Anticipated DAD for Global Connectivity in Hybrid MANETs

Alicia Triviño-Cabrera, Gonzalo Casado-Hernández, Eduardo Casilari, Francisco J. González-Cañete
Dpto. Tecnología Electrónica
Universidad de Málaga
Spain
atc@uma.es

Abstract— **Several schemes that provide the integration of MANET into external networks have been developed. These protocols are fundamentally based on the discovery of an Internet Gateway that supports the ad hoc routing functionalities as well as the dissemination of the IPv6 prefix information to enable stateless address auto-configuration in the mobile nodes. However, most of these schemes neglect the consequences of the DAD (Duplicate Address Detection) procedures that the devices should perform in order to verify the uniqueness of the self-configured IPv6 address. The aim of this paper is the analysis of the DAD technique in scenarios with multiple points of attachment under the global connectivity paradigm. Additionally, anticipated DAD is proposed in order to avoid significant delays associated to the timers that conventional DAD employs.**

Index Terms— **MANET, Global Connectivity, Internet, Gateway, DAD.**

I. INTRODUCTION

The development of light-weighted mobile devices in conjunction with the increment of their computational power has allowed the pervasive computing. Under this new paradigm, MANETs (Mobile Ad hoc Networks) must be adapted to support the integration to external networks as the Internet.

This integration introduces different challenging issues as the address auto-configuration. With this technique, mobile nodes generate an IP address that allows them to be reachable from any external Internet node. Following the autonomous philosophy associated to the MANET essence, a stateless configuration seems to be the most adequate strategy for this type of networks [1]. The self-configuring process is usually initiated by acquiring one prefix appropriate to the network. This prefix information could be broadcasted by the Internet Gateway responsible for the corresponding domain where the node resides. Once the device receives the information, it generates a global IPv6 address by concatenating a random value, for example the EUI-64 MAC identifier, to the prefix to be utilized. As the concatenated information could be maliciously altered or extracted from different sources even randomly, this operation does not ensure the uniqueness of the address as in a state-full configuration such as DHCP [2]. Therefore, mobile nodes should trigger a Duplicate Address Detection (DAD) to confirm that the selected address is not in use by any other node.

One of the most extended techniques for DAD was proposed in [3]. Following this technique (the so-called try-and-wait DAD), nodes wishing to acquire a global IPv6 address request a route to a hypothetic node that possesses the self-generated address. If no response is received during an interval of time (T_{DAD}), the node will assume that the address is unique within the MANET. The main drawback of this technique is related to the fact that a node may interrupt external communications during the T_{DAD} interval whenever it decides to change its point of attachment to the exterior. Since the decision of selecting a new Internet Gateway is strongly dependent on the mechanism employed to obtain the global connectivity, in this paper the authors analyze the consequences of DAD for two relevant supports: the global connectivity [4] and the prefix continuity [5].

Additionally, authors propose the employ of a new technique based on that exposed in [6] that may suppress the interruption of the communications produced by try-and-wait DAD. This new scheme is based on the anticipation of the DAD procedures.

In this work, only pre-service DAD is considered, that is, nodes only verify the uniqueness of the address when they construct a tentative address. The in-service technique or the procedures by which a mobile device continuously checks whether its address is not in conflict with some other existing terminals is regarded as out of scope. Although this verification is also appropriate in real scenarios where mergings or unions of MANETs are present, we consider that the utilization of a conflict-detection procedure that monitors the traffic is a better option [7].

The rest of the paper is organized as follows. In section 2, some relevant mechanisms that allow the global connectivity in MANETs are presented. Section 3 explains the different DAD techniques that can be applied into this type of networks. In Section 4, the anticipated DAD is presented. Section 5 exposes the simulation results obtained in order to verify the forthcomings of the proposed DAD. Finally, in Section 6 the paper is concluded.

II. GLOBAL CONNECTIVITY

In order to achieve global connectivity in a multi-hop ad hoc network, an Internet Gateway should be incorporated. The main characteristics of this new element as well as its utilization differentiate the developed mechanisms.

Most of the proposals are based on an entity with restricted or even no mobility which is specifically placed to act as the Internet Gateway. The Gateway is in charge of propagating the prefix information by the emission of Modified Router Advertisements or MRA messages [4]. This functionality could be accomplished in similar ways to the route discovery associated to MANETs, that is, periodically or proactively, under reactive manner or on-demand and finally, using an hybrid approach that combines the previous strategies.

The most extended mechanism is referenced as the global connectivity [4]. This scheme is based on a fixed gateway that is located in the coverage area of the Access Router. The presence of multiple gateways emitting different MRA messages may produce a significant load in the network. In order to reduce this effect, there exists another proposal where mobile nodes only broadcast the MRA associated to the selected gateway. With this operation, mobile nodes form a continuous path to the Gateway that is comprised of devices which share the same prefix. This could be considered a simplification of the prefix continuity mechanism proposed in [5].

In scenarios where multiple gateways coexist, mobile nodes usually base the best gateway selection on the number of hops, as most routing protocols do. However, some other criteria could be applied.

Both previous supports share a clear inconvenience as they do not analyze the effects that the address auto-configuration provokes when switching between two different gateways occurs. One of the supports that does take into consideration these consequences is presented in [7]. This mechanism is specifically intended for scenarios where multiple fixed gateways provide access to the Internet. These elements periodically announce their prefixes through MRA messages so that nodes receiving this information generate the corresponding IPv6 addresses even if they are not going to employ them immediately. As nodes possess IPv6 addresses appropriate to more than one gateways in the MANET, they can dynamically change the global address that they utilize for their external communications if, for example, one gateway ceases to be operative. This anticipated characteristic seems to be quite advantageous in mobile networks in order to reach a seamless switching. However, the authors of this proposal consider the verification of the uniqueness of the IPv6 address out of scope.

III. DAD (DUPLICATE ADDRESS DETECTION)

In a stateless address auto-configuration, mobile nodes receive the prefix information related to the network where they are placed. With this information, they could construct an IPv6 address by concatenating certain data that is considered to be globally unique, for example, the IEEE MAC identifier. However, the self-generated IPv6 address is not guaranteed to be unique due to several reasons. Firstly, terminals with duplicate MAC address exist on the market because of non-registered or erroneously manufactured devices. On the other hand, users may intentionally alter the configured IPv6 or MAC address. In addition, the use of globally unique ID as part of the IPv6 address is not generally accepted as this utilization eases the users tracking, which may imply negative consequences on their privacy [8].

Therefore, if intrusions are desirable to be suppressed in the communications, a new mechanism should be applied after the address auto-configuration. This new technique is called pre-service Duplicate Address Detection (DAD) as the nodes check the validity of the self-configured IPv6 address before utilizing it. Additionally, DAD could be also applied continuously in order to ensure the uniqueness of the IPv6 address in those scenarios where mergings of MANETs that share the same prefix are expected to occur. This strategy is called the in-service or strong DAD as meanwhile nodes utilize the IPv6, they may perform it. In our opinion, in-service DAD could be suppressed by some other strategies as Weak DAD [9]

One of the most extended techniques for DAD was proposed in [3]. Following this technique (the so-called try-and-wait DAD), a node wishing to acquire a global IPv6 address requests a route to a hypothetic device that possesses the self-generated address. If no response is received during an interval of time (T_{DAD}), the node will assume that the address is unique within the MANET. Despite of its simplicity, its main drawback is related to the fact that nodes may interrupt external communications during the T_{DAD} interval. In scenarios with multiple Internet Gateways where mobile nodes connects through different points of attachment, this time, usually 1 second, causes noticeable latencies and may even provoke the break of the on-going connections. This inconvenience has been the main reason for the proposal of some other techniques that behave in a reactive way, i.e., nodes do not check the uniqueness of the chosen address but must test the packets in order to detect potential address conflict. Additionally to the difficulties associated to the discovery of these conflicts, the reactive strategy causes unnecessary computational work that implies gratuitous power consumption.

IV. ANTICIPATED DAD

Mobile nodes in a MANET may receive multiple MRA messages originated by different gateways. Each of these messages announces diverse prefix network information which can be employed by the devices in the auto-configuration procedures in order to obtain a topological correct IPv6 address. By the conventional try-and-wait DAD, nodes select the gateway that it considers to be the best one according to some criteria. After this decision is performed, it may exclusively initiate the DAD procedure associated to the prefix information received from the selected gateway. The rest of the information extracted from the other MRA messages is discarded.

Alternatively, [6] explains a scheme where mobile nodes utilize all the MRA messages to construct an adequate IPv6 address associated to each of them without the utilization of any DAD technique. By this method, devices possess configured IPv6 addresses even if they do not employ them immediately. In this paper, we study the inclusion of the simple try-and-wait DAD procedures in this scheme. Although time-outs periods are still present in the method, since nodes do not usually require the IPv6 address that is being configured, on-going communications are not interrupted. At the moment that

nodes switch the gateway to utilize, the IPv6 address associated to the new gateway that is going to be employed is already available.

In order to accomplish this task, nodes should include certain computational structures as it is proposed in [6]. Firstly, they should incorporate the PIB (Prefix Information Base) where nodes associate the prefix information received in the MRA messages to the configured IPv6 address. For each entry in the PIB, a flag indicates if the DAD procedure is being performed.

When a modification in this structure occurs (a new IPv6 address is constructed or a previous one is not valid any longer), the mobile node notifies this change to the rest of the MANET by the emission of a MID (Multiple Interface Declaration) message [10]. Although this type of message was originally proposed in the OLSR (Optimized Link State Routing), we include them as part of the mechanism for the anticipated DAD. This message informs about the IPv6 addresses that a node possesses. By the analysis of these MID messages, the nodes maintains the MAAIB (Multiple Address Association Information Base) updated. In this structure, an association among the multiple addresses that a device may configure is established. This table indicates the address to look up at the routing table to forward the corresponding packets to a certain node.

The MAAIB is also revised when the mobile device generates a new IPv6 address. Previously to the emission of the RREQ to the hypothetic node with the same IP address, it checks if there exist any other node with the same IPv6 address stored in this table.

V. SIMULATION RESULTS

Due to the difficulties associated to real tests, the improvements of anticipated auto-configuration have been verified by the use of simulations. It was necessary to develop a software module that includes the anticipated DAD in the global connectivity mechanism as well as in the prefix continuity support. This module has been integrated into the Network Simulator tool, ns-2.29 on Linux [11].

The simulation scenarios consider a 2500 m x 500 m area where two gateways are located in the extremes of the surface. The ad hoc network is formed by 50 mobile nodes whose movements are based on the commonly used Modified Random Way-Point model, an extension of the conventional Random Way-Point with a minimum speed to ensure the stability of the results [12]. To evaluate different mobility scenarios, we have varied the maximum speed as shown in Table 1. In order to reach stability in the results, nodes movements are initiated with the Michigan Distribution Function [13].

The traffic is associated to 10 CBR sources with a rate of 4 packets/second. The origin of the sources corresponds to a mobile node from the MANET meanwhile the destination is a device that belongs to a fixed network and must be accessed through the access router.

Table 1 summarizes the parameters used in the simulations.

TABLE 1. SIMULATION PARAMETERS

Simulation Area	2500 m x 500 m
Mobile nodes	50
Gateways	2 GWs fixed at (100m, 250m) and (2400m, 250m)
Mobility pattern (Random WayPoint)	Maximum speed: [1, 10] m/s. Minimum speed = 1 m/s Pause Time : 0 seconds
Traffic pattern	10 CBR sources to an external host Rate = 4 packets/s Packet size= 512 B
Simulation Time	2500 s
Transmission Range	250 m
Runs per point	3
Ad hoc protocol	AODV
Internal Queue	64 packets
MRA interval	10 seconds

The obtained data are represented in Figures 1 to 6. In these figures, we include the results for the mechanism when no DAD technique is employed. These results could be considered the theoretical optimal limit that the support could reach when no duplicate address assignment occurs. In addition, we compare the results of our proposal to the performance of the mechanism when conventional or try-and-wait DAD is employed. To facilitate the understanding and to show the general tendencies of the evaluated algorithms, the results of the different simulations have been also summarized through a linear regression, resulting in the straight lines of the figures.

The performance of this technique has been quantified by the estimation of the following metrics:

- Percentage of Lost Packets. It is defined as the ratio between the lost data packets and the data packets generated by the sources in the MANET. In our case, the number of packets that reach the corresponding Internet node is equivalent to the number of data packets received at the Access Routers as neither loss nor delays are assumed in the external Internet route.
- End-To-End Delay. It represents the average value of the time that the received data packets take to reach the destination from their origin. This parameter includes the time the nodes stay in the internal queues, the retransmissions at the MAC level, and the forwarding through multiple intermediate nodes.
- Normalized Overhead. It corresponds to the ratio between the total control packets and the received data packets. Each hop of any control packet between two nodes is computed as a new control packet.

As an initial step, we analyze the performance of the global connectivity mechanism in its proactive gateway discovery. The results are shown in Figures 1, 2 and 3. The above-mentioned metrics increase when the mobility of nodes is higher. This behavior is supported by the fact that when nodes change their position frequently, the known routes becomes invalid soon. Therefore, nodes should perform a route

discovery process meanwhile the packets are stored in their internal queues so that overhead and delay increase. Prior to the detection of the route breakage, data packets could have been dropped, circumstance that may imply a higher ratio of lost packets.

The dependence on the speed is higher when the conventional DAD is employed. This effect is due to the timeout periods associated to the gateway switchings that interrupt the on-going sessions. Delay is increased meanwhile the packets are stored and even some of them are dropped if the buffer space becomes complete. As a lower number of packets are received, the inclusion of conventional DAD also leads to a higher normalized overhead. If we consider the number of control packets, the results are similar when we apply the two studied DAD strategies.

Anticipated DAD results show a similar performance to the optimal case considering the above-mentioned metrics when no DAD is executed but, in addition, the verification of the uniqueness of the configured IPv6 is executed.

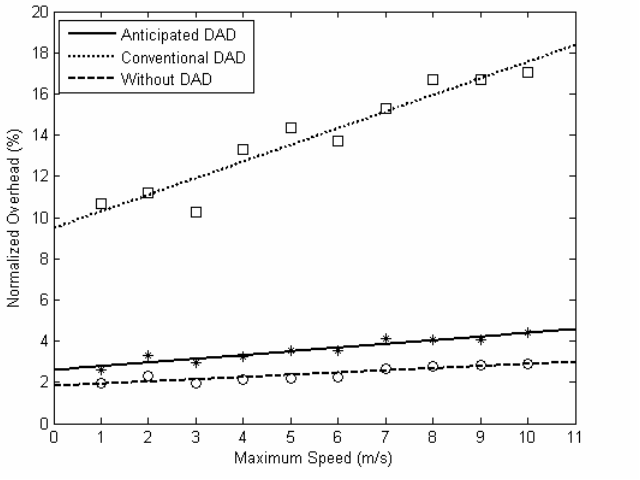

Figure 3. Normalized Overhead as a function of the maximum Speed in the Global Connectivity Mechanism

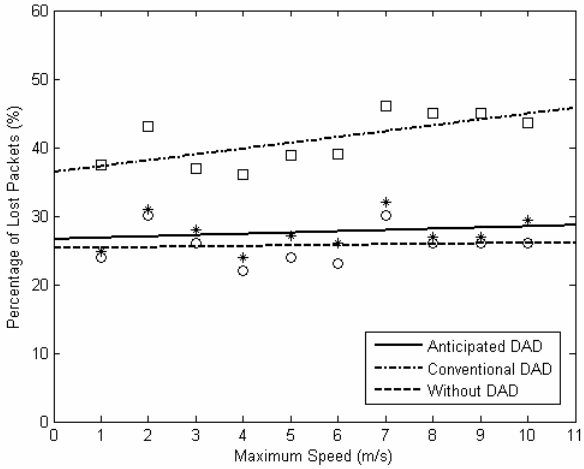

Figure 1. Percentage of Lost Packets as a function of the maximum Speed in the Global Connectivity Mechanism

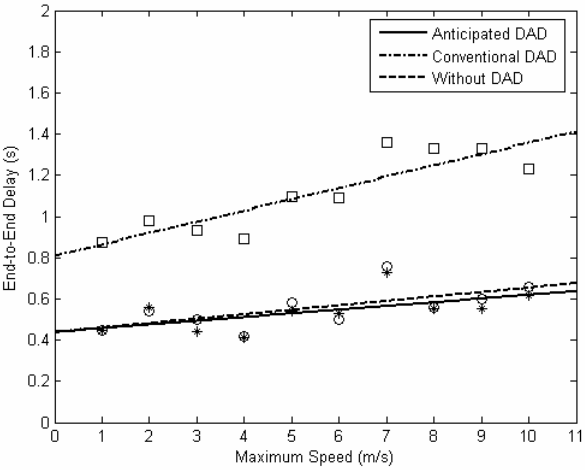

Figure 2. End-to-End Delay as a function of the maximum Speed in the Global Connectivity Mechanism

Considering the prefix continuity as the mechanism for the integration of MANETs into the Internet, we can notice that the behavior is similar to the obtained by the global connectivity. Anticipated DAD clearly reduces the negative consequences associated to the verification of the uniqueness of the configured IPv6 address by the conventional DAD. The results are shown in Figure 4, 5 and 6.

Therefore, the anticipated DAD leads to an improvement of the performance of the network in the two supports considered for the integration of MANET into external networks.

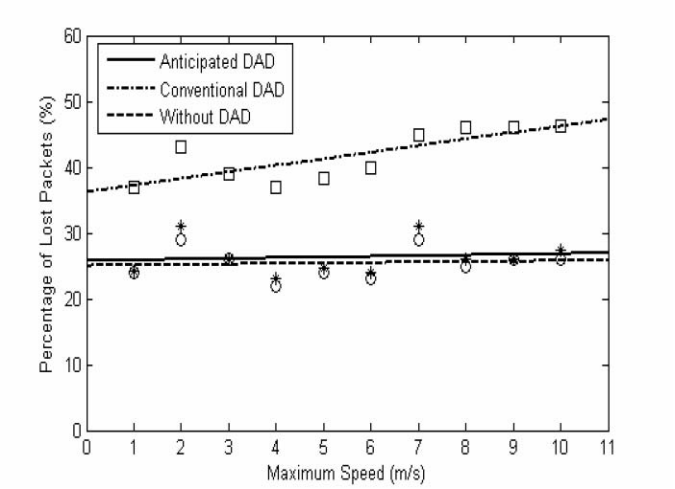

Figure 4. Percentage of Lost Packets as a function of the maximum Speed in the Prefix Continuity Mechanism

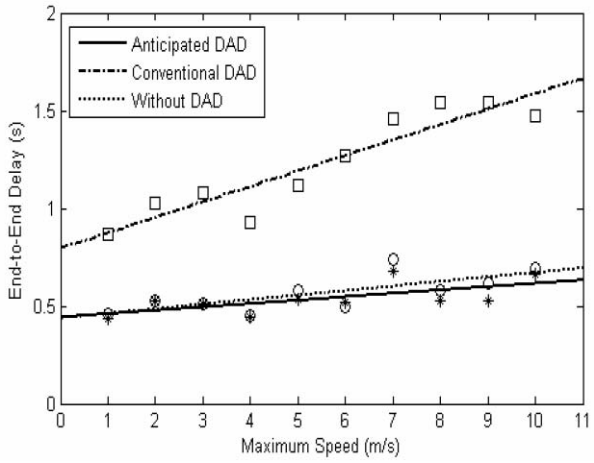

Figure 5. End-to-End as a function of the maximum Speed in the Prefix Continuity Mechanism

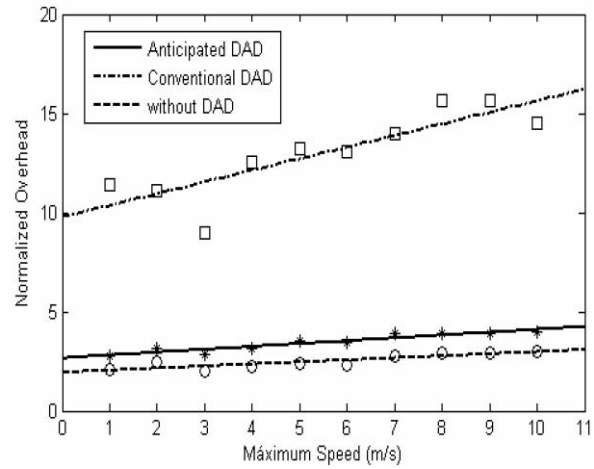

Figure 6. Normalized Overhead as a function of the maximum Speed in the Prefix Continuity Mechanism

VI. CONCLUSIONS

In this paper, an anticipated DAD has been included in the global connectivity mechanism for the integration of MANETs into external networks. This technique suppresses the waiting time associated to the try-and-wait DAD. The improvement of this inclusion is shown by the comparison to the conventional procedure. In addition, the application of this technique implies a performance similar to the theoretical limit obtained by the utilization of the MANET without DAD.

REFERENCES

[1] S. Thomson, T. Narten, "IPv6 Stateless Address AutoConfiguration", IETF RFC 2462, 1998.

[2] S. Alexander, M. Droms, "DHCP Options and BOOTP Vendor Extensions", IETF RFC 2132, March 1997

[3] C. Perkins, R. Wakikawa, J. Malinen, E. Belding-Royer, Y. Suan: "IP Address Autoconfiguration for Ad Hoc Networks", IETF Draft, work in progress, November 2001

[4] R. Wakikawa, J. Marinen, C. Perkins, A. Nilsson, A. J. Tuominen" Global Connectivity for IPv6 Mobile Ad hoc Networks", IETF Internet Draft, work in progress, January 2005.

[5] C. Jelger, T. Noel, A. Frey, "Gateway and address autoconfiguration for IPv6 adhoc networks", IETF Internet Draft, work in progress, October 2003.

[6] S. Ruffino, P. Stupar, "Automatic configuration of Ipv6 addresses for MANET with multiple gateways", IETF Draft, work in progress, February 2006.

[7] K. Weniger, "Passive Duplicate Address Detection in Mobile Ad hoc Networks", In Proceedings of IEEE Wireless Communications and Networking Conference (WCNC) 2003, New Orleans, USA, March 2003.

[8] T. Narten, R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", IETF RFC 3041, January 2001.

[9] N. Vaidya, "Weak Duplicate Address Detection in Mobile Ad Hoc Networks", in Proceedings of MOBIHOC'02, 2002.

[10] T. Clausen, P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", IETF RFC 3626, October 2003.

[11] K. Fall., K. Varadhan., "Ns Notes and Documentation", The VINT Project. UC Berkeley, LBN 2005.

[12] J. Yoon, M. Liu, B. Noble, "Random waypoint considered harmful", in Proceedings of Infocom'03, pp. 1312-1321, San Francisco. April 2003.

[13] E. Hyytia, P. Lassila, L. Nieminen, J. Virtamo, "Spatial Node Distribution in the Random WayPoint Mobility Model", IEEE Transactions on Mobile Computing, vol no. 56, pp. 680-694, June 2006.

[14] C. Perkins, E. Belding-Royer, S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", IETF RFC 3561, July 2003.