepts like site-local addresses which are deprecated. In addition, it does not have any code implementation. VIPWAVE, ND++, and VND were selected as possible implementations to work with.

Table 1: Decision matrix for different protocol proposals.

Characteristic	**Legacy ND**	**WiND**	**VIPWAVE**	**Hierarchical SAA**	**ND++**	**VND**
Unique Prefix	Yes	Yes	Yes	No	Yes	Yes
Distinct Prefix	No	No	Yes	No	No	No
Ad-hoc	Yes	No	No	Yes	Yes	No
Last revision's year	2007	2021	2020	2002	2019	2021
Code availability	-	Full code available	No code available	No code available	Full code available	Some code available
Level of specification of the author	-	Abstract proposal with general examples of how to apply it to VNETs	Very specific	Open considerations for functionalities	Open considerations for functionalities	Very specific
Type of networks	Generally wired networks.	6LoWPAN networks.	802.11p/WAVE networks.	Generally oriented to MANETs.	Extension of ND for MANETs.	Vehicular networks.

VIPWAVE is suited as it contemplates unique and distinct prefixes, has code implemented, and was made specifically for VANETs. The same goes for VND, except it does not consider a distinct prefixes scenario. ND++ is also a good alternative because of its flexibility for both infrastructure and ad-hoc scenarios and the availability of its code.

After this analysis, it was chosen to work with the VND proposal and make a comparison between this approach and the legacy Neighbor Discovery protocol.

4 Performance evaluation

To evaluate the performance of the protocols, a simulation was designed on the software OMNeT++[2]. The IPv6 implementation used was from the INET framework[1]. The code used to simulate VND was an existing implementation of the protocol on OMNeT++ [6].

The scenario chosen for the simulation of the chosen protocols is a section of a double-way highway with three lanes per direction. The length of the section is 600 meters. Vehicles enter the highway following a binomial distribution, at maximum speed. Each vehicle is a node equipped with 802.11p. The RSU is located in the middle of the highway, at 300 meters horizontal and 50 meters vertical. For a coherent comparison, in the VND protocol testing, no vehicle was allowed to forward messages for other vehicles. Figure 1 shows an example of the test scenario. A red light on the back of a vehicle represents that the car is braking.

4.1 Settings for the vehicular traffic

The experiments were carried out with two control variables: vehicular density and maximum speed allowed on the highway. The density and maximum speed

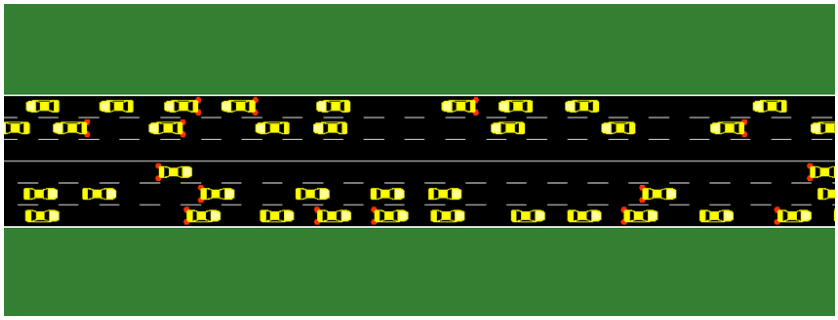


Fig. 1: Screenshot of one of the scenarios simulated in SUMO.

Table 2: Congestion levels for highway testing scenario.

Level of congestion	**Traffic density**	**Vehicle speed**
Slight	[29-37] veh/km/ln	[48-81] km/h
Moderate	[37-50] veh/km/ln	[24-64] km/h
Severe	Above 50 veh/km/ln	Below 40 km/h

were chosen according to the HCM LOS F rating, following the levels of congestion in CoTEC [3]. These levels are summarized in Table 2.

The SUMO tool that generates the vehicles' traces needs the number of vehicles that will enter the highway and the duration of their trip on it. Therefore, it was necessary to obtain these values from traffic density and vehicular speed. The number of vehicles at the same time on the highway can be calculated as (1), where *density* is set according to the congestion levels of table 2 and corresponds to the number of vehicles per km per lane.

$$N_{veh} = density * lanes * length\ of\ the\ street \tag{1}$$

The time the vehicles will be on the street can be approximated to the duration of one trip on the highway, therefore it can be calculated as (2).

$$T_{veh} = \frac{length\ of\ the\ street}{maximum\ velocity} \tag{2}$$

Three values were chosen for the vehicular density, one for each congestion level. For the Slight and Moderate levels, the density value was chosen as the average value of each range: 33 and 43.5 veh/km/lane, respectively. For the Severe level, the vehicular density of 58 veh/km/ln was chosen. The maximum speed is limited in ranges for each level of congestion. However, to make a full comparison between each level, the full range of velocities was used. The range was from 1 m/s (3,6 km/h) to 23 m/s (82.8 km/h) with a step of 1 m/s. The time limit was set to 100 seconds for each configuration tested. Due to the stochastic nature of the system, ten runs were made for each experiment, and so the measurements were averaged to obtain a consistent result.

4.2 Settings for the vehicular network

The traces of the vehicles are generated in SUMO. Once generated, they are imported to OMNeT++ through the VEINS framework. In OMNeT++, an RSU is placed in the scenario at the middle of the highway (300 meters horizontally) and 5 meters away from the center (vertically). For the VND implementation, a Mobile Anchor is added. These scenarios do not include any type of obstacles so no shadowing is considered. Other configuration parameters are shown below in Table 3.

Table 3: Network parameters for vehicular communications.

Parameter	**Value**
Transmission power	200mW
Path loss	Simple path loss model
Alpha value for path loss	2
Carrier Frequency	5.89 GHz
Bitrate	6Mbps
Sensitivity	-91dBm
Noise	-100dBm

4.3 Metrics of evaluation

To compare the performance of each proposal, common metrics should be applied. The metrics were chosen to make the analysis are the following:

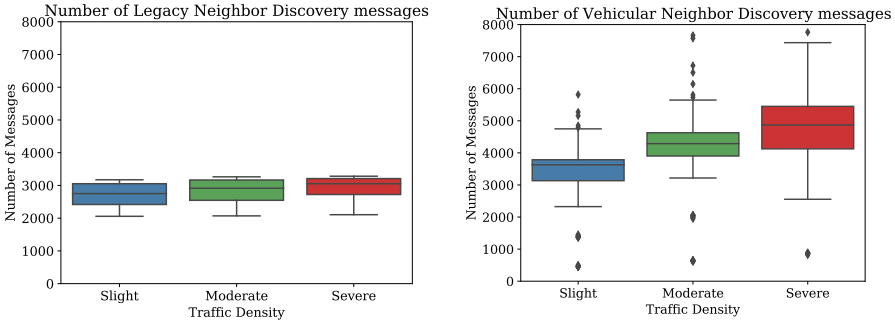
1. Number of ND messages (signaling overhead): This metric is defined as the sum of ND-related packets sent by each node. The metric was used in [5]. Vehicular networks suffer from channel saturation, leading to possible packet losses as the network becomes larger and denser. The objective of this metric is to evaluate the saturation of the network through the magnitude of Neighbor Discovery traffic for a different number of vehicles and speeds.
2. Average end-to-end DAD delay: This metric was used in [13]. It is defined as the average time difference between the sending of a DAD message from the source node and the determination of that address being duplicated or not after checking in the NCE table. This metric considers multihop and multicast messages. Given the context of vehicular networks, it is extremely necessary to guarantee fast message exchanges between nodes. As DAD is performed every time a node joins a new network and is required before it can exchange data, the average E2E DAD delay becomes of special interest. The objective of this metric is to compare the delays in communication during DAD procedures in the network for different vehicle numbers and speeds.

4.4 Simulation results

The results for each metric are aggregated by the density of street traffic. On the following plots, the top and bottom borders of the boxes correspond to the lower and upper quartiles, the middle line in the box is the median, the whiskers represent min and max, and the diamonds represent outliers.

Number of Neighbor Discovery Messages Figure (2a) shows the number of ND-related messages on the legacy ND protocol. The resulting number of messages is around 2000 and 3000, for all traffic density levels. The distributions of the number of messages were expected. The network traffic increases as the vehicular traffic do, as seen in the height of the boxes. The range of values was also the expected one. The lack of outliers indicates that the data has low dispersion.

Figure (2b) shows the number of ND-related messages on the VND protocol. Only the wireless link traffic was considered in this measurement. These results are considerably different in comparison to the results from legacy ND's evaluation. The expected pattern of increasing the number of messages with greater traffic density is also present. However, the differences between each level are more noticeable than the results from the standard ND. Moreover, each distribution has a larger height than in the standard, which indicates that the number of ND-related messages transmitted is greater in VND: the difference of ND messages in comparison with the legacy protocol is approximately 1000, 2000, and 3000 more messages for the Slight, Moderate and Severe levels respectively. The length of the boxes is also different from the legacy case and it varied with traffic density.



(a) Legacy Neighbor Discovery

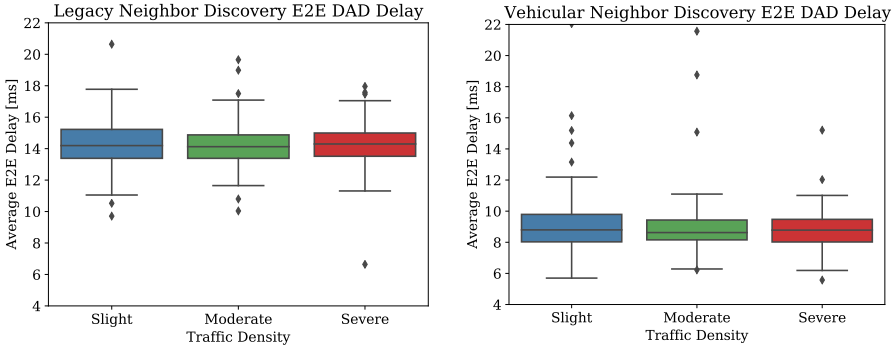
(b) Vehicular Neighbor Discovery

Fig. 2: Number of ND-related messages by traffic density.

Average End-to-End Delay Figure (3a) shows the average end-to-end delay in milliseconds for DAD messages in the legacy ND protocol. The resulting

average delay was around 14 milliseconds. In this case, the DAD communication occurs between the host and all nodes in the same on-link subnet for DAD in the form of multicast messages from the host. This resulted in a similar distribution for all traffic density levels; the boxes have similar lengths and heights.

Figure (3b) shows the average end-to-end delay in milliseconds for DAD messages on the VND protocol. The resulting average delay was around 9 milliseconds. In this case, the DAD communication occurs between the vehicles and the RSU in a centralized fashion. The form of the boxes is similar for all traffic density levels and all three stayed at the same level of delay. The average delays for Vehicular Neighbor Discovery were lower than the ones in the legacy protocol, 5 milliseconds approximately less than the legacy protocol.



(a) Legacy Neighbor Discovery (b) Vehicular Neighbor Discovery

Fig. 3: Average End-to-end Delay by traffic density.

5 Discussion

The simulation results show that, as expected, the number of neighbor discovery messages increases with the traffic density in both protocols, being VND the one generating the greater amount of network traffic. VND also suffered a major impact in network traffic from street traffic density, exhibiting a bigger number of messages for the higher densities. The difference in the number of messages is due to the additions that VND makes over the original legacy neighbor discovery. For example, VND has a communication scheme for the address authentication task that can generate more messaging than the legacy protocol. A vehicle using the legacy protocol can obtain its link-layer address by receiving a periodic Router Advertisement message and then sending a multicast NS to its tentative address as illustrated in Fig. 4. Instead, VND has to at least send a router solicitation with mobility information, trigger an RA response, send an NS with address registration, and finally receive an NA with address registration as seen in Fig.

5, which generates even more messages if the DAD is over multihop. Another factor is the fact that the vehicles are periodically sending RS messages to have a road map created with RSU information.

For the case of the average end-to-end delay, it showed to be similar in all traffic densities, for both protocols. However, the VND delays were lower in comparison to the legacy ones. This can be attributed to the fact that VND's DAD messages are mainly between the nodes and the RSU and MA. VND concentrates the registering of addresses in the static nodes in the network in contrast to the legacy which makes each node responsible for its registration. This lower delay for DAD messages is an advantage over the legacy DAD because the vehicle can start communicating on the link as soon as it receives the confirmation of the address registration from an RSU, whereas the legacy has to wait for a fixed timer to start communications.

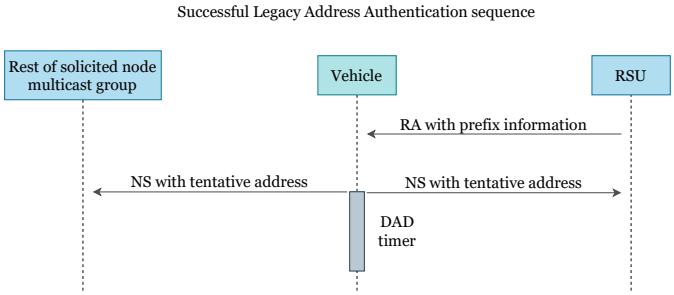


Fig. 4: Successful Legacy Address Registration.

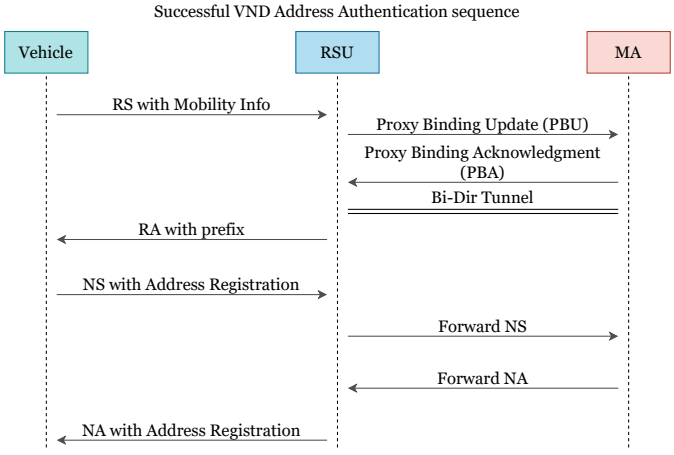


Fig. 5: Successful Vehicular Neighbor Discovery Address Registration.

6 Conclusions

In this work, we have presented an evaluation of the performance of Neighbor Discovery in vehicular communication networks. Given the dynamics in a vehicular environment, the evaluation seeks to establish the level of signaling overhead and end-to-end delay for establishing that no duplicate IPv6 addresses exist, providing a vehicle the capability to communicate via IP-based protocols. The evaluation includes a comparison with a recent proposal proposed as an IETF Internet-Draft, namely the Vehicular Neighbor Discovery (VND) protocol [8], which bases the handling of IP addresses in combination with a mobility management scheme.

According to the results, VND suffers from a trade-off between having a faster address registration process than legacy ND, in exchange for more messages in the network. Although channel saturation is a known issue in vehicular communication networks and it can be critical to the operation of some protocols, given the dynamics of the vehicular network, faster neighbor discovery may be a priority over medium congestion. Therefore, the need to proposing and defining new ND protocols that better handle the case of IP-based communications over vehicular networks.

7 Acknowledgments

This work has been supported by the Cisco Research Grant 2019-199458 (3696) and the ANID Basal Project FB0008. The authors would like to thank the valuable help of Mr. Bien Aime Mugabarigira and Prof. Jaehoon (Paul) Jeong from Sungkyunkwan University, Republic of Korea.

References

1. Inet framework. https://inet.omnetpp.org/
2. Omnet++ discrete event simulator. https://omnetpp.org/
3. Bauza, R., Gozalvez, J., Sanchez-Soriano, J.: Road traffic congestion detection through cooperative vehicle-to-vehicle communications. In: IEEE Local Computer Network Conference. pp. 606–612 (2010). https://doi.org/10.1109/LCN.2010.5735780
4. Cespedes, S., Lu, N., Shen, X.: Vip-wave: On the feasibility of ip communications in 802.11p vehicular networks. IEEE Transactions on Intelligent Transportation Systems **14**(1), 82–97 (2013). https://doi.org/10.1109/TITS.2012.2206387
5. Grajzer, M., Głabowski, M.: Performance evaluation of neighbor discovery++ protocol for the provisioning of self-configuration services in ipv6 mobile ad hoc networks. In: 2014 16th International Telecommunications Network Strategy and Planning Symposium (Networks). pp. 1–6 (2014). https://doi.org/10.1109/NETWKS.2014.6959266
6. Jeong, J.P.: Ipwave basic protocols project ietf-108 hackaton. https://github.com/ipwave-hackathon-ietf/ipwave-hackathon-ietf-108 (2020)

7. Jeong, J.P.: IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases. Internet-Draft draft-ietf-ipwave-vehicular-networking-20, Internet Engineering Task Force (Mar 2021), https://datatracker.ietf.org/doc/html/draft-ietf-ipwave-vehicular-networking-20, work in Progress
8. Jeong, J.P., Shen, Y.C., Xiang, Z., Cespedes, S.: Vehicular Neighbor Discovery for IP-Based Vehicular Networks. Internet-Draft draft-jeong-ipwave-vehicular-neighbor-discovery-11, Internet Engineering Task Force (Feb 2021), https://datatracker.ietf.org/doc/html/draft-jeong-ipwave-vehicular-neighbor-discovery-11, work in Progress
9. Simpson, W.A., Narten, D.T., Nordmark, E., Soliman, H.: Neighbor Discovery for IP version 6 (IPv6). RFC 4861 (Sep 2007). https://doi.org/10.17487/RFC4861, https://rfc-editor.org/rfc/rfc4861.txt
10. Thubert, P.: IPv6 Neighbor Discovery on Wireless Networks. Internet-Draft draft-thubert-6man-ipv6-over-wireless-09, Internet Engineering Task Force (May 2021), https://datatracker.ietf.org/doc/html/draft-thubert-6man-ipv6-over-wireless-09, work in Progress
11. Thubert, P., Nordmark, E., Chakrabarti, S., Perkins, C.E.: Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery. RFC 8505 (Nov 2018). https://doi.org/10.17487/RFC8505, https://rfc-editor.org/rfc/rfc8505.txt
12. Weniger, K., Zitterbart, M.: Ipv6 autoconfiguration in large scale mobile ad-hoc networks. Proceedings of European Wireless **1** (04 2002)
13. Xiang, Z., Shen, Y.C., Jeong, J.P.: Ipv6 neighbor discovery with multi-hop communication for ip-based vehicular networks. In: 2019 International Conference on Information and Communication Technology Convergence (ICTC). pp. 813–818 (2019). https://doi.org/10.1109/ICTC46691.2019.8939883