Ad Hoc Networking in the Internet: A Deeper Problem Than It Seems

Emmanuel Baccelli, Thomas Heide Clausen, Philippe Jacquet

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Ad Hoc Networking in the Internet: A Deeper Problem Than It Seems

Emmanuel Baccelli — Thomas Clausen — Philippe Jacquet

N° 6725

Novembre 2008

Thème COM

ISSN 0249-6399 ISRN INRIA/RR--6725--FR+ENG

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA

centre de recherche
SACLAY - ÎLE-DE-FRANCE

Ad Hoc Networking in the Internet: A Deeper Problem Than It Seems

Emmanuel Baccelli *, Thomas Clausen†, Philippe Jacquet *

Thème COM — Systèmes communicants
Équipes-Projets Hipercom

Rapport de recherche n° 6725 — Novembre 2008 — 15 pages

Abstract: Self-organized networks, also known as ad hoc networks or MANETs, are expected to soon become important components in the Internet architecture. Numerous efforts currently focus on the accomplishment of scalable and efficient mobile ad hoc routing, an essential piece in order to fully integrate ad hoc networks in the Internet. However, an orthogonal and yet as important issue lies with ad hoc IP autoconfiguration. Indeed, prior to participation in IP communication and routing, a node must acquire IP addresse(s) to configure its interface(s). These IP addresses may be required to be unique within a certain scope and/or topologically "correct". Since nodes may be mobile and neither the set of nodes in the MANET nor their connections to each other is pre-determined, the proper configuration must be detected and acquired automatically. This paper reviews the applicability, in the particular context of MANETs, of standard automatic address configuration and prefix allocation protocols, and identifies the different categories of issues that are not solved by these protocols. The paper then elaborates further on why these issues are more profound than they seem, as they pertain to graph theory and are in fact real scalability and architectural issues for the Internet of tomorrow.

Key-words: Ad hoc, Scalability, IP, Architecture, Autoconfiguration, Routing, Network, Wireless, Standardization, IETF

* INRIA
† Ecole Polytechnique

Centre de recherche INRIA Saclay – Île-de-France
Parc Orsay Université
4, rue Jacques Monod, 91893 ORSAY Cedex
Téléphone : +33 1 72 92 59 00

Ad Hoc Networking in the Internet: A Deeper Problem Than It Seems

Résumé : Ce rapport de recherche traite le sujet de l'intégration des réseaux ad hoc dans l'architecture Internet actuelle. Par le biais de l'étude du problème de l'autoconfiguration IP dans ces rseaux sans-fils et mobile, le rapport identifie des problèmes fondamentaux ayant traits à la théorie des graphes et au passage à l'échelle de nouveaux modèles architecturaux.

Mots-clés : Ad hoc, Passage à l'échelle, Architecture, Autoconfiguration, Routage, IP, Réseau, Sans-fils, Normalisation, IETF

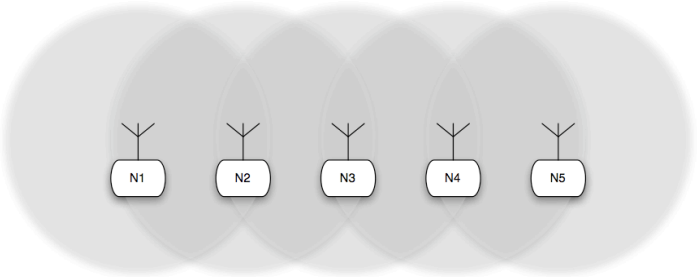

Figure 1: MANET communication. The light grey area indicates the radio coverage area of each MANET interface.

1 Introduction

A MANET consists of a loosely connected set of MANET routers. Each MANET router features one or more wireless interfaces called MANET interfaces, through which it communicates over IP with other MANET routers within radio range, as shown in Fig. 1. Beyond this "single hop" wireless communication, a MANET router can also achieve "multihop" wireless communication with destinations outside its radio range, through intermediate MANET routers relaying IP packets over their MANET interface(s), towards the destination.

In practice, different types of MANET scenarii are expected. In the so-called *subordinate MANET scenario* depicted in Fig. 2, the MANET is connected to at least one external network N (typically the Internet) that imposes a specific addressing hierarchy on the MANET, i.e. the use of addresses or prefixes derived from a global prefix. Typical instances of this scenario include public wireless networks of scattered fixed WLAN Access Points participating in a MANET of mobile users, and acting as border routers. Another example is coverage extension of a fixed wide-area wireless network, where one or more mobile routers in the MANET are connected to the Internet through technologies such as UMTS or WiMAX. In the so-called *standalone MANETs scenario* on the other hand (see Fig. 2), the MANET does not contain any router able to provide other routers requesting configuration with addresses or prefixes derived from a global prefix. Typical instances of this scenario include private or temporary networks, set-up in areas where neither wireless coverage nor network infrastructure exist (e.g. emergency networks for disaster recovery, or conference-room networks). In every envisionned scenrio, MANET interfaces exhibit very specific properties [2], including (i) communicating over a semi-broadcast medium, which means potential assymetric reachability, and (ii) fuzzy neighbor relationships between MANET routers. Moreover, MANET routers may be mobile and may thus join and leave the MANET at any time, at a rate that can be substantially higher than in usual networks.

Prior to participation in IP communication, each MANET router that does not benefit from appropriate static configuration needs to acquire IP addresses for each of its MANET interface(s), and may also need to automatically acquire authority over one or more IP prefixes to configure attached nodes (i.e. hosts

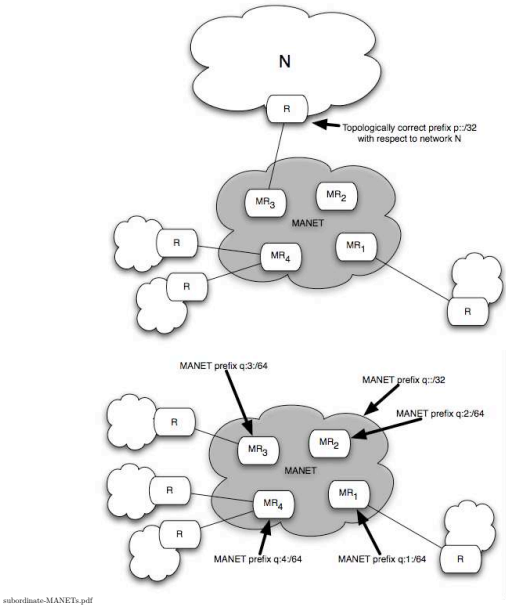

Figure 2: On top, a subordinate MANET, which is imposed an addressing hierarchy by a superordinate router. Below, an standalone MANET, root of the addressing hierarchy.

or routers), if any. In most cases it is required that the router is the only entity within a certain scope currently using this address, or managing this prefix.

Since nodes may be mobile and neither the set of nodes in the MANET nor their connections to each other is pre-determined, the proper configuration must be detected and acquired automatically. This paper reviews the applicability, in the particular context of MANETs, of generic automatic IP address configuration and IP prefix allocation protocols, focusing on protocols compliant with IPv6. The paper also identifies the different categories of issues that are not solved by these existing mechanisms, and then elaborates on why these issues are more profound than they seem.

2 Review of Standard Protocols' Applicability

The primary goals of ad hoc IP autoconfiguration are to provide autoconfiguration mechanisms which allow each MANET router to:

1. configure IP addresses that are unique within the MANET, on their MANET interface(s),
2. be allocated IP prefixes that are disjoint from prefixes allocated to other routers within the MANET,

3. maintain, within the MANET, the uniqueness of configured addresses and the disjoint character of allocated prefixes, even in cases where whole networks merge into a single network (i.e. network merging),
4. be allocated topologically correct prefixes, in the subordinate MANET scenario.

This section reviews the applicability of existing standard protocols for the purposes listed above, assuming that MANET routers also run these standard protocols as usual over non-MANET interfaces, if any are present in the network.

2.1 Applicability of DHCP

The Dynamic Host Configuration Protocol (DHCP [3]) enables automatic allocation of an IP address to a node by a DHCP server. A node requiring an IP address contacts a DHCP server and requests an address. The DHCP server will dynamically assign an address from a certain pool of addresses, and allocate a so called "lease" of that address to the client. The client can then use the address for a certain time. If the client wants to keep the address for a longer time, it has to prolong the lease. If the DHCP server is not on the same link as the DHCP client, it is possible to use one or more DHCP relay agent to forward the messages to a different subnet.

Issues with DHCP Fundamental Assumptions. DHCP works on the basic assumption that every node in the MANET can directly communicate with either (i) the DHCP server, or (ii) a DHCP relay which can communicate with either the DHCP server or another relay.

Part (i) of this assumption is often wrong in a MANET, as each node may see a different set of neighboring MANET nodes. On the other hand, part (ii) of this assumption relies on the guarantee that the recursion will end at some point (by reaching the root, i.e. the DHCP server). Because of the dynamics in MANET topology and MANET membership, there is no such assurance in a MANET, as the DHCP server may be unreachable, or a loop may have appeared along the path.

Moreover, DHCP works with the assumption that either (a) there is a unique DHCP server in the network, or (b) if there are several DHCP servers in the network, they are manually configured accordingly. Because of the dynamics in MANET membership, there is no such assurance in a MANET, as topology changes may produce a situation where several servers with conflicting configuration parameters (e.g. managing non-disjoint pools of local addresses) become part of the same MANET. Servers may thus require dynamic (re)configuration.

Similarly, DHCP works with the assumption that should there be DHCP relays, they benefit from appropriate manual configuration. Because of the dynamics in MANET membership and topology, there is no such assurance in a MANET. Configuration may not remain appropriate over time, and relays may thus require dynamic (re)configuration.

What DHCP Can and Cannot Do in MANETs. DHCP "as is" could be used to some extent for address configuration purposes (goal 1, listed above). However DHCP's applicability in this context is limited. Indeed, if the topology is or becomes such that a MANET router does not have access to a DHCP server directly nor through a relay, DHCP is not operational.

DHCP "as is" could also be used to some extent for uniqueness maintenance purposes (goal 3, listed above). However DHCP's applicability in this context is limited. Since different DHCP servers will not automatically check the disjoint character of the pools of addresses they provide leases from, if the topology is or becomes such that several DHCP servers with conflicting configuration lease addresses in the same MANET, there is no guarantee that configured addresses will indeed be unique.

2.2 Applicability of SLAAC/NDP

Stateless Address Autoconfiguration (SLAAC [5]) enables automatic configuration of an IP address to a host without contacting any kind of server. A host first constructs a tentative IPv6 address by attaching its host identifier (in most cases its MAC address) to the well-known link-local prefix. It then operates duplicate address detection, that verifies that no other host on the link has the same address by broadcasting NDP messages [4]. If the address is not unique, the autoconfiguration process will abort. Upon a successful address uniqueness test, a host may request a prefix from any router on the link by an exchange of NDP messages. It will again attach its host identifier to that router prefix and repeats the address uniqueness test sequence.

Issues with SLAAC/NDP Fundamental Assumptions. SLAAC relies on NDP signalling, which works on the basic assumption that each node in the MANET can communicate directly with every other node in the MANET, i.e. all the nodes are connected to a single multicast-enabled link. This assumption is often wrong in a MANET, as each node may see a different set of neighboring MANET nodes.

What SLAAC/NDP Can and Cannot Do in MANETs. SLAAC "as is" could be used to some extent for address configuration and uniqueness maintenance purposes (goal 1 and 3, listed above), for instance when no DHCP server is available. However SLAAC's applicability in this context is limited, since NDP messages are not relayed beyond the "link" (or in MANET terms, beyond the first hop). If topology is or becomes such that the MANET is not contained in a single hop, there is no guarantee that the configured addresses will indeed be unique, since signalling will not reach all the concerned nodes.

2.3 Applicability of DHCP-PD

DCHP-PD [6] is a DHCP option that enables automatic allocation of IPv6 prefixes to routers using DHCP. A router may request a prefix allocation from a DHCP server by sending a DHCP request including the Prefix Delegation option. The server may then delegate a sub-prefix (i.e. a subset of its address

pool) to the router. The DHCP message containing the Prefix Delegation option may be relayed through one or more DHCP relays [3]. This protocol is the only standard solution available for prefix delegation.

Issues with DHCP-PD Fundamental Assumptions. DHCP-PD is based on DHCP, and thus encounters the fundamental issues described in Section 2.1, with respect to server reachability, and dynamic (re)configuration of servers and relays.

What DHCP-PD Can and Cannot Do in MANETs. DHCP-PD "as is" could be used to some extent for prefix allocation purposes (goals 2 and 4 listed above) and for uniqueness maintenance purposes (goal 3, listed above). However DHCP-PD's applicability in this context is limited. If topology is or becomes such that the MANET router cannot communicate with a DHCP server, DHCP-PD is not operational. Moreover, if topology is or becomes such that several servers with conflicting configuration become part of the same MANET, there are no automatic (re)configuration mechanisms available in order for servers to dynamically adapt to the situation.

3 Problem Analysis At First Sight

At first sight, it is rather obvious that the distributed and dynamic nature of MANETs brings the need for address generation algorithms that can complement existing solutions by supporting operation without fixed hierarchies to provide routers with appropriate addresses and prefixes. In addition, the multi-hop aspect of MANETs brings specific needs as far as address and prefix uniqueness is concerned, as detailed below.

If prefix or address uniqueness is required within a specific scope (which is the case most of the time), and if the address/prefix generation mechanism in use does not ensure address/prefix uniqueness, then additional issues arise.

Pre-service issues relate to the fact that before a generated address or prefix is assigned and used, it should be verified that it will not create an address conflict within the specified scope. This is essential in the context of routing, where it is desireable to reduce the risks of loops due to routing table pollution with duplicate addresses.

In-service issues, on the other hand, relate to problems that come from the fact that even if an assigned address or prefix is currently unique within the specified scope, it cannot be ensured that it will indeed remain unique over time.

Phenomena such as MANET merging and MANET partitioning may bring the need for checking the uniqueness (within the specified scope) of addresses or prefixes that are already assigned and used. This need may depend on (i) the probability of address conflicts, (ii) the amount of the overhead for checking uniqueness of addresses, and (iii) address/prefix uniqueness requirements from higher layers applications or protocols.

For instance, if (i) is extremely low and (ii) significant, then checking pre-service

uniqueness of addresses and prefixes may not be used. If on the other hand (i) is not extremely low, then checking pre-service and in-service uniqueness of addresses or prefixes may be required. In any case, if some applications/protocols have a hard requirement for address uniqueness assurance, in-service uniqueness checks of addresses and prefixes should always be used, no matter how unlikely is the event of address conflict.

An orthogonal category of problems concerns the potential availability of multiple address configuration servers (i.e. multi-homing), which brings the need to decide between either (a) using one prefix for the whole MANET, or (b) using several prefixes for the MANET. This paper does not focus on this particular problem. It is however worthy to mention potential consequences, which include prefix deaggregation, sub-optimal routing and/or substantial control overhead.

4 A Deeper Analysis: Taking A Step Back

Quite some efforts have recently been deployed in the research community and at the IETF in order to address the issues that pertain to IP autoconfiguration in MANETs. However, no consensus has been reached so far on how to even grasp the problem(s), despite extended work and discussions on the subject. Ironically, many solutions have recently been developed [9], while the problem itself is officially not fully understood. This section aims at taking a step back and analysing why.

4.1 Links on a MANET

A key notion that has yet to be introduced in this paper is the concept of a *link*. MANET protocols must indeed operate at layer 3 over opportunistic links formed over wireless broadcast network interfaces (MANET interfaces). However, MANET links exhibit very different properties compared to usual, well known link types such as an Ethernet link, or a point-to-point link. The definition of a MANET link type has thus also been the subject of some discussions in the field of IP autoconfiguration in MANETs.

The present Internet architecture uses the concept of link as a brick of which every network "construction" is made. A collection of axioms related to this concept are indeed assumed by most protocols at layer 3 and higher, as well as by current IP addressing schemes. For instance, one of these axioms is, that a link must be a well defined and bounded layer 2 / physical segment. Another axiom is that a given interface must connect a node to one, and only one link. Moreover, interfaces connected to a link must be able to communicate directly at layer 3 without IP datagrams forwarding and TTL/hop-limit decrement. These axioms make it possible to have a clear distinction between which nodes are *off-link*, and which nodes are *on-link*, allowing a straight equivalence between a given link and a given IP prefix. Moreover, these axioms make it possible to model the Internet topology as a tree-like graph connecting such links, and thus permit IP prefix aggregation.

The archetype, to which every link is more or less supposed to resemble, is

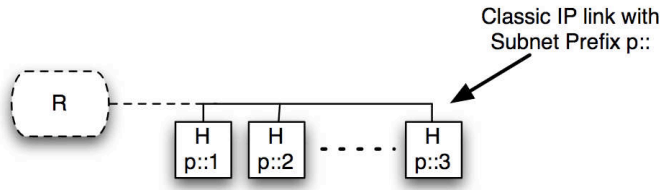

Figure 3: An ethernet link: a cable connecting a router (marked R) and hosts (marked H). The IP prefix p:: is assigned to the link.

the ethernet link: basically a cable connecting several nodes together (see Fig. 3). The most simple example of link is a point-to-point link, which is basically a special case of ethernet link, with a cable connecting exactly two nodes. Another common example of link is a Wifi 802.11 link (generally used in infrastructure mode) which is also conceptualized similarly to an ethernet link. This is done by simply replacing the "scope of the cable" by the radio scope, i.e. nodes inside the radio range of the Wifi Access Point are on-link, while other nodes are off-link.

However, the properties of a link on a MANET hardly resemble those of an ethernet link. Indeed, decentralized connections between nodes on a MANET appear and disappear opportunistically over the air, and this air is difficult to segment, as it is not clearly bounded (as seen for example in Fig. 1). Distinction between nodes that are on-link and nodes that are off-link is not straightforward, and there is thus no standard relationship between between an IP prefix and such a link. This fundamental lack raises issues with respect to current IP addressing and prefix aggregation schemes, as well as backward compatibility concerns with respect to many protocols and applications already deployed at layer 3 and higher.

4.2 MANET Topologies

The difference between such MANET topologies and topologies supported so far in the Internet can also be seen from a graph theory point of view. Indeed, the current Internet architecture is designed to work on networks modeled as mostly static graphs (if needed via the introduction of virtual vertices and/or virtual links). MANET topologies, however, are better described as mostly dynamic *hyper-graphs* as shown in Fig. 4, where an edge may connect more than two vertices - contrary to a graph, where an edge always connects exactly two vertices.

Hyper-graphs are in general more suitable than graphs to model MANET topologies since interferences between wireless neighbors can be described with edges connecting more than 2 vertices, while on the other hand they cannot be realistically depicted with edges in a graph, just connecting vertices two by two. Moreover, the mobile and wireless nature of most nodes in a MANET brings the need for a more dynamic model, that can successfully track topologies that potentially change much more frequently.

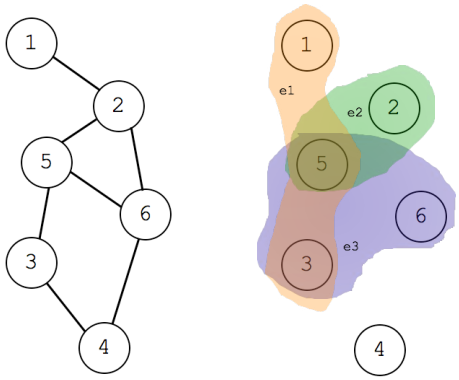

Figure 4: On the left, a graph: each edge connects exactly two vertices. On the right a hyper-graph with three edges e1, e2 and e3: an edge may connect more than two vertices.

However, many fundamental IP protocols, designed to work on graphs, and currently deployed in the Internet, do not work "as-is" on hypergraphs, and even less with dynamic topology in addition.

4.3 Hyper-Graph Modeling

With this point of view, the challenge is the integration of topologies derived from hypergraphs in the Internet architecture. Some quick fixes have been discussed including allowing multiple links per IP prefix, in order to solve problems due to multi-hoping and TTL decrements. However, even with simple topologies such as the one shown in Fig. 1, it is impossible to identify a segmentation of the air that would provide distinct links. For instance, a transmission between N1 and N2 cannot even be considered as being on a usual point-to-point link between N1 and N2 since this transmission will interfere with a concurrent transmission between N2 and N3. Moreover, allowing multiple links per prefix would not be backward compatible with many protocols deployed at layer 3 and higher [7]. Another quick fix was thus to push the issue down to layer 2 where routing would be performed, in order to hide hyper-graphs and other MANET properties from layers 3 and higher. However, pushing down the issue to layer 2 is more likely to break the layer model than to actually solve anything profoundly: routing is not supposed to happen below layer 3, even though it is recently proposed by approaches such as [16]. In fact, the problem at layer 2 essentially remains the same: how to automatically partition the air into distinct segments, and such with a topology that may, in addition, change very frequently?

A more radical approach may be to avoid using the link concept. However, the resulting complexity explosion, due to partial or total IP prefix deaggregation, is to be addressed. Suppression of the link concept deprives the Internet from its only means to identify distinct subsets of nodes that can be dealt with as a batch, thus enabling the scalability of protocols that discover and maintain the network. However, in MANETs, where any node may move and neither the set

of nodes in the MANET nor their connections to each other is pre-determined, a situation occurs: finding a practical and scalable algorithm for the establishment of such dynamic partitioning, that could be generically used to change the "granularity" of the network, is still an open problem.

4.4 Towards Supporting MANET Topologies in The Internet

At this point, it is clearer that the real issues tackle scalability, in terms of topology dynamism and size. Solutions are needed to co-organize at large scale, the current Internet on one hand, and on the other hand a growing part of its topology becoming increasingly dynamic (soon including ad hoc networks). In any case, for obvious reasons, it is not realistic to advocate a change that would require any alteration of any protocol already massively deployed in the Internet. Any solution to the problem of fully integrating MANETs in the Internet must thus take into account legacy infrastructure and protocols.

A first step to address this problem was recently proposed [2], providing a generic way to interface between the current Internet infrastructure and MANET opportunistic networks. A common mistake in this area is to consider that a MANET should simply emulate an Ethernet at layer 3, and that nodes in a MANET are just hosts. This leads to MANET nodes being perceived and configured as hosts in an Ethernet: a MANET interface would be assigned an IP address and a subnet prefix p:: (a prefix which is shared among all the nodes in the MANET). As such, nodes in a MANET would be on the same IP link.

However, for interfaces within the MANET (and with the same prefix) to communicate, layer 3 forwarding of IP datagrams may occur, and with such forwarding, TTL/hop-limit is decremented. Moreover, link-local multicast or broadcasts either do not reach all nodes within the subnet or if they are to reach all nodes within the subnet, they are to be forwarded by intermediate nodes. These characteristics break the classic IP link model and the applications which assume the characteristics of this model [7]. Thus, considering MANET nodes as mere hosts and configuring them as if the MANET forms a single subnet is not appropriate.

4.5 Generic IP Architecture Model Integrating MANETs

The key is in fact to isolate MANET specificities from an architectural point of view. As MANET nodes may both generate and forward traffic, they should rather be distinguished as multiple virtual entities: (i) a virtual MANET router, with at least one MANET interface, (ii) a virtual host, connected to the MANET router with a virtual classical interface, as shown in Fig. 5 (a MANET router may also have other hosts attached). Hosts, and their applications, are not exposed to the specific characteristics of MANET interfaces and are connected to the MANET via a router, similarly to how hosts on an Ethernet, are not exposed to the intricacies of what type of connectivity the router has beyond the Ethernet. Hosts on non-MANET interfaces thus assume a classic IP link model, and applications as well as protocols on these hosts can run unmodified (since they are only exposed to classic IP interfaces connected to a classic IP

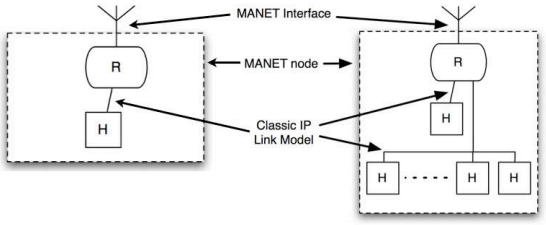

Figure 5: On the left, a simple MANET node: both a host and a router. On the right a more complex MANET node, with attached hosts. In both cases, usual protocols operate on interfaces other than MANET interfaces and on nodes other than MANET routers.

link).

MANET specific behaviors - such as hyper-graph topology, dynamics etc. - are exposed exclusively to MANET interface(s), as shown in Fig. 6. MANET interfaces are "seen" only by routers, assumed to be MANET aware and running appropriate protocols and applications, which may include modifications to classic protocols from the IP suite and/or additionnal protocols such as MANET routing or autoconfiguration protocols.

MANET interfaces forming a multi-hop MANET area may use a site (but not subnet) prefix, for aggregation purposes. However, each MANET interface on a MANET must be configured with a prefix disjoint from any prefix on any other MANET interfaces in the MANET, i.e. respective address ranges should not overlap (the simplest examples are /128 prefixes with IPv6, or /32 prefixes with IPv4). This ensures compatibility with the existing IP architecture, and at the same time enables MANET nodes to be identified while ensuring that a MANET is not wrongly viewed as a single subnet. Moreover, if the MANET router is delegated a prefix p:: (for instance with DHCP-PD [6]), MANET interface(s) of the router are not configured with this prefix. Nevertheless, this prefix can be assigned to classic IP links (a link in the grey area in Fig. 6). This enables hosts to be assigned addresses from within this prefix using existing standard solutions such as DHCP, SLAAC etc.

Note that this model also covers so-called MANEMO scenarii, where a whole network (host(s) and router) is mobile in a ad hoc fashion. This type of scenario is also known as the nested NEMO scenario [10], which has recently received growing attention in the community. Such a scenario could indeed be well depicted by Fig. 5, where for instance, the central router R would be the access router of the nested NEMO.

5 Conclusion

In this paper, we have identified new ad hoc networking scalability challenges, through the analysis of problems concerning automatic IP configuration in MANETs. We have analyzed why ad hoc IP autoconfiguration cannot be solved

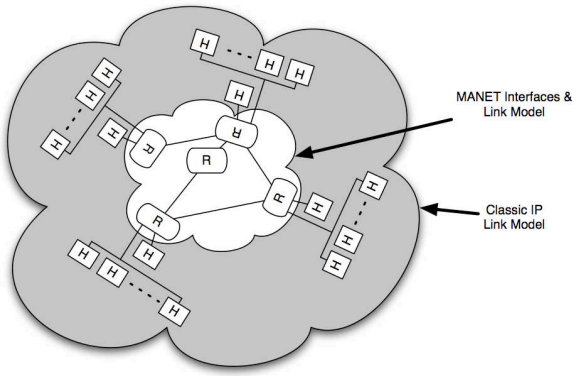

Figure 6: Proposed architecture: MANET specificities are isolated, and concern only MANET interfaces and routers (center white cloud). Any other node or interface type runs usual protocols and complies with the current Internet architecture (in the grey part of the network).

by off-the-shelf protocols from the IPv6 suite. New types of issues are indeed left unaddressed by these protocols, which were not designed for opportunistic, wireless multi-hop networking. This paper then elaborated further on why these issues are more fundamental than they seem at first, as they tackle concepts that are at the base of the whole Internet architecture. These issues were identified as pertaining to graph-theory, and are essential scalability and architectural challenges for the Internet in the near future. In terms of standardisation (for instance in the IETF), a unified and scalable integration model for ad hoc networking in the current Internet architecture is greatly needed in order to coherently manage different parallel efforts concerning self-organized networking, including ROLL [11], MANET, [12], 6LOWPAN [15], AUTOCONF [13], or MEXT [14], among others.

References

[1] E. Baccelli et al. "Address Autoconfiguration for MANET: Terminology and Problem Statement," Internet Engineering Task Force (IETF) Internet Draft, draft-ietf-autoconf-statement-04 (work in progress), 2008.

[2] I. Chakeres, T. Clausen, J. Macker, "Mobile Ad hoc Network Architecture," Internet Engineering Task Force (IETF) Internet Draft, draft-ietf-autoconf-manetarch-07 (work in progress), 2008.

[3] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6," Internet Engineering Task Force (IETF) RFC 3315, July 2003.

[4] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IPv6," Internet Engineering Task Force (IETF) RFC 4861, September 2007.

[5] Narten, T., Thomson, S., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration," Internet Engineering Task Force (IETF) RFC 4862, September 2007.

[6] Troan, O. and R. Droms, "IPv6 Prefix Options for DHCPv6," Internet Engineering Task Force (IETF) RFC 3633, 2003.

[7] D. Thaler, "Multi-Link Subnet Issues," Internet Engineering Task Force (IETF) RFC 4903, 2003.

[8] E. Baccelli, T. Clausen, "A Simple Address Autoconfiguration Mechanism for OLSR," Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), Kobe, Japan, May 2005.

[9] C. Bernardos, M. Calderon, H. Moustafa, "Survey of IP address autoconfiguration mechanisms for MANETs," Internet Engineering Task Force (IETF) Internet Draft, draft-bernardos-manet-autoconf-survey-03 (work in progress), 2008.

[10] E. Baccelli, T. Clausen, R. Wakikawa, "Route Optimization in Nested Mobile Networks (NEMO) using OLSR," Proceedings of the IASTED International Conference on Networks and Communication Systems (NCS), Krabi, Thailand, 2005.

[11] Routing Over Low power and Lossy networks (ROLL), IETF Working Group, http://www.ietf.org/html.charters/roll-charter.html

[12] Mobile Ad-hoc Networks (MANET), IETF Working Group, http://www.ietf.org/html.charters/manet-charter.html

[13] Ad-Hoc Network Autoconfiguratio (AUTOCONF), IETF Working Group, http://www.ietf.org/html.charters/autoconf-charter.html

[14] Mobility EXTensions for IPv6 (MEXT), IETF Working Group, http://www.ietf.org/html.charters/mext-charter.html

[15] IPv6 over Low power WPAN (6LOWPAN), IETF Working Group, http://www.ietf.org/html.charters/6lowpan-charter.html

[16] IEEE P802.11 TASK GROUP S, http://grouper.ieee.org/groups/802/11/Reports/tgs_update.htm

Centre de recherche INRIA Saclay – Île-de-France
Parc Orsay Université - ZAC des Vignes
4, rue Jacques Monod - 91893 Orsay Cedex (France)

Centre de recherche INRIA Bordeaux – Sud Ouest : Domaine Universitaire - 351, cours de la Libération - 33405 Talence Cedex
Centre de recherche INRIA Grenoble – Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier
Centre de recherche INRIA Lille – Nord Europe : Parc Scientifique de la Haute Borne - 40, avenue Halley - 59650 Villeneuve d'Ascq
Centre de recherche INRIA Nancy – Grand Est : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex
Centre de recherche INRIA Paris – Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex
Centre de recherche INRIA Rennes – Bretagne Atlantique : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex
Centre de recherche INRIA Sophia Antipolis – Méditerranée : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399