ADDRESS CONFIGURATION SCHEMES IN MOBILE AD HOC NETWORKS

Julien Ridoux and Anne Fladenmuller

LIP6-UPMC
8, rue du Capitaine Scott
75015 Paris - FRANCE
{Julien.Ridoux, Anne.Fladenmuller}@lip6.fr

Abstract

This paper presents an overview of proposals concerning the auto-configuration of Mobile Ad Hoc Networks. We will shortly describe the solutions used in wired networks, the characteristics of Mobile Ad Hoc Networks and the basic problems raised by the auto-configuration in mobile environments. We will present the existing solutions to this problem. The adaptation of mechanisms such as MobileIP is one of the proposed solutions. Independently of this, alternative mechanisms based on geographical or Peer-To-Peer routing have been proposed. We provide highlights on the characteristics of these different approaches.

1 Introduction

Thanks to the improvement of radio communications, the connectivity between people increases. The concept of Mobile Ad hoc NETwork (MANET) has been proposed as a way to compose networks from mobile nodes without any fixed and dedicated infrastructure. The goal for these networks is to be able to be spread quickly and easily in situations where there is no possibility and no time to set up a fixed infrastructure. With this goal, the auto-configuration of these mobile networks is crucial.

Most papers about MANETs concern proposals or improvements of routing protocols to make them take into account the characteristics of wireless environments. Fewer try to propose solutions to addressing configuration issues. We are fully aware that routing and addressing are closely related. This is moreover true as in the Internet Protocol (IP), addresses are at the same time a unique identifier of the node and its relative localization in the network thanks to the hierarchical topology of the Internet. The addressing and routing IP functions are therefore strongly bound together. Because of these observations we sometimes refer to papers that focus more on routing than addressing issues. Nevertheless we want to show it doesn't necessarily have to be combined together.

The paper is organized as follows. Section 2 describes some background concepts to improve the understanding of auto-configuration mechanisms and mobility handling. Section 3 discusses the characteristics of MANETs and their configuration problems. Section 4 describes approaches different from the classical IP one to improve the scalability of Mobile Ad hoc Networks configuration.

2 Different Types of Mobility

Several approaches are possible to deal with different types of terminal mobility. The mobility of the user may correspond to a nomadic behavior, roaming or an ad hoc mobility. In the following sections we describe the mechanisms proposed to handle each one of these mobilities.

2.1 Configuration of Wired Networks

Background about wired network configuration is needed in order to clearly understand the paradigm of MANETs configuration. As we said one kind of mobility is due to the nomadic behavior of users *i.e.* users can connect to the Internet with the same computer from different IP domain. For instance a user may plug his/her computer on the network at the office or from a conference room when he/she is on the move. The mobile node is not reachable when it is moved, but it can be connected through a fixed network to the Internet without resetting the computer configuration. Configuration tools such as DHCP servers can provide addresses for nomadic users. Organizations owning a wide IP network use centralized configuration servers such as DHCP servers to configure automatically their network. This mechanism allows the dynamic configuration of transient users in the network.

A newer approach concerns distributed auto-configuration of wired networks. This approach is the one chosen by IPv6 stateless address auto-configuration mechanisms [28] or by the Zeroconf working group [23]. These approaches rely on the ability of network elements to realize a Duplicate Address Detection

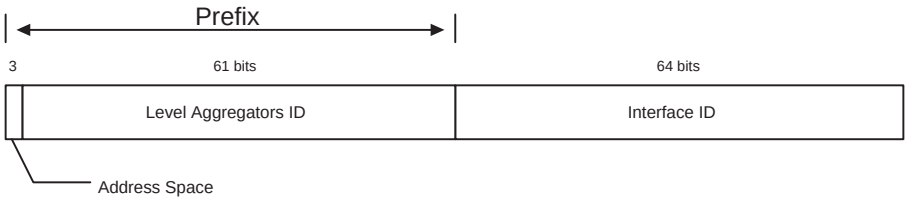


Figure 1: IPv6 Address

(DAD) and, depending on the version of the Internet Protocol in use, on the presence of a node providing Router Advertisements.

In the case of Zeroconf for IPv4, a new node N configures itself with a temporary address belonging to a special range. N chooses randomly another address in the reserved range 169.254/16 and broadcast a request containing this address. If none of the other nodes of the network answers the request within a defined time period, N considers it can use the proposed address. If the address is already in use, N receives an answer and repeats the process with another randomly chosen address. During the configuration process the temporary address used to send the request is supposed to be unique.

The IPv6 stateless address auto-configuration [28] is slightly different from the IPv4 mechanism because of the nature of IPv6 addresses. An IPv6 node owns several addresses per interface and at least a link local and a global address. Global addresses are routable in the whole Internet whereas routers do not forward link local addresses. The field Address Space (*cf.* figure 1) identifies the category the address belongs to (global, link local etc). IPv6 addresses are formed from a prefix and a suffix. The prefix can be received from a router on the link for global addresses or predefined for link local addresses. The suffix is based on the Medium Access Control (MAC) interface address.

When a new node N arrives in the network, it receives a prefix from its edge router. This mechanism called *Router Advertisement* allows a router to broadcast its address prefix periodically to all the nodes on its subnets. Upon receipt of a *Router Advertisement* N forms a global address and uses its link local address to realize a DAD on the global address.

Since the MAC address of an interface may not be unique ([12],[17]), nodes need to check if they can use the just formed address. The DAD is a process based on multicast communications which ensures that two nodes in the same network can't configure themselves with the same address. Roughly, a node N that is not configured uses a link local address to send a request to all of its neighbors on the Local Area Network (LAN). This request contains the proposed address that node N has built from the router's prefix and its MAC address. If one of the other nodes of the LAN is already configured with the proposed address, it will answer to N's request. If none of the nodes answer the request after a predefined timeout, N considers that the address is not in used and that it can use it.

2.2 Macro-mobility

In this section we present some background on MobileIP, the reference protocol to handle macro-mobility, since we will latter on explain different adaptations that have been made to match MANETs characteristics.

MobileIP (MIP) is a protocol that has been proposed in order to handle seamlessly the mobility of nodes running the IP protocol. This proposal has become a standard for IPv4 [4], and will probably become one for IPv6 in a short future [7]. This model of mobility has been described several times in many papers. We will describe it shortly in order to clarify its understanding for the rest of the paper.

The figure 2 illustrates the common situation of MobileIP. A mobile node belongs to its *Home Network i.e.* its main organization. Inside this *Home Network* the mobile node is referenced by a *Home Address*. This *Home Address* identifies the node permanently, even if it is not in its *Home Network*. Since the IP routing is hierarchical, the mobile node address identifies the node and its subnet. When the mobile node moves, packets addresses to its *Home Address* keep being routed to its *Home Network*. This is the reason why the mobile node can't keep using its *Home Address* after he moved to a *Foreign Network*.

When the mobile node moves, it may visit a network belonging to another IP domain. This network is referred to as the *Foreign Network*. The *Foreign Network* owns a particular entity named a *Foreign Agent*. A *Foreign Agent* is responsible for giving the mobile node a temporary address called a *Care of Address*.

When a mobile node moves to a *Foreign Network* it registers to the local *Foreign Agent*. After the mobile node registered it receives its *Care of Address* and informs its *Home Agent* of its new address. The *Home Agent* binds the *Care of Address* with the *Home Address*. Since that moment all the traffic from or intended to the mobile node will transit through a tunnel between the *Foreign Agent* and the *Home Agent*. This process is completely transparent to the mobile node's correspondent that keeps on communicating to the mobile node by using its *Home Address*. With this macro-mobility, model mobile nodes can move to different organizations or Internet Ser-

vice Provider (ISP).

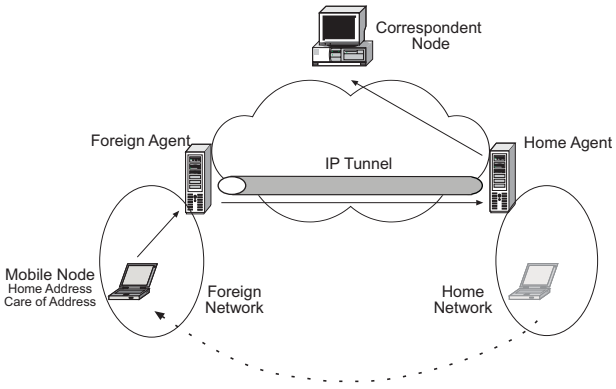


Figure 2: Communication example in MobileIP

Some improvements have been proposed to enhance the performances which can for instance allow the mobile node to communicate directly with its correspondent. One main drawback of MobileIP comes from its low performances in case of frequent handhoffs since this protocol requires to set up a tunnel between the *Home Agent* and each *Foreign Agent*. Some improvements have thus been proposed as we will see in the following section.

2.3 Micro-mobility

Until now three main solutions have been proposed to enhance MIP: CellularIP [32],[1], HAWAII [21] and Hierarchical MobileIP (HMIP) [11]. These approaches complement MobileIP since they have been proposed in order to decrease the latency time due to frequent handoffs of mobile nodes. When the mobile moves frequently, it sends update messages to its *Home Agent* and a new tunnel has to be established between the *Home Agent* and the new mobile's *Foreign Agent*.

The three proposals here are roughly based on the same idea. They modify the architecture of MobileIP in two distinct levels by the introduction of a local or regional agent. This agent is responsible for a local IP domain such as a campus or a Metropolitan Area Network. Depending on the version of IP in use, the mechanisms of this three approaches are slightly different.

In the case of IPv4, the mobile node registers to its *Home Agent* by using the regional agent address as its own *Care of Address*. The mobile node's *Home Agent* keeps a tunnel to the regional agent during all the time the mobile node it is responsible for stays in the IP domain. When the mobile moves from one radio cell to another within the same domain, its localization update is only forwarded to the regional agent. Moreover the interruption time between two handoffs becomes shorter since the necessary updates are done closer to the mobile node.

With IPv6 the process is simpler. To prevent too many address reconfigurations and DADs, the regional agent broadcasts its address prefix. As long as the mobile node stays in the regional agent domain, it doesn't have to change its address.

We haven't described more precisely these three approaches since the main focus of our paper is the auto-configuration schemes of mobile nodes when they move from one network to another. That is why we won't discuss these points further.

3 Addressing Issues in MANETs

MANETs are usually presented as mobile networks without any fixed infrastructure. They are suitable for temporary communications where it is not required to set up a network architecture. That is why MANETs are usually seen as spontaneous networks bound by a common goal (army, sanitary organizations ...).

In MANETs all the nodes act as *end user terminals* as well as *routers*. From this aspect they completely differ from other mobile approaches such as MIP. As these Ad hoc networks are built from scratch, their basic topology is flat. This is a major difference with common IP networks which addressing structure organization is hierarchical. Moreover even if they are considered as mobile networks, they are not necessarily connected to the Internet through a base station. This is another difference from MIP since there is no obvious need of Internet connectivity.

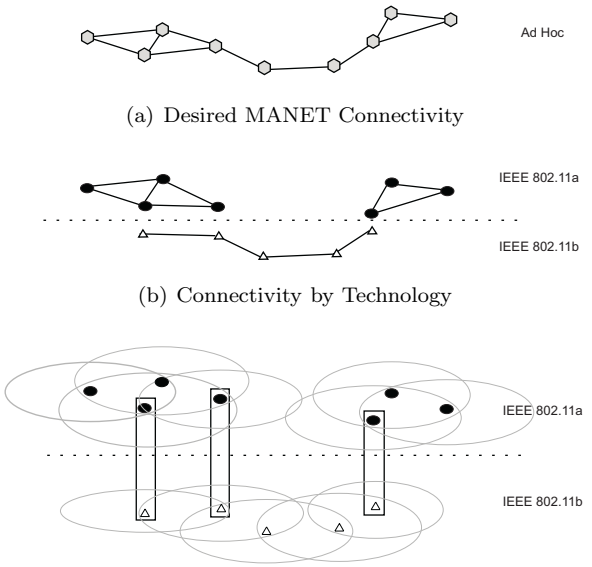
3.1 Basic Problems for MANETs

Until this point MANETs have been described through their functional characteristics. But the reality of MANETs is that they are based on different link layer technologies. The recent explosion of wireless network technologies (IEEE 802.11, BlueTooth etc) makes it possible to set up MANETs. But these MANETs may have to use several standards. At the moment we can't predict if one of these support technologies will override all the others. The actual evolution seems to indicate that they will probably have to coexist with each other.

Because of these competing technologies, the link layer architecture of MANETs is different from the one in use in traditional IP networks. Usually an IP subnet is composed of one unique link layer technology. Several subnets with different link layer technologies can interconnect to each other in some edge points of the subnets. For instance different LANs using Ethernet may interconnect their ISP network running ATM.

In the case of MANETs, not all the nodes run the same link layer technology. Since these technologies keep on improving, mobile nodes will probably be able to use different link layer technologies. It becomes possible for one mobile node to carry different chipsets allowing it to communicate using different wireless technologies. That is why it is likely the number of interconnection points between different MAC technologies will keep on increasing and these

points will be scattered everywhere in the MANET (*cf.* figure 3).



(a) Desired MANET Connectivity

(b) Connectivity by Technology

(c) Different MAC Layer Technologies.

Figure 3: Different representation of the same physical topology

Since MANETs are multi-hop networks, each node acts as a terminal as well as a router. This characteristic becomes a problem in case of broadcast or multicast communications since nodes decrease the TTL parameter of IP multicast packets at each hop. Local multicast communications *i.e.* in the same Local Area Network won't work since each MANET node is a router. It can also be an issue in case of the coexistence of different radio technologies. For some of them, for instance Hiperlan 1, the Layer two already deals with routing issues, whereas for some other it doesn't. It will then be more complex to manage such heterogeneity.

Another characteristic of MANETs concerns routing protocols. They are slightly different from the ones used in wired IP networks. MANET routing protocols are usually classified in two categories: proactive and reactive routing protocols. On the one hand proactive protocols such as DSDV [19], WRP [26] or OLSR [3] compute routes to MANET destination before they have to use it. On the other hand, reactive protocols such as AODV [20] or DSR [14] establish routes on demand only.

In the case of MANETs, centralized configuration architecture such as DHCP can't stand as a reliable solution since a server or nodes can be disconnected from the MANET from time to time. A fully distributed approach such as Zeroconf or any DAD approach may becomes "tricky", since these approaches require the participation of all the nodes of the network (*i.e.* a reliable multicast communication channel). Because of the possible sporadic attendance of the nodes we can't assume that a DAD can be used as in a wired network. For example a node could configure itself with the address of another node that has been shortly unreachable from the rest of the MANET.

Moreover approaches based on DAD mechanisms as described above don't provide much help in the case of splitting or merging networks. If several networks merge, it is possible that several nodes formerly in each merged partition own the same address. In order to prevent this situation to happen, the DAD must be performed again by all the MANETs nodes. The cost in overhead communication could be high. Until now, no solution has been proposed to improve the DAD process so that it can detect that two MANETs have merged. A supplementary process is necessary to detect that different subnets have merged. If a MANET splits in different parts, the consequences are not as strong as in the previous case since each part of the original MANET contains nodes that use unique addresses, but each partition has to be able to configure new arriving nodes.

3.2 A Dedicated Addressing Layer

ANANAS [6] is an approach that tries to give some answers to one of the problems presented in section 3.1. ANANAS considers MANETs as stub networks *i.e.* mostly all the communications are originated from or intended to the MANET. This hypothesis is far from the use of a "traditional MANET". The authors of ANANAS consider that there isn't much traffic between nodes within the same MANET.

As seen in section 3.1 the characteristics of MANETs lead to problems for the implementation of multicast or broadcast communications. MANET nodes don't consider themselves as belonging to the same LAN since the TTL parameter of the broadcast or multicast IP packet decreases each time it is forwarded to a node.

As said above not all nodes of a MANET use the same link layer technology. This situation is presented in figure 3. With this example we see that the MANET as we would like it to be (figure 3(a)) relies on different layer 2 technologies (figures 3(b) and 3(c)). ANANAS provides a new abstraction layer called *Ad Hoc Layer* between the IP and the MAC layers. This layer has two main goals. The first one is to allow IP packets to be sent to all the nodes of the MANET regardless of their link layer technology. The IP layer sees a homogeneous set of nodes where MANET nodes with several MAC technologies are transparent interconnection points. The second goal is to provide to the IP layer a virtual LAN. This allow for a simpler implementation of multicast and broadcast communications in a MANET.

The ANANAS approach doesn't provide any new way of routing. They rely on the existing routing protocols. The *Ad Hoc Layer* adds two new address translation processes : one between the MAC layer and the *Ad Hoc Layer* the other between the *Ad Hoc Layer* and the IP layer. This implies a new address

resolution process and a new route discovery process in the *Ad Hoc Layer*.

The ANANAS approach contains questionable points. MANETs are spontaneously organized networks, seeing them only as stub networks may be a too restrictive hypothesis since the most often considered spreads of MANETs are natural disasters, army operations or campus environments.

Since the authors consider only MANETs with an Internet connection, they keep relying on the IP addressing scheme even if they introduce a new kind of address to uniquely identify the MANET nodes. The authors justify this choice by claiming that the IP stack is the standard for network application. This point is true, but even if a MANET provides the IP interface to the applications, it doesn't mean that the MANET has to use the IP addressing and routing as we will see in section 4.

Finally the proposed ad hoc address is based on the MAC address of the node interface. As described in [12] and [17], the MAC address is not obviously unique so this may not be a good choice. At least the use of the MAC address as a unique identifier (if we consider that it is possible) allows the identification of the user and then the possibility for other people to keep track of him.

Nevertheless ANANAS gives new answers to some of the problems of MANETs. Even if this approach contains some restrictions, the ideas developed in it may be improved or combined with other mechanisms to provide better functionalities to the IP layer.

3.3 MobileIP and MANET

We just have seen an "underlying IP proposal", but some proposals have been made in the IP layer in order to give an answer to the problems generated by MANETs. Here we consider MANETs with or without Internet connectivity. From now on we will refer to MANETs without any Internet connectivity as standalone MANETs by opposition to Internet connected MANETs.

The auto-configuration solutions we have presented for wired networks are not suitable "as is" for MANETs. But some proposals try to adapt these mechanisms to provide auto-configuration possibilities to MANETs.

3.3.1 MANET Working Group Proposal

The MANET working group of the IETF proposes an approach based on a DAD process to configure the MANETs [5]. This draft proposes a mechanism which adapts the DAD process described above to MANETs. Since a DAD run once can't ensure that all the nodes have been reached, [5] proposes a repeated DAD within the MANET. This repeated DAD based on a flooding is used to increase the reliability of the DAD process. As this improvement is only the repetition of the DAD process, this is more an engineering fix than a complete solution.

As we have seen above the DAD is based on timeout. The correct values of the timeout can be difficult to set accurately in a MANET. Since different MANETs have different and changing topologies a particular timeout value won't be useful for all of them. Since the repetition can't completely ensure that the DAD process would be performed correctly, it is difficult to evaluate the real interest of this approach.

3.3.2 Internet Connected MANETs

In the case of Internet connected MANET the situation is different from the previous one *i.e.* at least one node of the MANET is in the radio range of an Internet access point (a WiFi access point for example). This connection point to the Internet is referred to as a gateway for the MANET. This situation is really close to the MobileIP process presented in section 2.2 where the gateway acts as a *Foreign Agent*.

This gateway provides a prefix for the configuration of the nodes. In IPv4, [8] proposes a reserved prefix for the MANET, whereas in IPv6 [22], the gateway just acts as a router, advertising its prefix to the nodes of its subnet. These configurations are similar to the MobileIP process [7].

In order to explain these approaches we are going to refer to the IPv6 solution [22]. In [22], a new specific IPv6 multicast address is proposed to reference all the possible gateways in the MANET. When a node N arrives in a MANET it is assigned a global temporary address (this can be its Home Address or a temporary address based on a specific MANET prefix). N sends a request to the multicast address referencing all the gateways. The answer of one of the gateways gives it a valid prefix and a route to the gateway.

When N wants to communicate with a node D, it has to chose between two methods depending on the topology and the routing protocol in use in the MANET. The first method allows N to send packets by filling their destination field with D's global address. In this case N relies on next hop routing of the other MANET nodes. The second solution recommended by [22] involves the gateway. N sends packets with the address of the gateway as the destination address field of the IP packet. The IP address of D is registered in a routing header. If D belongs to the MANET, any intermediate MANET node or the gateway itself can reroute the packets. Another advantage appears when there are several gateways in the MANET. With the second solution the node can chose which gateway it wants to use.

This proposal implies that the gateway knows the address of all the MANET nodes to be able to route correctly all the packets. This point may lead this proposal to hardly scale to large MANETs. Moreover these proposals don't address any particular solutions to the problem of merging or splitting MANET.

3.3.3 Addressing Agent

In order to adapt the DHCP auto-configuration model to MANETs, [9] propose an *Addressing Agent* approach. This proposal is roughly based on the election of one of the MANET nodes as an address configuration server. This node, acting as the *Addressing Agent*, keeps a list of all the MANET nodes. This list contains the mapping of MAC to IP addresses.

The goal of this approach is to provide exactly one *Addressing Agent* to each MANET. If no *Addressing Agent* exists, one has to be chosen. If several *Addressing Agents* are present in the MANET one must be chosen as the unique *Addressing Agent*. In this situation the detection of multiple *Addressing Agents* is realized thanks to the address configuration messages. The *Addressing Agent* with the lowest MAC address is chosen.

This approach is interesting since it provides scenarios for union or splits. In the case of the union of several MANETs, only the *Addressing Agent* with the lowest MAC address will act as an address configuration server. Some nodes will have to be readdressed and the communications will be interrupted with them. The interest of this approach is that after the readdressing, the new MANET will be a coherent set of configured nodes.

When a MANET splits into different partitions, there won't be any address conflicts in either of the resulting partitions. But only one of them will own an *Addressing Agent*. Each one of the other partitions will have to elect a new *Addressing Agent* in a common way.

We see that this approach provides a solution to handle MANET splits without any problem. A solution is proposed to make possible the union of several MANETs that can lead to an interruption in communication for the nodes that need to be readdressed. But some simulation results provided by [9] show that the time spend by the *Addressing Agent* approach to readdress the nodes in case of union is really close to the time spent by DAD based approaches.

3.4 Duplicate Address Detection for MANETs

In the previous section we presented the basic adaptations of IP mechanisms to MANETs environments. In order to improve the reliability of these solutions, some proposals have been presented. In the following section we are going to present two of them.

3.4.1 Weak Duplicate Address Detection

As we have seen before, the DAD can't always be achieved in MANETs. [29] is a more formal explanation about this observation. In this paper, the author introduces the notions of *Strong DAD* and *Weak DAD*. He defines *Strong DAD* as the process that allows at least one node to detect a duplicate address just after this address has been chosen by another node. This *Strong DAD* corresponds to the notion of DAD we used until now. Unlike the *Strong DAD*, the *Weak DAD* has a more relaxed definition. *Weak DAD* ensures packets are routed to the correct destination, but it doesn't imply that this process allows immediate detection of identical addresses.

[29] presents in a formal way that a *Strong DAD* can't be guaranteed in MANETs when message delays are not bounded. That is why a simple DAD only based on timeout can't be considered as reliable. Instead, the author proposes *Weak DAD* mechanism based on enhancement of a link state routing protocol. This *Weak DAD* may be extended to other protocols.

In this approach, each node of the network owns a unique identifier. Each time a node sends a control packet indicating its link state; it adds its identifier to the packet. Each node keeps states on the links it is connected to, the corresponding nodes it is in relation with and their identifier. If a node N receives a control packet with an address he knows but a different identifier, N concludes it has detected a duplicate address. From this point, N begins to announce the duplicate address and keeps sending the packets to the node it knows that previously uniquely owned the address.

This paper presents the DAD mechanism in a formal way. Another point is that it proposes a way to really allow two MANETs partitions to merge without any need of a network identifier. Moreover this process keeps the partition in a coherent state until all the address conflicts are solved. Finally this proposed solution stands in a slight modification of existing protocols.

3.4.2 MANETConf

MANETConf [18] is another approach for stand-alone MANETs. It proposes a reliable DAD, which ensures that all the configured nodes of the MANET answer to the DAD request. Moreover, the DAD process has been extended to a two phase process: initiation and validation.

The attribution of an address is done as follows. A new arriving node (the requester) asks for the help of a former configured neighbor (the initiator) in order to obtain its configuration information. The initiator broadcasts an address for the requester on the MANET, so the requester doesn't have to use a temporary address in order to obtain the definitive one.

Another difference from DAD based approaches concerns the answer of the MANET nodes to the initiator's request. In the DAD described until now, only the node that owns the requested address, answers the DAD request. Here it is the opposite. All the nodes have to answer to the request. This ensures that the requester won't use the address of a node that has been temporarily disconnected from the MANET.

If a node doesn't answer after a given number of

attempts, it is considered as having left the MANET. Its address can be relinquished to the set of unassigned addresses. This implies that each node of the MANET keeps a list of all assigned addresses in their MANET. This list is maintained in a soft state way thanks to the DAD requests themselves.

MANETConf proposes a mechanism to handle splitting MANET. All nodes have a universal identifier. The node N that is configured with the lowest IP address represents the MANET identifier which is defined by the tuple (IP address, universal identifier). When the MANET splits, only one partition will own the node N (we call this partition A and B the other one). When a new node M arrives in B, N is not able to answer to the DAD request. Then M's initiator realizes that N doesn't belong to its MANET. M's initiator then broadcasts a cleanup message on the MANET partition to inform the others that the MANET has split. Thanks to this process all the nodes from B are able to update their address list. The process is similar for A's nodes. Addresses of B's partition nodes become free address for A's nodes and vice versa.

In MANETConf two nodes, M and N, that initiate a communication, exchange their MANET identifier. If the identifiers are different M and N realize their MANETs have merged. Because M and N know all the addresses in use in their MANET they can identify which nodes own conflicting addresses. These nodes with conflicting address will need to perform a new DAD to be configured again.

It is important to notice that in case of partitions union, a node P and some of its radio range neighbors may have conflicting addresses. In that case, since P needs a configured Initiator, some nodes may remain unreachable until the situation is fixed.

We see that the "MANETConf DAD request" generates more traffic than the "classical DAD" one. This is done to ensure the reliability of the DAD. So far, no studies have been conducted to compare the communication cost between the MANETConf's DAD and the DAD proposed by the MANET Working Group. Such a work would be interesting to determine in which cases each approach gives the best results. It is very likely that this extra cost will not always be worthy as it would depend on execution scenarios: topology, nodes mobility ...

4 Scalability in MANETs

All approaches presented before and dealing with address allocation in MANETs don't scale very well. As it is difficult to extend such solutions to ensure scalability in wider MANETs, some other approaches have to be considered. Other existing solutions have been proposed for very wide networks and should be looked at for that purpose. These proposals are not IP based but rely either on geographical position of nodes or on peer-to-peer solutions to route data to the destination.

4.1 Partition Prediction

In [30] and [31] the authors describe a way to identify mobility patterns thanks to movement vector of MANETs nodes. The use of these movement vectors is based on the geographical position plotting between different moments. By using those mobility patterns, they propose a way to ensure the reliability of any service in MANETs. [30] proposes a mechanism to allow servers in a MANET to detect the future partitions and to replicate themselves in each predicted partition.

Thanks to the mobility pattern recognition, servers are able to classify all their client nodes in different mobility groups. When servers detect a possible split they replicate themselves in the future partition to ensure the service continuity. At the same time, [30] proposes a fully distributed algorithm so that the mobile nodes can choose the server that fits them at best. The MANET nodes just simply need to discover the server with a similar movement vector.

As the address auto-configuration process can be considered as one of the first services to guarantee, this proposal can be interesting to enhance the robustness of existing mechanisms. Nevertheless this solution uses a strong centralized approach to detect partitions and its applicability as such may be questionable. It would be interesting to evaluate the possibility of making this partition detection in a distributed manner.

4.2 Geographical Routing

Since the solutions used in wired networks can't directly be used for MANETs, some completely different ways of routing have been developed. Among others, the geographical routing approaches take advantage of the improvements made in earth's positioning technologies. Since it is now possible for laptops and PDAs to carry a GPS chipset, the use of nodes position becomes a reality. Even if the GPS technology is mainly useful in the case of outdoor networks, other proposals have been made in order to provide location information without the GPS. [25] is an example of GPS-free positioning.

GLS (Grid Location Service [10], [13]), LAR (Location Aided Routing, [27]) and DREAM (Distance Routing Effect Algorithm for Mobility, [27],[16]) are only based on geographical addressing and forwarding. DREAM is a proactive protocol whereas LAR is a reactive one. Both of them use the geographical position and forwarding facility to reach their destinations. In case they don't know the position of the destination LAR and DREAM use flooding to determine in which direction they have to send the packets.

GLS also uses geographical forwarding, but with GLS, a node N keeps its location information stored

in some other nodes of the network. These nodes are called location servers for N and are chosen based on their unique identifier value. Each node may become a location server for some other nodes. The geographical space is divided into a hierarchy of grids that is supposed to be known by all the MANET nodes. The organization of the grids in GLS is a quad tree decomposition. Each node chooses a location server at each level of the grid hierarchy. This ensures the location information of each node to be reachable by all the nodes of the MANET.

Moreover the quad tree structure has been well studied in graph theory and gives good performances to the GLS proposal. In terms of configuration, the geographical routing approach doesn't have any limit in terms of number of nodes. In the case of network merging, the organization of the location servers may change. Since the choice of node's location servers depends on the nodes identifiers, new merged nodes may have to be chosen as new location servers. It could be interesting to study the cost of new location server choice for each node.

4.3 Indirect Routing

Without any need of geographical information, Indirect routing is an alternative different from the geographical routing approach to replace the IP addressing and routing. The Tribe protocol [2] provides such functionalities. By using a well-known hash function, Tribe build a virtual network topology that reflects the physical relative position of the mobile nodes. Based on this concept, the Tribe protocol [2] uses a well-known hash function to build a virtual network topology that reflects the physical relative position of mobile nodes. Each node of the network manages one region of the virtual addressing space. Nodes use a unique identifier that could be for instance an IP address. Thanks to the hash function, a new node N can determine which other node P will maintain its location information. Since the hash function is known from all the nodes in the network, each of them knows that it has to contact P to retrieve N's location information.

The Regions of the virtual space are adjacent in Tribe. So the node S that contacted P can reach N by forwarding the message to its neighbor whose region is the closest to N's one. Thanks to this indirect routing, we see that the addressing and routing functionalities become independent from each other. This allows the nodes to use another addressing scheme and another routing than the IP one. This is an important property since the MANETs may not have a connection point to the Internet and so may not use the IP routing. Another property of this approach is its high scalability characteristic, indeed Tribe can be considered as a fully distributed Home Agent approach thanks to its peer-to-peer nature.

The problem of this approach comes from the merging and splitting of MANETs. The merging of two MANETs may be difficult to handle without too many problems by Tribe. If two MANETs running Tribe merge, they will have to manage two virtual spaces. Each virtual space can be seen as an independent virtual space layer. This allows Tribe to handle this situation but makes it have to manage several virtual spaces.

The split of MANETs may be more complex. Since a MANET can result from several unions, Tribe deals with several virtual space layers. When it splits, the resulting partitions may not correspond to a particular layer. So each partition keeps on dealing with several virtual spaces. It is difficult to imagine that the coherence of each virtual space can be easily maintained. Another point during a split is that a node N and its virtual home agent are not necessary neighbor, they probably won't be in the same partition. This can lead to a long interruption of the communication between N and the other nodes of the partition he lies in.

4.4 The Terminodes Project

The Terminodes Project [15] proposes a model for Geographical routing that can be applied to standalone or Internet connected MANETs. This paper mainly focuses on the routing part issues but introduces an example of addressing based on positioning.

In the Terminodes approach, nodes are assigned a unique identifier (End-system Unique Identifier, EUI) that uniquely identifies them along their movements. At the same time, nodes own a transient position based address (Location Dependent Address). The nodes use this address to send and receive packets during their movements.

The routing process is composed of two parts: Remote and Local routing. The Remote routing is used to forward the packets in the direction of the destination. The Local routing is used to reach the destination node from an intermediate destination neighbor node.

For the configuration purpose, the Terminodes project uses an indirect routing close to the architecture of Peer-To-Peer (P2P) networks. As in P2P networks (like [24]), the Terminodes addressing part uses a hash function to distribute the location information of a node D along the nodes of the MANET. A well-known hash function $H(EUI_D)$ determines an area called Virtual Home Region (VHR). This VHR is defined by a center and a radius. All the nodes included in the VHR keep the location information of D.

When a node S wants to send a message to D, it contacts first the nodes belonging to D's VHR by computing the center of the VHR thanks to the hash function. One of the node of D's VHR sends back to S the position of D. Thanks to the hash function, the location information of the nodes is distributed in a subset of nodes of the network. That offers a high scalability property to this proposal.

Proposal	Stand-alone	Architecture	Reliability	Scalability	Union/Split
MANET WG	Yes	Distributed	Repeated DAD	Good, distributed architecture	No
Internet Connected	No	Centralized	Simple DAD	The gateway knows all the addresses in MANET	Union
Addressing Agent	Yes	Centralized	-	The addressing Agent keeps a state on each MANET node	Union and Split
MANETConf	Yes	Distributed	Improved DAD	Each node knows all the others	Union and Split
Geographical Routing	Yes	Distributed	-	Good, distributed architecture	Union and Split
Indirect Routing	Yes	Distributed	-	Good, distributed architecture	Difficult to handle
Terminodes	Yes	Distributed	-	Good, distributed architecture	Difficult to handle

Table 1: Characteristics comparison of the presented approaches

[15] don't provide too many details on the way to handle split and union of MANETs. If several MANETs merge, the VHR of a node N may contains nodes from other partitions. These nodes don't own N's location information. So they can't answer to the request of nodes that are looking for N's localization. In the case of a splitting MANET, a node N and its VHR may stand in different partition. In this case N becomes unreachable until it computes a new VHR. For both of the cases a more detailed mechanism is needed to allow Terminodes to handle MANET split and union.

5 Conclusion

We have identified different types of mobility, each raising different configuration issues. Some solutions have been proposed but they are only adapted to restricted mobility conditions. MANETs appear to concentrate most addressing routing and configuration problems. There is no perfect solutions at the moment to deal with such environments. Classical IP solutions remain necessary if not for routing, at least for addressing issues as they are used by all the Internet applications. They could also constitute a good convergence Layer for the coexistence of different radio technologies.

Another observation concerns the nature of MANETs. If a MANET is connected to the Internet by few nodes, these nodes will probably be the bottlenecks of all the traffic between Internet and the MANET. Because of the small and limited radio bandwidth capacity of mobile nodes, we may consider such MANET as standalone MANETs. That is why we think that alternative routing proposals should be considered.

Such approaches different from IP routing solutions propose independent mechanisms to improve the scalability of MANETs. These approaches based on Geographical Forwarding, Peer-To-Peer or a hybrid scheme between these two, allow to keep IP only as an API for network applications. Their common characteristics is to define a unique identifier for each mobile node. The Peer-To-Peer approaches have another advantage, unlike the Internet Protocol or the Geographical Forwarding, they separate addressing and routing issues. This could thus allow a mobile node to keep its identifier whichever routing protocol is used in the network it is connected to.

Concerning the fusion and partitioning of MANETs,

few approaches propose a complete solution with a high scalability. The only approaches that can allow fusion and partitioning are the geographical ones. At the same time these approaches also allow partition predictions as detection is based on the movement vector of each mobile node. These vectors are currently deduced from geographical position of nodes.

Finally we present in table 1 some of the main characteristics of the approaches we presented. We consider that a good addressing scheme must have good scalability properties, that it can be configured with or without an Internet gateway and that he can handle easily union and splits of MANET. These considerations tend to make us consider more carefully alternative proposals. At the moment, only the Geographical Routing such as GLS has good scalability properties and is capable of handling union and partitioning.

References

[1] A. Valko, A. Campbell and J. Gomez. Cellular IP. Internet-Draft, November 1998. draft-valko-cellularip-00.txt - Work-in-progress.

[2] A.C. Viana, M.D. de Amorim, S. Fdida and J.F. de Rezende. Indirect Routing Using Distributed Location Information. In *IEEE International Conference on Pervasive Computing and Communications (PerCom). Dallas-Fort Worth, Texas.*, March 2003.

[3] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum and L. Viennot. Optimized Link State Routing Protocol. Internet-Draft, March 2003. draft-ietf-manet-olsr-08.txt - Work-in-progress.

[4] C.E. Perkins, B. Patil and P. Roberts. IP Mobility Support for IPv4, August 2002. IETF RFC 3344 - Standard Tracks.

[5] C.E. Perkins, E.M. Royer and S. Das. IP Address Autoconfiguration for Ad Hoc Networks. Internet-Draft, November 2001. draft-ietf-manet-autoconf-01.txt - Work-in-progress.

[6] G. Chelius and E. Fleury. ANANAS: A New Ad Hoc Network Architectural Scheme. Research Report RR-4354, Inria, January 2002.

[7] D. Johnson, C.E. Perkins and J. Arkko. Mobility Support in IPv6. Internet-Draft, February 2003. draft-ietf-mobileip-ipv6-21.txt - Work-in-progress.

[8] E.M. Belding-Royer, Y. Sun and C.E. Perkins. Global Connectivity for IPv4 Mobile Ad Hoc Networks. Internet-Draft, November 2001. draft-royer-manet-globalv4-00.txt - Work-in-progress.

[9] M. Günes and J. Reibel. An IP Address Configuration Algorithm for Zeroconf. Mobile Multi-hop Ad Hoc Networks. In *Proceedings of the International Workshop on Broadband Wireless Ad-Hoc Networks and Services. Sophia Antipolis, France*, September 2002.

[10] N. Guba and T. Camp. Recent Work on GLS: a Location Service for an Ad Hoc Network. In *Proceedings of the Grace Hopper Celebration (GHC)*, 2002.

[11] H. Soliman, C. Castelluccia, K. El-Malki and L. Bellier. Hierarchical Mobile ipv6 mobility management (hmipv6). Internet-Draft, October 2002. draft-ietf-mobileip-hmipv6-07.txt - Work-in-progress.

[12] IEEE. Guidelines for 64-bit global identifier (eu-64) registration authority, May 2001. http://standards.ieee.org/regauth/oui/tutorials/EUI64.html.

[13] J. Li, J. Jannotti, D. De Couto, D. Karger and R. Morris. A Scalable Location Service for Geographic Ad Hoc Routing. In *Proceedings of the 6th ACM International Conference on Mobile Computing and Networking (MobiCom '00)*, pages 120–130, August 2000.

[14] D.B. Johnson and D.A. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. In *Mobile Computing*, volume 353. Kluwer Academic Publishers, 1996.

[15] L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, J. P. Hubaux and J. Y. Le Boudec. Self-Organization in Mobile Ad Hoc Networks: the Approach of Terminodes. *IEEE Communications Magazine*, 39(6), June 2001.

[16] M. Mauve, J. Widmer and H. Hartenstein. A Survey on Position-based Routing in Mobile Ad Hoc Networks, November 2001.

[17] Microsoft. How to troubleshoot duplicate MAC address conflicts, December 2001. http://support.microsoft.com/support/kb/articles/Q164/9/03.asp.

[18] S. Nesargi and R. Prakash. MANETConf: Configuration of Hosts in a Mobile Ad Hoc Network. In *IEEE INFOCOM 2002*, New York, NY, June 23-27 2002.

[19] C.E. Perkins and P. Bhagwat. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In *ACM SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications*, pages 234–244, 1994.

[20] C.E. Perkins and E.M. Royer. Ad-hoc On-Demand Distance Vector Routing. In *MILCOM '97 panel on Ad Hoc Networks*, November 1997.

[21] R. Ramjee, T. La Porta, S. Thuel, K. Varadhan and L. Salgarelli. IP micro-mobility support using HAWAII. Internet-Draft, June 1999. draft-ietf-mobileip-hawaii-00.txt - Work-in-progress.

[22] R. Wakikawa, J.T. Malinen, C.E. Perkins, A. Nilsson and A.J. Tuominen. Global Connectivity for IPv6 Mobile Ad Hoc Networks. Internet-Draft, November 2002. draft-wakikawa-manet-globalv6-01.txt - Work-in-progress.

[23] S. Cheshire, B. Aboba and E. Guttman. Dynamic Configuration of IPv4 Link-Local Addresses. Internet-Draft, August 2002. draft-ietf-zeroconf-ipv4-linklocal-07.txt - Work-in-progress.

[24] S. Ratnasamy, P. Francis, M. Handley, R. Karp and S. Shenker. A Scalable Content Addressable Network. In *Proceedings of ACM SIGCOMM 2001*, 2001.

[25] S.Capkun, M. Hamdi and J.P. Hubaux. GPS-Free Positioning in Mobile Ad Hoc Networks. In *The 34th Hawaii International Conference on System Sciences*, 2001.

[26] S.Murthy and J.J. Garcia-Luna-Aceves. An Efficient Routing Protocol for Wireless Networks. *Mobile Networks and Applications*, 1(2):183–197, 1996.

[27] T. Camp, J. Boleng, B. Williams, L. Wilcox and W. Navidi. Performance Comparison of Two Location Based Routing Protocols for Ad Hoc Networks. In *IEEE INFOCOM 2002*, New York, NY, June 23-27 2002.

[28] S. Thomson and T. Narten. IPv6 Stateless Address Autoconfiguration, December 1998. IETF RFC 2462 - Standards Track.

[29] N.H. Vaidya. Weak Duplicate Address Detection in Mobile Ad Hoc Networks. In *Proceedings of the third ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pages 206–216. ACM Press, June 2002.

[30] K.H. Wang and B. Li. Efficient and Guaranteed Service Coverage in Partitionable Mobile Ad Hoc Networks. In *IEEE INFOCOM 2002*, June 23-27 2002.

[31] K.H. Wang and B. Li. Group Mobility and Partition Prediction in Wireless Ad Hoc Networks. In *IEEE International Conference on Communications (ICC 2002)*, New York, NY, April 2002.

[32] Z.D. Shelby, D. Gatzounas, A. Campbell and C.Y. Wan. Cellular IPv6. Internet-Draft, November 2000. draft-shelby-seamoby-cellularipv6-00.txt - Work-in-progress.