Study of Gateway Selection Criteria in Hybrid MANETs

Alicia Triviño-Cabrera, Gonzalo Casado-Hernández, Eduardo Casilari, Francisco J. González-Cañete
Dpto. Tecnología Electrónica, Universidad de Málaga (SPAIN)
Phone: +34-952137191, Fax: +34-952131447, e-mail: atc@uma.es

***Abstract* — Internet Connected MANETs require the utilization of specific Gateways that enable mobile nodes to exchange packets with external hosts. With this purpose, the Gateways are responsible for providing the mobile nodes of the necessary information to allow the construction of a valid global IP addresses. In some scenarios, mobile nodes may be reachable from different Internet Gateways. Under these circumstances, the mobile node should decide which the best gateway is according to certain metrics. In this paper, two criteria for gateway selection are analyzed. First, the commonly utilized criterion of minimum number of hops to the Gateway is considered. On the other hand, a stability criterion is employed by which a node maximizes the time that it is attached to the selected gateway in order to minimize the number of gateway hand-offs or switchings. The evaluation of the performance of the ad hoc network shows that the gateway switchings can be beneficial if shorter routes are employed.**

I. INTRODUCTION

Wireless Internet access receives significant attention nowadays. At certain locations as airports, hotels or conference, people with mobile devices are usually connected to external network through Access Routers (AR). As the coverage area of these devices is restricted, several ARs may be deployed in the area where the connection is to be guaranteed. An alternative solution is based on the utilization of Mobile Ad hoc NETworks (MANET) that can easily extend the coverage area of the Access Routers by employing multi-hop transmission.

Stand-Alone Mobile Ad Hoc Networks are formed by the aggregation of wireless devices that communicate among themselves without any centralized infrastructure. In order to ensure the communication between distant terminals, the nodes self-configure the routing tables following a distributed strategy or ad hoc routing protocol. These specific routing protocols must enable the construction of multi-hop routes as well as the detection of the breaks that occur in the existing paths due to the movement of the nodes that compose them.

When MANETs are integrated into external networks as the Internet, the utilization of a Gateway is required. These extended mobile ad hoc networks or Hybrid MANETs should be provided with an extra mechanism in order to employ the Gateway properly. Several mechanisms have been already proposed. They mainly differ in the characteristics of the introduced Gateway (dedicated/not dedicated, mobile/fixed) as well as in the mechanism for Gateway Discovery, that is, the procedure by which a gateway announces the prefix information that they utilize. This information should be employed for the IPv6 address auto-configuration procedures in the ad hoc nodes following the stateless strategy [1]. When a node generates its own IPv6 addresses, the Duplicate Address Detection (DAD) may also be performed in order to verify the uniqueness of the self-constructed address. The conventional DAD in MANETs is based on a try-and-wait mechanism that implies a disruption of the on-going communications for a time period of typically 1 second.

In some scenarios, mobile nodes may access several Gateways. Under these circumstances, the device should decide the gateway to employ when it is going to establish communications with external hosts. Several parameters could be considered to take this decision as the number of hops in the route to the Gateway, the traffic load, the delay, the gateways's processing capabilities, etc [2]. In this paper, two metrics will be analyzed and evaluated. Firstly, as the most popular criterion for isolated MANETs, the minimum number of hops will be studied. Although this strategy seems to be adequate for stand-alone ad hoc networks, this criterion can lead to a significant number of gateway switchings that may deteriorate the network performance as each gateway switching requires the utilization of DAD procedures. In order to reduce the expected deterioration associated to DAD procedures, another criterion could be applied. In the Maximum Gateway Usage mode, a node maximizes the time period of utilizing the selected Gateway and, therefore, it keeps its current global address.

The paper is structured as follows. Section II introduces the technologies that are involved in the integration of ad hoc nodes into external networks. Section III presents the proposed mechanisms for the integration of MANET into external networks. The considered criteria for Gateway Selection are explained in Section IV while, in Section V, the results of the performed simulations are presented. Finally, in Section VI the paper is concluded.

II. TECHNOLOGIES FOR HYBRID MANETS

Integration of MANETs into external networks requires an extensive study of several aforementioned technologies. First, any mobile node requires a global IPv6 address in order to be reachable from external networks. To ensure the Internet hierarchical scheme, an entity must be in charge of providing the necessary information to enable mobile nodes to get or configure an appropriate IPv6 address. This functionality could be associated to a dedicated entity, as in a Dynamic Host Configuration Protocol (DHCP) server, which supplies the IPv6 global address to all the terminals within a

This work has been partially supported by TEC2006-12211-C02-01

specific domain [3]. Although this strategy has been proposed in several mechanisms, it presents a major drawback: the additional equipment (a centralized entity) restricts the applicability of MANET structure [4] [5] [6] [7].

A solution to suppress this equipment is based on the stateless address auto-configuration. Under this scheme, the Access Router periodically sends Router Advertisements (RA messages) containing all the prefixes that it can process [2]. The terminals requiring a global IPv6 address concatenate a random value, for example the EUI-64 MAC identifier, to the prefix to be utilized [8]. However, the self-generated IPv6 address is not guaranteed to be unique due to several reasons. Firstly, devices with duplicate MAC address exist on the market because of non-registered or erroneously manufactured interfaces. On the other hand, users may intentionally alter the configured IPv6 or MAC address. In addition, the use of globally unique IDs as part of the IPv6 address is not generally accepted as this utilization facilitates the users tracking, which may imply negative consequences on their privacy [9].

Therefore, providing that system intrusions are 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 several MANETs sharing the same prefix are expected to be merged. This strategy is called the in-service or strong DAD since all nodes using the given IPv6 address must execute the said mechanism. In our opinion, in-service DAD could be suppressed by some other strategies as Passive DAD [10] so we will only consider pre-service DAD in our studies.

One of the most extended techniques for DAD was proposed in [11]. 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 same 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 its simplicity, the main drawback of this procedure is related to the fact that nodes may interrupt external communications during the T_{DAD} interval. In the scenarios with multiple Internet Gateways where mobile nodes are connected to different points of attachment, the aforementioned time period of typically 1 second, causes noticeable latencies and may even provoke the break of the on-going connections. This particular drawback resulted in proposal of other, more reactive techniques, i.e., nodes do not check the uniqueness of the chosen address but must test the packets in order to detect potential address conflict [10]. Apart from the aforementioned problems associated with the conflict discovery, the reactive strategy causes unnecessary computation in the remote node, resulting in extensive power consumption.

Finally, the reception of RA messages also allows mobile nodes to know the domain where they reside. When a terminal detects changes in the RA messages it assumes it was moved to another domain. Consequently, it initiates the corresponding procedures to continue the on-going sessions. In the IPv6 context, the Mobile IPv6 technology specifies the procedures to communicate meanwhile changes in the point of attachment take place [12].

III. GLOBAL CONNECTIVITY

The RA messages play a vital part on the MANETs, as indicated in the previous sections. However, as they were originally defined for infrastructured wireless networks, the RA messages are restricted to a single hop and they can not be forwarded. This is a clear limitation for those mobile devices that are out of the range of the AR. Therefore, an Internet Gateway should be incorporated into the MANET. Two main functionalities are associated to this Gateway. Firstly, they will construct MRA (Modified Router Advertisement) messages that are similar to RA messages received from the AR but with the difference that they can be broadcasted in a multi-hop MANET. Secondly, this element will provide the ad hoc routing capabilities that are not present in the AR. Thus, the Internet packets destined to a MANET node are forwarded from the AR to the Gateway and only this Gateway will eventually initiate the ad hoc routing procedures.

The main characteristics of the Internet Gateway 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 emission of MRA messages could be accomplished in a way similar 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 referred to as the Global Connectivity support [13]. 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 exert a significant load on the network. In order to reduce this effect, there is another proposal where mobile nodes only re-broadcast the MRAs associated to their selected gateway. In such a way, mobile nodes form a continuous path to the Gateway that is comprised of devices sharing the same prefix. This could be considered as a simplification of the prefix continuity mechanism proposed in [14].

Both previous schemes share a clear drawback since they do not analyze the effects that the address auto-configuration mechanism when switching between two different gateways occurs, i.e. a node changes the selected Gateway to connect to the Internet. One of the supports that does take into consideration these consequences is presented in [15]. This mechanism is specifically intended for scenarios where multiple fixed gateways provide access to the Internet. The

idea proposed in [15] is based on the fact that the nodes receiving MRAs from different Gateways generate the corresponding IPv6 addresses even if they are not going to employ them immediately. Since the nodes use their IPv6 addresses appropriate to more than one gateway in the MANET, they can dynamically change the global address that they utilize for their external data exchange if, for example, one gateway ceases to be operational or moves out of the sight.

IV. CRITERIA FOR GATEWAY SELECTION

In scenarios where multiple gateways coexist, mobile nodes should apply certain criteria in order to select the gateway to communicate through with external hosts. Several factors, namely the load traffic, the gateway´s capabilities, the delay of the processed communications, etc. could be considered when taking this decision. In this study, two main metrics are considered:

- Minimum Hop Count Criterion. A Gateway is selected for connection if the number of hops between the MANET node and the said Gateway is minimun.
- Maximum Gateway Utilization Criterion. When applied, a node utilizes the selected Gateway until it becomes unreachable for the ad hoc node because of the network mobility. This fact is detected by the node when it stops receiving the corresponding MRA.

V. SIMULATIONS AND RESULTS

Due to the problems related to hardware tests of the aforementioned Gateway selection scenarios, their application was analyzed using simulations performed with the Network Simulator tool, ns-2.29 on Linux [16].

As the mechanism for the integration of ad hoc networks, the Global Connectivity support is employed. Anyway, similar results are obtained when the Prefix Continuity mechanism is utilized. Table 1 summarizes the parameters used in the simulations.

TABLE I. Simulation Parameters

Simulation Area	2500 m x 500 m
Mobile Nodes	50
Gateways	2 fixed Gateways at (100m, 250m) and (2400m, 250m)
Mobility Pattern (Random WayPoint)	Maximum Speed: [1, 10] m/s. Minimum Speed: 1 m/s Pause: 0 second
Traffic Pattern	10 Constant Bit Rate sources (From a mobile node to a fixed node) Rate: 4 packet/s Packet Size: 512 B
Simulation Time	2500 s (per run)
Transmission Range	250 m
Runs per point	3
Ad hoc Protocol	AODV
Internal Queue	64 packets
MRA Interval	10 seconds
DAD Interval (T_{DAD})	1 second

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

- Packet Loss Rate. 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 considered 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 that 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.

The obtained data are represented in Figures 1 to 3. To facilitate the understanding and to show the general tendencies of the evaluated criteria, the results of the different simulations have been also summarized through a linear regression, resulting in the straight lines of the figures.

These figures show that the criterion based on the Minimum Number of Hops is more appropriate than the criterion of the Maximum Gateway Utilization. Although the number of Gateway Switchings decreases when the Maximum Gateway Utilization is employed, the utilization of longer routes may cause an increment of the interferences in the network as more retransmissions take place. These interferences may provoke potential looses and delays. Furthermore, the employ of longer routes may not either be convenient as the expected Route Duration is lower than the shortest path [17]. Even if the gateway in use is still reachable for that node, the route that should be employed in order to forward the packet to the Internet will break more often than the path employed by the criterion of Minimum Number of Hops. In the analyzed scenarios, this effect seems to be more inefficient than the execution of more DAD processes.

VI.CONCLUSIONS

In this paper, the impact of the gateway selection criteria has been analyzed in order to be applied when MANETs are integrated into external networks and DAD procedures are performed. Specifically, two criteria have been studied: the minimum number of hops and the maximum gateway usage.

The results show that the utilization of shorter routes is recommended even if the number of gateway switchings increases.

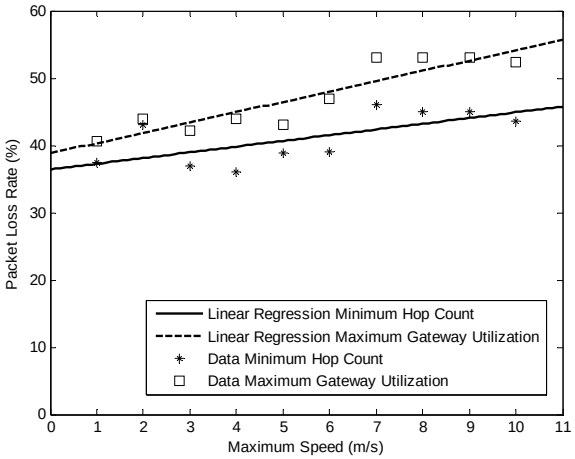

Figure 1. Packet Loss Rate versus Maximum Speed.

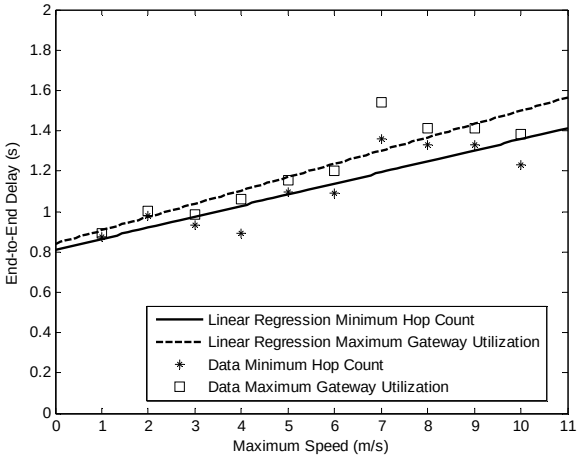

Figure 2. End-to-End Delay versus Maximum Speed.

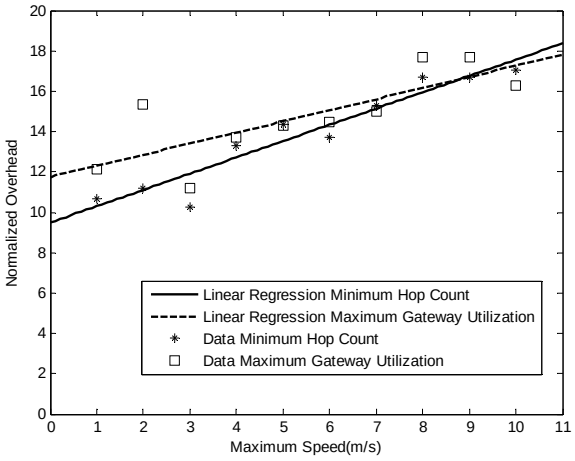

Figure 3. Normalized Overhead versus Maximum Speed.

REFERENCES

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

[2] S. Singh, J.Kim, C. Perkins, T. Clausen, P. Ruiz, "Address autoconfiguration for MANETs: definition and problem statement", IETF Internet Draft, work in progress, March 2006.

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

[4] A. McAuley, K. Manousakis, "Self-Configuring Networks" , in Proceedings of *21st Century Military Communications Conference Proceedings* , 2000.

[5] M. Mohsin, R. Prakash, "IP Address Assignment in a Mobile Ad Hoc Network", in Proceedings of *MILCOM 2002* ,2002.

[6] A. Tayal, L. Patnaik, "An address assignment for the automatic configuration of mobile ad hoc networks", in Proceedings of *Personal Ubiquitous Computing* , 2004.

[7] T. Clausen, E. Baccelli, "Simple MANET Address Autoconfiguration" IETF Internet Draft, work in progress, February 2005.

[8] C. Huitema, "IPv6: the new Internet Protocol", Prentice-Hall, ISBN:0-13-850505-5 , 1998.

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

[10] H. Jeong, D. Kim, J. Park, H. Kim, C. Toh, "Passive Duplicate Address Detection for On-demand Routing Protocols", IETF Draft, work in progress, October 2006.

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

[12] D. Johnson, C. Perkins, J. Arkko,"Mobility Support in IPv6", IETF RFC 3775, June 2004.

[13] 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, March 2006.

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

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

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

[17] A. Triviño-Cabrera, J. García-de-la-Nava, E. Casilari, F.J. González Cañete, "An Analytical Model to Estimate Path Duration in MANETs", in Proc. Of the 9-th ACM/IEEE International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems, October 2006.