On the reliability of duplicate address detection in mobile ad hoc networks with Neighbor Discovery++ address auto-configuration protocol.

Monika Grajzer*†
*Gido Labs sp. z o.o.
ul. Romana Maya 1, 61-371 Poznań, Poland
Email: monika.grajzer@gidolabs.eu

Mariusz Głąbowski†
†Poznan University of Technology
ul. Polanka 3, 60-965 Poznań, Poland
Email: mariusz.glabowski@put.poznan.pl

***Abstract*—The approaching vision of the Future Internet and the Internet of Things calls for new methods that would provide a variety of roughly connected devices with a full networking capabilities. These are expected to enable to communicate freely and efficiently in diversified set-ups and configurations, which are mobile and ad hoc in nature. One of the key challenges that needs to be addressed is the aspect of self-configuration and unique address assignment. To address this challenge we have proposed a Neighbor Discovery++ protocol. In this paper we present our recent study on the reliability of duplicate address detection with our proposed solution. The evaluation is performed in realistic mobile ad hoc network environment. We will also discuss on the tradeoff between maximizing reliability and minimizing protocol overhead. The results reveal that Neighbor Discovery++ is a good basis for the stateless address auto-configuration services allowing to achieve reliability close to 100% with very low overhead levels.**

I. Introduction

The approaching vision of the Future Internet and the Internet of Things (IoT) opens new communication endeavours but also brings new challenges to the attention of the researchers. Current realizations mostly concentrate on scenarios where smart devices connect in a centralized manner with a smartphone being a hub providing the Internet connectivity. However, it is expected [1], [2] that next generation networks will allow to go a step beyond and provide a variety of roughly connected devices with full networking capabilities allowing them to communicate freely and efficiently in diversified set-ups and configurations.

There are, however, several challenges that need to be addressed to approach the above vision. One of them is the aspect of self-configuration and IPv6-based Internet connectivity which should be provided to the wide range of small, smart devices and wearables in mobile ad hoc network (MANET) set-ups. It is envisioned [2] that future IoT devices will be able to configure themselves in a "plug-and-play" manner with external configuration actions kept minimal or none. Therefore, the aspects of address auto-configuration (AAC) become crucial in this context. In the future networks with billions of roughly interconnected devices assigning a unique address is not straightforward, even when exploiting IPv6 protocols. Hence, new control and configuration solutions are needed to extend IPv6 [3]. In the demanding environment of future innovative networks each new address has to be verified [3], [4], since address duplications, even between more distant nodes, can be very harmful for the whole network configuration. The reliability of the duplicate address detection procedure is thus of significant importance and should be duly considered.

Current stateless address auto-configuration (SAA) solutions for MANETs [5]–[11] are not sufficient to address the above issues, since they either lack adequate scope (are limited to 1-hop neighborhood of each node) [5], [6] or robustness and efficiency [7]–[11]. This is particularly visible for large-scale networks.

To address the above challenges of SAA in MANET networks we have proposed a method of efficient duplicate address detection (DAD) as an extension to one of the core IPv6 protocols – Neighbor Discovery protocol [5], [6]. Our solution – the Neighbor Discovery++ (ND++) [12]–[14] – is targeted for diversified MANET networking environments and provides enhanced address duplication capabilities enabling to verify address uniqueness between more distant nodes. Moreover, ND++ is capable of reacting to network changes and keeping protocol overhead low, even in demanding networking conditions.

In this paper we present our recent study on the reliability of DAD in ND++. Verification of address uniqueness, being performed through DAD procedure, is the key goal of ND++ protocol. Although ND++ reliability is close to 100% for an ideal channel conditions, it drops in more realistic and demanding networking environments. Therefore, we present here the evaluation of 3 possible methods which increase the probability of a successful duplication detection. We will also elaborate on the tradeoff between increasing protocol reliability and minimizing the imposed overhead. The obtained results reveal the particular protocol set-up which allows for a duplication detection probability that can guarantee proper DAD while keeping protocol overhead low even in the networks with tens and hundreds of nodes. This makes ND++ an interesting solution for future networking focused on the interconnection

M. Grajzer is a scholarship holder within the project "Scholarship support for Ph.D. students specializing in majors strategic for Wielkopolska's development", Sub-measure 8.2.2 Human Capital Operational Programme, co-financed by European Union under the European Social Fund.

The presented work has been funded by the Polish Ministry of Science and Higher Education within the status activity task "Struktura, analiza i projektowanie nowoczesnych systemów komutacyjnych i sieci telekomunikacyjnych" in 2015.

of significant number of mobile, ad hoc devices into the Internet of Things.

This paper is organized as follows: Section II presents the related work and elaborates on the differences with our proposed solution, Section III describes key mechanisms and features of ND++ protocol and Section IV presents possible enhancements to ND++ functionality. Finally the simulation results are presented in Section V. Section VI concludes the paper.

II. Related work

Considering the ND++ protocol and, in particular, the aspects of its reliability, three key groups of reference work can be distinguished as most relevant: 1) the reference IPv6 Neighbor Discovery protocol, 2) enhancements to ND proposed to address particular needs of MANETs and 3) extensions to routing protocols proposed to address also auto-configuration goals. All of them refer to the IPv6-based solutions.

Concerning 1) both the IPv6 ND protocol [6] and the IPv6 SAA procedure [5] were designed for fixed network environments and therefore are limited in scope to the link-local neighborhood. This means that they verify address uniqueness only with "on link" direct neighbors leaving more distant duplications unresolved. Such a situation is not acceptable in MANETs. On a contrary ND++ has wider range covering possibly a whole MANET domain.

The methods from the second group [7]–[11] are characterized by relatively high protocol overhead and are not always capable of being easily deployed with other commonly used IPv6 solutions. Our solution, ND++, can control protocol overhead and keep it at the very low level without the need for external configuration nodes, as reported in [15]. We will evaluate more on the relation between overhead and protocol reliability in this paper. Moreover, ND++ is fully compliant with IPv6 standards and backward compatibility with ND [6] is ensured. The importance of this aspect is also depicted in [3].

Finally, the third group of solutions is focused on the exploitation of OLSR routing protocol [11], [16]. We refer to it, since both in our approach and in OLSR the concept of Multipoint Relays (MPRs) is introduced. However, it is argued [3], [4] that routing and AAC should be independent processes and we follow this approach.

The broad comparison between ND++ and other related works has been presented in [13]. Unfortunately, to the best of our knowledge, none of the authors of reference works targeting MANET environment has published the results reflecting the reliability of the proposed solution. Therefore, in the process of evaluating the reliability of ND++, we will take on an assumption that the reliability should be as close as possible to 100%, with the acceptable deviation of 5-10%. DAD and address uniqueness verification is one of the key networking features and a reliability of this process is influencing many other factors, one of them being routing. Hence, it should be maximized as a top priority goal.

III. Basic ND++ concept

ND++ protocol is aimed at providing DAD capabilities to MANET nodes by extending the range of the Neighbor Discovery protocol in order to cover the whole MANET domain/subdomain, instead of just 1-hop neighborhood of each node. However, with the extended range, the problem of controlling the protocol overhead arises. It is challenging, since AAC is typically the first action the network nodes undertake when they start their operation and at that point unique and confirmed node identifiers are not assigned yet. This prevents the applicability of most flooding mechanisms which rely on a high level structure of overlay nodes (e.g. the MDR mechanism [17]) – due to the fact that these nodes cannot be chosen without operational, unique node identifiers. To address this challenge in ND++ we have proposed to modify ND protocol in such a way that MPR mechanism from the OLSR protocol [18] could be used as a means of restricting unbounded flooding of multihop protocol messages. To the best of our knowledge MPR mechanism is the only solution applicable for being incorporated during SAA procedures.

The above approach is enabled by a 2-step DAD procedure, which is the core part of ND++ [12], [13]. It is denoted as DAD++ and is firstly performed in the range of 1-hop, similarly as in the standard Neighbor Discovery. Secondly, the procedure is repeated in the extended range of *n* hops covering preferably whole MANET domain (n-DAD). Thus, n-DAD is performed by means of sending a query for the address of interest within a specified scope by means of a multihop Neighbor Solicitation (mNS) messages [12], [13], which are similar to the unicast NS messages [5], [6] used at the first DAD++ step.

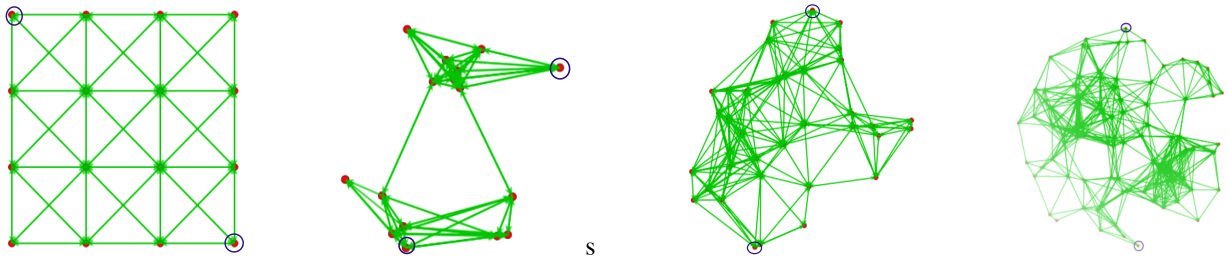
In the meantime, each node in the network collects information about its 2-hop neighborhood by exchanging link-local messages (1-hop scope) with its neighbors [12], [13]. Based on these data it chooses Multipoint Relays (MPRs) – nodes that will forward ND++ information on its behalf, following the heuristic defined in [18] or its modified variant. We will elaborate more on this aspect in Section IV. Having an address verified as unique in the range of 1-hop (which is performed at the first step of DAD++) is sufficient to perform both this kind of information collection and MPR selection process.

Ones MPRs are chosen for each node, they are forwarding packets from their MPR selectors. Our recent results suggested [14], [15] that it should be mandatory with ND++ to detect by each forwarding node the copies of previously forwarded messages and to suppress them. This enables to control protocol overhead and to prevent unrestricted message number increase with the protocol's range increase. In this paper we will present several means of restricting forwarding of the copies of previous messages.

What is important to notice is that ND++ is aimed at verification of address uniqueness, not at the SAA procedure as a whole. Therefore, it is expected that ND++ will be complemented by some additional prefix assignment mechanism to complete SAA and provide each node with a routable IPv6 address.

IV. Methods for increasing DAD reliability in realistic MANET environments

Limiting the number of multicast mNS messages by suppressing all the copies of previous messages during forwarding led to the significant drop in the protocol overhead. It also



(a) Cross-Grid (16 nodes)
(b) Uniform Disc (16 nodes)
(c) Uniform Disc (36 nodes)
(d) Uniform Disc (100 nodes)

Fig. 1. Selected topologies with nodes marked, which are assigned duplicated addresses

allowed for achieving very good, stable and range-independent overhead characteristics under ideal channel conditions [15]. The procedure was performed by inferring in each MPR node that two messages having the same target address (i.e. the address that is being verified), Random ID of the sending node and sequence number are duplicated. We will reference this scheme as a baseline solution further on. Such an approach led to maximal overhead suppression and allowed for achieving reliability of 98-100% for all investigated network sizes and topologies in ideal channel conditions with no path loss and path delay incorporated [19]. Hence, these values refer to the theoretical protocol reliability which is influenced only by the protocol characteristics and other artefacts that are still present at the Internet layer of TCP/IP model (ICMP level).

In real MANET networks, however, many factors that influence networking protocols are related to physical and MAC layers – including, but not limiting to, channel characteristics and MAC collision issues resulting often from the hidden terminal problem (which cannot be easily dealt with in case of multicast transmissions). Our investigations of the ND++ reliability in realistic channel conditions exposed a significant drop in the probability of successful duplication detection to the level of approx. 70% and even below for some topologies [19]. At this stage we have modelled the channel as a log-distance path loss model. We have not taken fading effects into consideration, since on one hand introducing fading channel without the log-distance path loss have not influenced the ND++ reliability and on the other hand fading channels result in both signal degradation and gain. Gain, however, is significantly influencing topology by adding temporary, new, wide-range connections between nodes, whereas for the ND++ evaluation we have taken the objective to keep investigated topologies as stable as possible.

In order to deal with the reliability decrease depicted above we have proposed and investigated three methods for the modification of a forwarding scheme:

- *FRW_COUNT*, which allows for a retransmission by each MPR node of a specified number of copies at most.
- *NDAD_COUNT*, which repeats the n-DAD query several times, similarly to an approach proposed as optional for basic ND protocol [5], [6], with a difference that in ND++ we use it for the second DAD++ stage only. This approach has an advantage over *FRW_COUNT* that in case a positive reply to DAD++ query is received (i.e. duplication was found), the next trials for address verification are neglected. In such a situation the overhead is diminished. Moreover, the additional increased overhead (comparing to the baseline solution) is spanned across wider timeframe than in *FRW_COUNT* variant. However, this is performed on the additional cost of the total time needed to finish DAD++, which to some extend increases and influences protocol latency.
- *USE_SRC_ADDR* – in this variant the detection of copies of previously forwarded messages is done based on the source address instead of a target address. In the verification based on a target address two messages that originated from the same source and reached the current MPR via two different paths are treated as duplicated and only one of them will be forwarded further. The modification to source address comparison enables to keep the multipath message propagation – in the above case two messages from different paths would have different source addresses (since source address is changed during forwarding to the forwarder main address) and are both to be forwarded further. This way we exploit the advantages of multipath propagation, which are particularly important in MANET networks. However, it has to be noticed that the overall protocol overhead is increased.

V. ND++ RELIABILITY EVALUATION

Below we present the simulation-based evaluation of the three ND++ variants presented above and discuss their influence on both ND++ reliability (denoted as the probability of successful duplication detection) as well as protocol overhead and its latency expressed, following [4], as a node timeout to obtain the IP address or to obtain the information that it is already in use by another node (i.e. duplicated).

A. *Simulation environment*

The evaluation was performed in the NS-3 simulation environment [20]. This simulator was chosen since it is one of the biggest and best evolved simulators. It also has a very good IPv6 stack implementation. Therefore we have decided to select NS-3, however we have also been investigating OMNET++ (for details please refer to [21]). An IPv6-only MANET network was modelled in NS-3 with variable number of nodes (16, 36 or 100 nodes). The wireless network was configured as 802.11g network with OFDM mode at the rate of 54Mbps to allow for a maximum throughput. We have investigated 3 different topologies: predefined grid topologies (including the variants with (Cross-Grid) and without (Grid) diagonal connections) and a random node distribution on the disc area (Uniform Disc). The grid-based topologies were selected due to their deterministic characteristics allowing for scaling them and thus for comparing results between topologies with different number of nodes but with a similar layout. The random Uniform Disc is a good representative of random topologies, which allows to obtain connected graph topologies regardless of node count with a straightforward setup. Selected topologies are presented in Fig. 1. For the protocol overhead experiments the 95% confidence intervals of the t-Student distribution were monitored – the simulation run was terminated when the half of the confidence interval length was within 10% of the estimated average value. Initially 10 data points were collected for each averaged value, but this number was increased if necessary to meet the 10% criterion. For more details on the experiment organization please refer to [14], [21].

B. Probability of successful DAD

For the purposes of evaluating ND++ reliability the investigated scenarios were reflecting a situation when a selected node has been assigned a new address and was verifying its uniqueness by means of ND++ DAD++ procedure [12], [13]. The new address is duplicated and already belongs to another node in this network. These two nodes are selected so that their distance (in terms of the number of hops) is possibly large given particular topology (see Fig. 1). The reliability experiments were performed with a 50 times repetition count – each time a single query for a single address was sent and the result was recorded as either "*duplication detected – address invalid*" or "*duplication not detected – address confirmed*". As such the resulting probability levels (expressed in %) have accuracy of 2%. The results were colected vs. the *HopLimit* parameter specifying protocol's range in terms of the number of hops each multihop ND++ message can reach.

Our previous results on the probability of duplication detection, reported briefly in [19], were affected by the simulator misconfiguration issue which caused background MPR selection overhead to raise significantly and was a source of increased number of collisions, which are normally not present. In this paper we not only provide updated results but, moreover, investigate in more detail relationships influencing ND++ reliability and present new findings and conclusions.

The new experiment results obtained under realistic channel conditions, described in more detail in Section IV, reveal the drop in the overall performance (probability of successful duplication detection) (please see Fig. 2 for reference). The drop resulted in the probabilities of about 80-90% for Grid and Uniform Disc topologies and even as low as approx. 60% for Cross-Grid topology. Approximately similar levels are obtained regardless of a node count in the network, which suggests that the reason for this effect is related to the impact of channel drops and collisions on the fundamentals of flooding processes. Interestingly, Cross-Grid topology was giving the best results under ideal channel conditions (it has small diameter, short end-to-end paths, only few MPRs). Though, our detailed analysis has shown that the particular characteristic of this topology, which made it very successful in ideal conditions, is the source of its performance drop in realistic conditions. In this topology during MPR selection procedure the nodes connected through diagonal links become preferred by the MPR selection algorithm because they provide connection to many other nodes (especially for the nodes at the edge of the network). However, these connections are weak, since the wifi signal strength is counter-proportional to the node distance. As such connections with the MPRs, which are the most crucial for successful flooding, are composed of the weak links on which the drops are likely to occur. This effect can corrupt the MPR-based flooding if there are not many MPRs in a network.

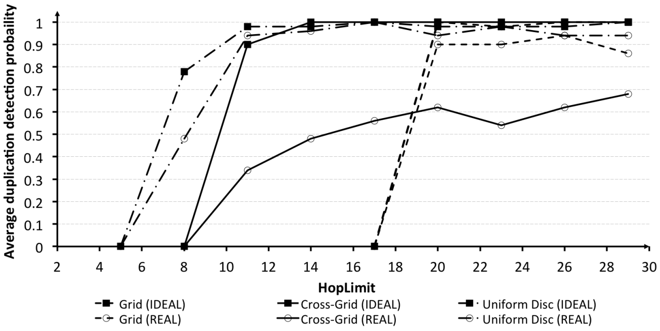
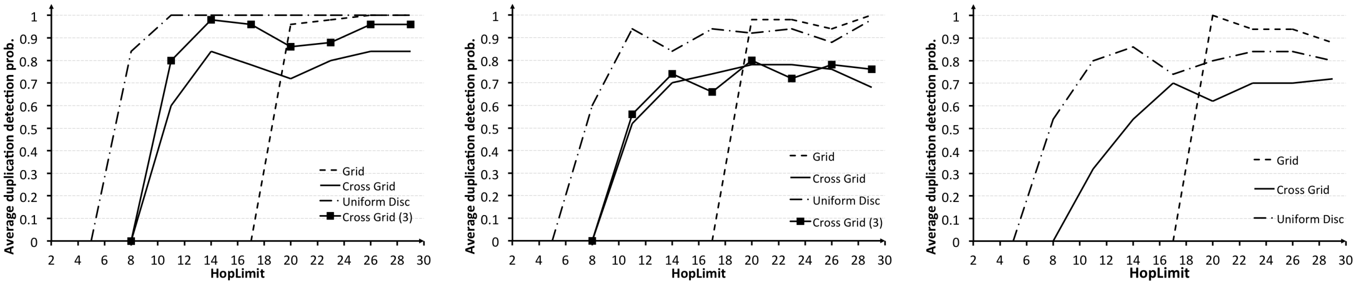


Fig. 2. Probability of successful duplication detection during single DAD++ query for a single address vs. *HopLimit* in a 100 node network for selected topologies – comparison between ideal and realistic channel

In Fig. 3 we present selected results for a 100 node network depicting probability of successful duplication detection as a function of a *HopLimit* parameter in each of the 3 investigated flooding variants (*NDAD_COUNT*, *FRW_COUNT* and *USE_SRC_ADDR*). *NDAD_COUNT* was performed with 2 consecutive repetitions of n-DAD, similarly to *FRW_COUNT*, which allowed for maximum 2 copies of each packet. For Cross-Grid topology additional result is given with the values of 3 instead of 2 for *NDAD_COUNT* and *FRW_COUNT* accordingly. *USE_SRC_ADDR* variant does not have any parametrized features, however it can be combined with one of the other two approaches. We have investigated several options with a goal to reach performance of 90% and above.

Each of the investigated flooding modifications led to the better ND++ performance, in terms of reliability assessment, in each of the investigated topologies and network sizes. However, the Cross-Grid topology required more effort in order to achieve duplication detection probabilities at the levels exceeding 90% – *NDAD_COUNT* with 3 consecutive repetitions of n-DAD. *FRW_COUNT* variant, even while allowing for 3 copies of each packet, did not manage to reach this threshold. Similar conclusions can be drown for *USE_SRC_ADDR* variant. For Grid and Uniform Disc the results close to 100% were achievable for both *NDAD_COUNT* and *FRW_COUNT* with the parameter of 2 (as specified above).

Comparing the 3 proposed flooding restriction variants it can be concluded that *USE_SRC_ADDR* was not able to meet our goals and cannot be used as a standalone ND++ option, only as possible supporting solution to one of the other two investigated methods. Moreover, *NDAD_COUNT* variant provided the best results in all investigated topologies and



(a) *NDAD_COUNT*

(b) *FRW_COUNT*

(c) *USE_SRC_ADDR*

Fig. 3. Probability of successful duplication detection during single DAD++ query for a single address vs. *HopLimit* in a 100 node network with realistic channel – comparison between *NDAD_COUNT*, *FRW_COUNT* and *USE_SRC_ADDR* variants

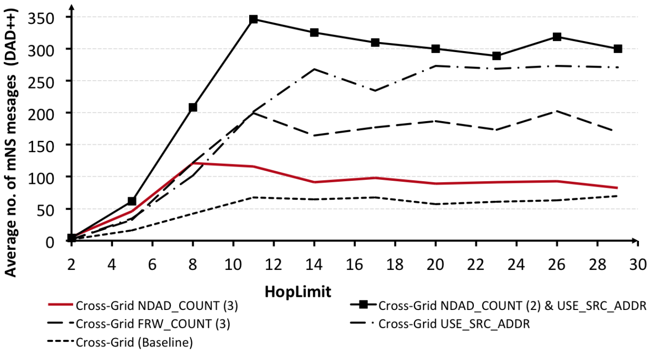


Fig. 4. Number of *mNS* messages generated during DAD++ in realistic environment with a single duplication in a network vs. *HopLimit* for 100-node network

network sizes with excellent results for Grid and Uniform Disc topologies at the levels of almost 100% even in 100-node network. It also provided very good results for the Cross-Grid topology with number of consecutive n-DAD trials increased to 3. Considering these findings and the benefits of this solution over *FRW_COUNT* depicted in Section IV, we recommend to use this option as a standard ND++ behaviour. The number of consecutive trials may be a configurable parameter which could be set accordingly considering the particular network type and topology under consideration.

Interestingly, *NDAD_COUNT* with 2 n-DAD trials combined with *USE_SRC_ADDR* option gave the results similar to *NDAD_COUNT* with 3 n-DAD trials for each network size and Cross-Grid topology. However, it seams that the features of *NDAD_COUNT* method allowing to finish DAD++ earlier if the positive reply is received would possibly allow for achieving better overhead levels in practical solutions, hence we recommend this solution as preferable.

C. Protocol overhead and latency

While assessing ND++ reliability and possible methods for its improvement it is also important to investigate the protocol overhead imposed by each of the proposed methods. For this purpose we have simulated ND++ in realistic networking conditions in a similar scenarios as depicted above. For each experiment we have measured a number of mNS messages generated in the entire network during a full DAD++ query for a single IPv6 address. A single duplication was present in a network – as such the total ND++ overhead generated in the address query would be approximately twice the one obtained for mNS messages (mNS are used to send an address query, similar mechanism is used to send a reply, but multihop Neighbor Advertisement messages are sent [12], [13]). The results were obtained with the accuracy control method similar to the one presented in [14], with an exception for the *NDAD_COUNT* case, where the total overhead values may vary significantly when the duplication is detected fast and remaining n-DAD trials are neglected. In such a case accuracy control could not be operational, since the diversity of the results in principle can be high. However, to ensure reliability of the results, 30 similar trials are averaged to obtain final estimated values, while in most cases with accuracy control 10 trials are enough.

The results reveal more diversity than the ones for an ideal channel conditions, mentioned in [15], however the general upper-bounded characteristic is kept and the curves are approximately linear for the *HopLimit* values large enough to cover whole MANET network. In Fig. 4 we present an exemplary comparison of the overhead estimation for a selected 100-node Cross-Grid topology – the most demanding among the investigated cases. The comparison is made between baseline protocol setup, *NDAD_COUNT* variant with 3 trials, *FRW_COUNT* variant with 3 duplications allowed and a combination of *USE_SRC_ADDR* and *NDAD_COUNT* variant with 2 trials. The findings reveal that a standalone *NDAD_COUNT* variant generates much less overhead than a combined *NDAD_COUNT* and *USE_SRC_ADDR* solution, which confirms our suggestion from Section V-B to select *NDAD_COUNT* as a standard ND++ behaviour.

In diversified network types and sizes the evaluation of the ND++ overhead has shown that *NDAD_COUNT* is the best option not only concerning the probability of duplication detection but also the message count. In general, achieved results do not exceed approx. 170 mNS messages per whole DAD++ procedure in a 100-node network (for Grid topology, comparing to about 90 frames in the baseline scenario). This level corresponds to approx. 20kB of total traffic leading to 200B (1.6kbits) per node, which is a very good result. Other variants generate higher overhead, especially *USE_SRC_ADDR* generates on average twice the traffic of *NDAD_COUNT* variant. This holds true for all network sizes and topologies.

One possible concern with the *NDAD_COUNT* option is the aspect of the protocol latency. While n-DAD queries are repeated several times in this approach the total time needed for ND++ to verify the address increases. Typically with each trial it increases for the time specified as the value of *NDAD_RETRANS_TIMER*, which is a configurable parameter. In the investigated ND++ set-up it is set to 1s. Hence with each new n-DAD trial DAD++ is prolonged for an additional 1s at most (if a reply with information about duplicated address arrives, it is shorter). Whole DAD++ in the current set-up takes minimum 5s and maximum 7s for Cross-Grid topology and 3 consecutive n-DAD trials. These values could be smaller, since they are all based on configurable parameters. In the currently investigated scenarios latency was not critical, however if shorter DAD++ times are required, it is possible to achieve it with ND++ on the cost of additional overhead for MPR selection traffic. This is due to the fact that MPR messages have to be exchanged fast enough to enable for MPR selection within the timeframes specified by DAD++ scheduled procedures. For the currently investigated scenarios the ND++ latency seems to be sufficient, especially taking into account that the valid link-local address can be confirmed within the time of 1s, right after 1-hop DAD procedure is finalized.

VI. Conclusions

The presented research was aimed at evaluation and selection of one of the ND++ flooding variants that would ensure protocol reliability in realistic MANET environments while keeping protocol overhead low. Among three investigated options (*NDAD_COUNT*, *FRW_COUNT* and *USE_SRC_ADDR*) the *NDAD_COUNT* variant was assessed as the best solution providing a good balance between maximizing ND++ reliability and minimizing overhead and protocol latency. In the optimal set-up it allowed to achieve reliability levels between 90% and 100% with the overhead not exceeding approximately two messages per node (four in case of the presence of duplication in a network), which is a very good result. *NDAD_COUNT* variant can be parametrized in order to address the needs of particular network environments. Our findings present that in most cases repeating n-DAD query for an address for 2 times is enough. The obtained ND++ message count is low enough to allow for even higher settings without the concern of generating too much protocol overhead, which could have negative impact on the other network functions. Hence, it can be observed that the reliability levels are asymptotically approaching 100% with the increased number of n-DAD trials needed to finalize DAD++ procedure. However, the protocol latency should be also considered while increasing the number of mandatory n-DAD trials, since significant values could lead to undesirable increase in protocol latency. In general the properties of ND++ with the *NDAD_COUNT* option included make it a very good solution addressing the needs of many diversified practical MANET set-ups. Therefore, we would see it as a good basis for building self-configuration services for the Future Internet and the Internet of Things.

References

[1] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[2] OECD, "Machine-to-Machine Communications. Connecting Billions of Devices," OECD Digital Economy Papers, No. 192, OECD Publishing, Jan 2012. [Online]. Available: /content/workingpaper/5k9gsh2gp043-en

[3] E. Baccelli, "Address Autoconfiguration for MANET: Terminology and Problem Statement draft-ietf-autoconf-statement-04," IETF Internet Draft (Work in progress, Expired), February 2008, https://tools.ietf.org/html/draft-ietf-autoconf-statement-04.

[4] L. J. García Villalba, J. García Matesanz, A. L. Sandoval Orozco, and J. D. Márquez Díaz, "Auto-configuration protocols in mobile ad hoc networks," *Sensors*, vol. 11, no. 4, pp. 3652–3666, 2011.

[5] S. Thomson, T. Narten, and T. Jinmei, "RFC4862: IPv6 Stateless Address Autoconfiguration," IETF Draft Standard, September 2007, http://www.rfc-editor.org/rfc/rfc4862.txt.

[6] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "RFC4861: Neighbor Discovery for IP version 6 (IPv6)," IETF Draft Standard, September 2007, http://www.rfc-editor.org/rfc/rfc4861.txt.

[7] K. Weniger and M. Zitterbart, "IPv6 autoconfiguration in large scale mobile ad-hoc networks," in *Proceedings of European Wireless*, vol. 1, 2002, pp. 142–148.

[8] ——, "IPv6 stateless address autoconfiguration for hierarchical mobile ad hoc networks," IETF Internet Draft (Work in progress, Expired), February 2002, http://tools.ietf.org/id/draft-weniger-manet-addressautoconf-ipv6-00.txt.

[9] X. Wang and H. Qian, "Dynamic and hierarchical IPv6 address configuration for a mobile ad hoc network," *International Journal of Communication Systems*, vol. 28, no. 1, pp. 127–146, 2015. [Online]. Available: http://dx.doi.org/10.1002/dac.2643

[10] J. Park, Y. Kim, and S. Park, "Stateless address autoconfiguration in mobile ad hoc networks using site-local address," IETF Internet Draft (Work in progress, Expired), July 2001, http://tools.ietf.org/id/draft-park-zeroconf-manet-ipv6.

[11] S. Boudjit, A. Laouiti, P. Muhlethaler, and C. Adjih, "Duplicate address detection and autoconfiguration in OLSR," *Journal of Universal Computer Science*, vol. 13, no. 1, pp. 4–31, 2007.

[12] M. Grajzer, "ND++ - an extended IPv6 Neighbor Discovery protocol for enhanced duplicate address detection to support stateless address autoconfiguration in IPv6 mobile ad hoc networks." IETF Internet Draft (Work in progress), March 2011, http://tools.ietf.org/html/draft-grajzer-autoconf-ndpp-00.txt.

[13] M. Grajzer, T. Żernicki, and M. Głąbowski, "ND++ – an extended IPv6 Neighbor Discovery protocol for enhanced stateless address autoconfiguration in MANETs," *International Journal of Communication Systems*, vol. 27, no. 10, pp. 2269–2288, 2014. [Online]. Available: http://dx.doi.org/10.1002/dac.2472

[14] M. Grajzer and M. Głąbowski, "Performance evaluation of Neighbor Discovery++ protocol for the provisioning of self-configuration services in IPv6 mobile ad hoc networks," in *Telecommunications Network Strategy and Planning Symposium (Networks), 2014 16th International*. IEEE, 2014, pp. 1–6.

[15] ——, "Enhanced Stateless Address Auto-configuration solution for low-overhead network self-configuration in IPv6 mobile ad hoc networks," in *Proceedings of the 2015 IEICE General Conference, ISSN 1349-1377*, Japan, 10-13 March 2015.

[16] S. Boudjit, C. Adjih, A. Laouiti, and P. Muhlethaler, "A duplicate address detection and autoconfiguration mechanism for a single-interface OLSR network," in *Technologies for Advanced Heterogeneous Networks*. Springer, 2005, pp. 128–142.

[17] R. Ogier and P. Spagnolo, "RFC 5614: Mobile Ad Hoc Network (MANET) Extension of OSPF Using Connected Dominating Set (CDS) Flooding," IETF Draft Standard, August 2009, http://wiki.tools.ietf.org/html/rfc5614.

[18] T. Clausen and P. Jacquet, "RFC3626: Optimized Link State Routing Protocol (OLSR)," IETF Draft Experimental, October 2003, http://www.rfc-editor.org/rfc/rfc3626.txt.

[19] M. Grajzer and M. Głąbowski, "On the probability of duplicate address detection with Neighbor Discovery++ protocol in IPv6 mobile ad hoc networks," in *Proceedings of the 2015 IEICE General Conference, ISSN 1349-1377*, Japan, 10-13 March 2015.

[20] "NS-3 simulator website." [Online]. Available: http://www.nsnam.org

[21] M. Grajzer and M. Głąbowski, "On IPv6 experimentation in wireless mobile ad hoc networks," *Journal of Telecommunications and Information Technology (JTIT)*, vol. 3/2014, pp. 71–81, 2014.