Integration of Mobile-IP and OLSR for a Universal Mobility *

Mounir BENZAID[1,2], Pascale MINET[1], Khaldoun AL AGHA[1,2], Cedric ADJIH[1] and Geraud ALLARD[1]

[1]INRIA, Domaine de Voluceau - B.P.105, 78153 Le Chesnay Cedex, France
{mounir.benzaid, pascale.minet, cedric.adjih, geraud.allard}@inria.fr

[2]LRI, Bât 490 Université Paris Sud, 91405 Orsay Cedex, France
alagha@lri.fr

***Abstract*—Trends in fourth generation (4G) wireless networks are clearly identified by the full-IP concept where all traffic (data, control, voice and video services, etc.) will be transported in IP packets. Many proposals are being made to enhance IP with the functionalities necessary to manage the mobility of nodes, so that networks can provide global seamless roaming between heterogeneous wireless and wired networks. In this paper, we focus on the management of universal mobility, including both large scale macro-mobility and local scale micro-mobility. We propose a hierachical architecture (i) extending micro-mobility management of a wireless access network to an ad-hoc access network, (ii) connecting this ad-hoc network to the Internet and (iii) integrating Mobile IP and OLSR, a routing protocol for ad-hoc networks, to manage universal mobility. This architecture is validated by an implementation based on DynamicsMobile-IP and OLSR version 7. We show how the brodcast of Mobile-IP Agent Advertisement can be optimized using OLSR MPR-flooding.**

Keywords: mobile ad-hoc networks, mobility management, macro-mobility, micro-mobility,Mobile-IP, OLSR.

I. INTRODUCTION

With recent technological advances in palm-top computers and cellular phones, it is apparent that wireless networks exist to facilitate mobility and have generated a large movement to bring Internet capabilities to these wireless mobile devices. Indeed, they enable a user to remotely access the Internet anytime and anywhere (e.g. from university, visited company, home, hotel, etc.). However, to forward data to a mobile node, it is necessary to locate it and follow it in its motion, which introduces complications in routing protocols. On the other hand, the introduction of GPRS in GSM infrastructure networks, the migration towards UMTS technologies, the widespread use of the IEEE802.11 standard and the development of Bluetooth wireless LAN offer mobile wireless access for already supported applications (e.g. multimedia applications with data, voice and video traffic, etc.). Today, it is crucial to offer to users of these mobile wireless networks services that are as close as possible to those already existing in wired networks, and to guarantee service continuity and Quality of Service (QoS). In addition, the convergence towards *full-IP* networks in fourth generation (4G) wireless networks enables flexibility to design the core IP network independently from the access network with many different access technologies.

The Mobile-IP [1] standard presents a fundamental solution for mobility management in the Internet. With Mobile-IP, the mobile nodes are able to send and receive data whatever their current point of attachment to the Internet. Although Mobile-IP is mostly used for nomadic computing with wired connections in which a mobile node is unplugged from one physical attachment point and plugged into another, it can be used in a wireless environment. However, in the Mobile-IP protocol, mobile nodes have to report every change of their access points through foreign subnetworks to their home network. Such a change during active data transmission or reception is called a “handoff”. For example, if we considered each wireless access point, which covers only a small geographic area, as an IP subnetwork (i.e. attachment point to the Internet), then each handoff between cells would cause a huge amount of control overhead. The registration process is very long compared to the link-layer handoff time, especially if the mobile node is far from its home network, due to the high roundtrip time of the Internet. In addition, in a micro-cellular and pico-cellular network infrastructure environment (e.g. UMTS, Bluetooth, HIPERLAN, etc.), Mobile-IP would have to execute

* This work has been partially financed by the French RNRT (http://www.telecom.gouv.fr/rnrt/) project ARCADE (http://www-rp.lip6.fr/arcade/).

a costly registration process at a high handoff rate.

To resolve this problem mobility management is often divided into two parts: macro-mobility and micro-mobility. Macro-mobility concerns the management of mobile nodes moving on a large scale, between different domains (or wide wireless access networks), while micro-mobility covers the management of mobile nodes moving at a local scale, inside a domain (or a particular wireless network). Macro-mobility is usually assumed to be managed through Mobile-IP and several protocols, such as Cellular IP [2] and HAWAII [3], have been proposed to manage the micro-mobility problem.

In situations (e.g., conference rooms, forests, airports, subways and battle fields, etc.) where it is either not possible or too expensive to deploy 2G (GSM) and 3G (UMTS) cell-based mobile network infrastructures, an infrastructureless mobile network can be used. A network based on this idea is called “Mobile Ad-hoc NETwork” (MANET) [4], [5]. The advantage of an ad-hoc network is that it extends mobility to wireless and autonomous domains, where each node acts as a router and performs the mobility’s functionalities. In addition to being able to operate autonomously, an ad-hoc network can be attached at some access point(s) to the fixed Internet.

In this work, we propose an integrated hierarchical architecture that extends micro-mobility management to an ad-hoc network and interconnects the ad-hoc network to the existing wired networks and Internet. The wireless multihop access network is entirely based on IP, uses the Optimized Link State Routing protocol (OLSR) and meets the requirements of future *full-IP* wireless networks, such as providing high-rate video, voice and data services to the cellular handset or handheld Internet devices.

The remainder of this paper is organized as follows. In Section II, we describe different proposals to manage mobility in the Internet; we focus on the definition of the macro/micro mobility architecture and related work to combine infrastructure/infrastructureless networks with Mobile-IP. Section III proposes an architecture for managing mobility (intra/inter domain) in the Internet and briefly describes the OLSR protocol. The principles of the integration of Mobile-IP and OLSR are presented in Section IV. In section V we describe our implementation based on Dynamics Mobile-IP and OLSR version 7.

II. SOLUTIONS FOR MOBILITY IN THE INTERNET

The mobile nodes in the Internet must be able to reach their correspondents and to be reached by them, while moving from one Internet attachment point to another. The current version of the network layer protocol (IPv4) is no longer sufficient to support these mobile nodes. Indeed, IP makes two implicit assumptions. First, a point at which a node is attached to the Internet remains fixed, and secondly a node’s IP address identifies the network or subnetwork to which it is attached. The protocol that manages the mobility must be transparent to the transport layer to guarantee continuity of service; it must be compatible with IP; and for reasons of scalability it must not require any changes to existing Internet hosts and routers. To meet these requirements “Mobile-IP” [1] was developed as a fundamental solution for the management of mobility in the Internet.

A. Mobile-IP

Routing of packets is based on the location information contained in the node’s destination IP address. This IP address includes two parts: the *network identifier* and the *host identifier*. If a mobile node moved to another network without changing its IP address, it would no longer be possible to correctly route packets to it. On the other hand, if a node is configured with a new IP address, it will lose its active upper layer protocol connections, such as TCP sessions. In this context, Mobile-IP protocol [1] has been developed within the IETF [6] to handle mobility through different IP networks. It is an enhancement of the Internet Protocol intended to enable nodes to maintain Internet connectivity with the same IP address regardless of their attachment IP subnetworks. Each mobile node is assigned an IP *home address* belonging to a particular network, known as its original or *home network*. The *home address* is static: it remains unchanged as the mobile node’s location varies, and any packet addressed to it is routed to the *home network*. When the mobile node is connected to the *home network*, it behaves like any non-mobile node and it may be reached through normal IP routing.

On the other hand, when the mobile node moves to another network, it can no longer be reached solely on the basis of its *home address*, but must be assigned an address belonging to the visited network, which is considered as a *foreign network* for this node. This address is called the *care-of-address*. The *care-of-address* makes it possible to identify the actual location of the mobile node and to route packets up to this new location.

The *care-of-address* changes whenever the mobile node's visited network changes.

The key feature of Mobile-IP design is that all required functionalities for processing and managing mobility information are embedded in three defined entities: the *Mobile Node* (*MN*), the *Home Agent* (*HA*) and the *Foreign Agent* (*FA*).

- A *Mobile Node* is a host or a router that changes its attachment point from one network or subnetwork to another without changing its IP address. The *MN* has only one *home network*.
- A *Home Agent*, which can be a host or a router, is located on the *home network*. The task of the *HA* is to maintain the current location information for the mobile nodes when they are away from home. Then, the *HA* tunnels packets to their present location.
- A *Foreign Agent* is a host or a router on a visited or a *foreign network* that registers the entrance of mobile nodes, detunnels and forwards packets to the visiting mobile node.

Mobile-IPv4 operation is illustrated in Figure 1. It shows an IP data packet sent by a correspondent node (IP address 126.C.C.C) to the *MN* (IP address 129.175.M.N). In this figure, the *MN* is shown to be away from its *home network*. Hosts with IP addresses 129.175.H.A and 128.93.F.A are acting as its *Home Agent* and *Foreign Agent*, respectively. The packet to the *MN* arrives on the *home network* via standard IP routing (step 1), then it is intercepted by the *HA* and is encapsulated before being sent to the *FA* (step 2) using the *care-of-address* (IP address 138.93.F.A). On receiving the encapsulated packet, the *FA* decapsulates (i.e. removes the outer IP header) and delivers the original packet to *MN* visiting its local network (step 3). *MN* can directly reply to the Correspondent using its *home address* (step 4).

The *care-of-address* is the termination point of a tunnel toward a *MN*. Mobile-IP can use two different types of *care-of-address*: a "*Foreign Agent care-of-address*" is an address proposed by the *FA* with which the *MN* is registered; a "*co-located care-of-address*" is an externally obtained local address that the *MN* can dynamically acquire by DHCP [7].

There are two mechanisms to update location for a *MN*:

- **Agent discovery and solicitation:** Each *MN* is associated to a unique *home network* as indicated by its permanent *home address*. In order to communicate with mobility agents (i.e. *FA* and *HA*), a *MN* must discover the IP addresses of these agents. These mobility agents periodically advertise their presence via an *Agent Advertisement* message (an extension added to the *ICMP Router Advertisement*). A *MN* may optionally solicit an *Agent Advertisement* message from any locally attached mobility agent through an *Agent Solicitation* message. Upon receiving this *Agent Advertisement* the *MN* determines whether it is currently connected to its *home network* or to a *foreign network*, and also detects when it has moved from one network to another. In addition, this enables it to find the *care-of-address* of the advertised *FA*.
- **Registration:** When a *MN* is away from home, it uses a registration procedure to keep its *HA* informed about its current location. To do so, it contacts the closest *FA* and sends a *registration request* message directly (if it is used a *co-located care-of-address*) or via this *FA* (if it is used a *FA-care-of-address*) to its *HA*. When the *HA* gets the request it knows where the *MN* is located at present and to which *care-of-address* it should relay the packets destined for the *MN*. Then, it responds by a *registration reply* message to grant or deny this mobility service. After successful registration, the *HA* is responsible for intercepting packets arriving for the *MN* on its *home network*, encapsulating and sending these packets through a tunnel to the actual mobile node's *FA*.

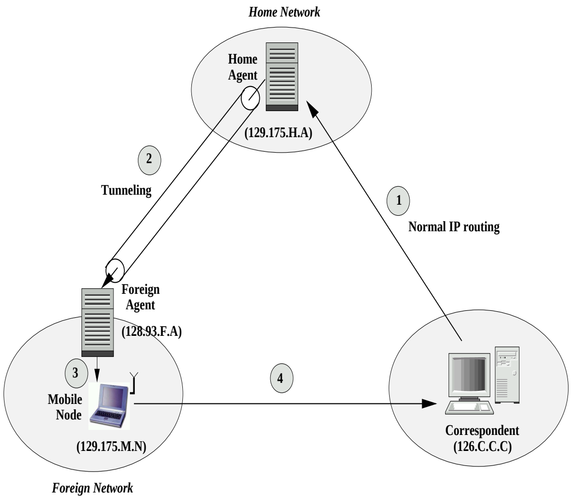


Fig. 1. Operation of Mobile-IPv4.

B. Micro-mobility approaches for wireless access networks

With the Mobile-IP paradigm, micro-mobility means the mobile node moves inside the same access network without changing the register mobility binding (i.e. association of a mobile node's *home address* with a *care-of-address*) on the *home* *network*. On the other hand, macro-mobility means movement between different networks, and requires registering the new *care-of-address* acquired in the visited network.

Mobile-IP lacks smooth, fast and transparent handoffs required for future *full-IP* wireless networks. Indeed, frequent handoffs inside a wireless access network tend to generate a huge amount of signaling overhead due to the required control messages between a mobile node and *home network*. Additionally, the need to acquire a new *care-of-address* and tunnel establishment results in latency and disruption to data traffic (e.g. packet loss, jitter, etc.). Also, if a large number of mobile nodes quickly migrate between *foreign networks*, Mobile-IP does not provide a scalable solution to support fast and seamless handoff control [2], [8].

Several proposals [2], [3], [9], [10] have been made to deal with this micro-mobility problem in wireless access networks. These protocols follow the approach of hierarchical mobility support in combination with Mobile-IP. They provide mobility in a well defined area, e.g., an access network, and allow mobility between different access networks to be handled by Mobile-IP as a macro-mobility solution. Two examples of protocols, Cellular-IP and HAWAII, are presented in the following.

1) Cellular IP: The Cellular-IP [2] proposal combines the smooth mobility support of cellular telephony systems with the flexibility, robustness and scalability of IP-based networks. Figure 2 illustrates an example of a Cellular-IP network. A Cellular-IP network is connected to the Internet via a gateway router. This router serves as the *HA* and *FA* within the wireless access network. A Cellular-IP network contains an arbitrary number of nodes, and Base Stations (BSs) which have a wireless interface. The mobile nodes are identified by their *home address*, and for macro-mobility purposes, they utilize the address of the gateway as their *care-of-address*.

Cellular-IP routing is based on routes established and updated by the mobile node during its connection to the network. Each Cellular-IP node maintains a *routing cache* that allows it to forward packets from the gateway to the mobile node and from the mobile node to the gateway. Downlink, a *beacon* packet is periodically sent by the gateway that floods the access network. This mechanism allows each BS to record the interface from which the *beacon* is received and uses it to forward packets towards the gateway. Uplink, in order to minimize control traffic, hop-by-hop transmission of regular data packets from the mobile node to the gateway enables nodes on the path to update their *routing cache*. On the other hand, the routes can be established and refreshed by the mobile node's transmission of *route-update* packets when it connects to the network and each time it performs a handoff.

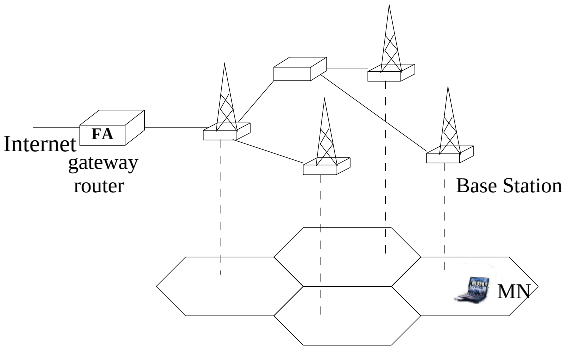


Fig. 2. Cellular-IP wireless access network model.

The handoff is managed by two different mechanisms: hard handoff and semi-soft handoff. The hard handoff provides no guarantees in terms of packet loss. In semi-soft handoff, a mobile node listening to *beacons* transmitted by two BSs can establish new *routing cache* mappings before the actual handoff takes place. In this way, handoff latency is reduced. Moreover, Cellular-IP presents a support for passive connectivity with a classical paging mechanism: some BSs maintain *paging caches* that are refreshed at regular intervals by *paging-update* packets.

2) HAWAII: Handoff-Aware Wireless Access Internet Infrastructure (HAWAII) [3] is a domain-based approach for managing mobility. As in Cellular-IP, HAWAII is responsible for intra-domain mobility limited to an administrative domain of an access network while inter-domain mobility is handled by Mobile-IP. In HAWAII a hierarchy based on domains is used as depicted in Figure 3. The gateway into each domain is called a *Domain Root Router* (*DRR*). Furthermore a HAWAII domain comprises several routers and Base Stations (BSs) running the HAWAII protocol, as well as mobile nodes. Each mobile node is assumed to have a *home domain*, and when entering a foreign HAWAII domain it obtains a *co-located care-of-address* from the *foreign domain*.

A mobile node in the HAWAII domain exchanges only Mobile-IP control messages with the BSs,

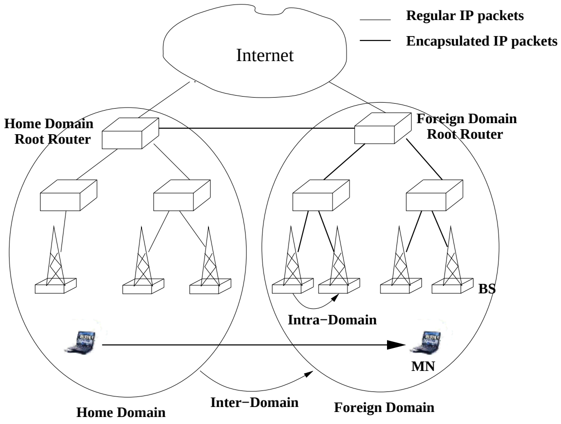


Fig. 3. HAWAII Hierarchy using domains.

while the path setup within a HAWAII domain is realized with three types of messages: *power-up*, *update* and *refresh*. BSs periodically send *Agent Advertisement* messages. Whenever the host detects a change of base station it issues a Mobile-IP *registration request* to the new BS. This registration is used to trigger a HAWAII path setup scheme inside the domain. The BS then sends a HAWAII path setup *power-up* or *update* message to the *DRR* on a hop-by-hop basis. This has the effect of establishing a route for that mobile node to the *DRR* and any intermediate routers on the path towards the mobile node. In addition, aggregate hop-by-hop *refresh* messages are periodically sent to maintain the routes. Moreover, the choice of using a *co-located care-of-address* and maintaining the mobile node address unchanged within a domain simplifies QoS per flow management (e.g. RSVP).

C. *MANET Capabilities*

Solutions based on a cellular approach require the deployment of an infrastructure. An alternative solution consists of using a MANET network that works without any pre-existing infrastructure deployment. In fact, a MANET network [11] is a collection of mobile nodes that communicate using a wireless medium, forming an autonomous network. There is no centralized access point or pre-existing infrastructure. Such networks have dynamic, random, sometimes rapidly changing topologies, limited bandwidth, variable throughput links, and limited power (e.g. battery operated devices). When a node needs to communicate with another node, it uses either a direct wireless link or a multi-hop route to reach the destination. This means that all the nodes must incorporate routing capability to ensure that packets are delivered to the designated destination.

Different routing protocols are proposed in the MANET working group of the IETF [11]. They address the problem of unicast routing, while taking into account the features of wireless, multi-hop, mobile ad-hoc networks. Such protocols can be divided into three categories: proactive, reactive and hybrid. With reactive protocols, a node discovers routes on-demand and maintains only active routes. Thus, a route is discovered whenever a source node needs to communicate with a destination node for which a route is not available. This discovery is based on pure flooding [12] in the network. Examples of reactive protocols include AODV [13] and DSR [14]. With proactive protocols, each node continuously maintains the routes to all other nodes in the network by the periodic exchange of control messages. When a node needs to send a packet to any other node in the network, the route is immediately available. Examples of proactive protocols include DSDV [15] (an adaptation of Routing Information Protocol [16]), OLSR [17] (an optimization of the Link State algorithm OSPF [18]) and TBRPF [19]. Hybrid protocols, such as ZRP [20], use a mixed approach of proactive and reactive techniques.

Some proposals aim to facilitate connectivity of stub ad-hoc networks to the Internet and routing interoperability based on Mobile-IP is achieved. The authors in [21] show how to integrate an ad-hoc routing protocol with Mobile-IP. Routing within the ad-hoc network is achieved by *routed*, a modified version of the RIP daemon, on each mobile node within the network. The *Foreign Agent* participates in the ad-hoc routing. The mobile nodes within range of the *Foreign Agent* cooperate to forward *Agent Advertisements* or Mobile-IP messages to other nodes outside its range. Each mobile node uses the *Foreign Agent* as its default router. A route manager is used to coordinate the manipulation of the IP routing table.

A proposal to integrate a reactive protocol, DSR [14] with the Internet routing and Mobile-IP is presented in [22]. An addressing architecture is proposed, where all the nodes in an ad-hoc network are assigned *home addresses* from a single IP subnet. Nodes within range of the *Foreign Agent* serve as gateways between the ad-hoc network and the Internet. DSR is utilized for routing within the ad-hoc network, while standard IP routing applies to the wired network. The gateway participates in both DSR routing and Internet routing. In the integration of Mobile-IP and DSR, *Foreign Agents* (implemented on gateways) are responsible for forwarding packets between the ad-hoc network and the Internet.

The most recent work on the connectivity between ad-hoc and wired networks is Mobile-IP for Mobile Ad-Hoc Networks (MIPMANET) [23]. In MIPMANET, nodes in an ad-hoc network that need Internet access register with the *Foreign Agent* and use their *home address* for all communications. Mobile nodes tunnel all packets to their *Foreign Agent*, which decapsulates the packets and forwards them to the destination. This tunneling between mobile nodes and the *Foreign Agent* is used to separate the ad-hoc network from Mobile-IP. On the other hand, the packets from hosts on the Internet addressed to mobile nodes are delivered by ordinary Mobile-IP mechanisms to the *Foreign Agent*. Then, the AODV protocol is used to deliver packets to the mobile nodes in the ad-hoc network. Nodes that do not require Internet access have no knowledge of external routes. Moreover, MIPMANET utilizes a mechanism called "MIPMANET Cell Switching" (MMCS), that allows a mobile node to determine when it should register with another *Foreign Agent*. This solution allows the coexistence of heterogeneous addresses in the ad-hoc network, i.e. each node can use its *home address* for communication inside the ad-hoc network.

III. PROPOSED ARCHITECTURE FOR MOBILITY MANAGEMENT

As mentioned above, although there have been a number of proposals [21], [22], [23] for interconnecting an ad-hoc network with the fixed Internet, none of them utilizes any of the emerging micro-mobility solutions. They simply extend Mobile-IP to serve the nodes further than a one-hop distance from the gateway. These schemes have the disadvantage of concentrating traffic on the ad-hoc nodes one-hop away from the gateway. The architecture that we propose for interconnecting ad-hoc networks to the fixed Internet with a macro/micro-mobility management follows the approach of hierarchical mobility support, where Mobile-IP protocol is used to support macro-mobility (inter-domain) and the OLSR protocol is used to support micro-mobility (intra-domain). In this hierarchical architecture, we introduce an intermediate level between the gateway and an ad-hoc network. This level consists of Base Stations which allow more flexibility in mobility management and higher bandwidth between the gateway and the ad-hoc network.

A. *Hierarchical mobility support*

The proposed architecture is depicted in Figure 4. An OLSR-IP access network constitutes an IP subnetwork and it is interconnected to the Internet via an *OLSR Gateway* (*OLSR-GW*). The motion of a mobile node inside an OLSR-IP access network is managed by the OLSR protocol. Mobility between different OLSR-IP access networks or IP subnetworks is managed by Mobile-IP.

An OLSR-IP access network consists of: (i) a random topology of ad-hoc mobile nodes and (ii) a fixed hierarchical structure connecting *OLSR-GW* and *OLSR Base Stations* (*OLSR-BS*) by wired links. For nodes, like Base Stations, having multiple interfaces (i.e. a wired one and a wireless one), the OLSR protocol is implemented on both interfaces. A node inside the OLSR-IP access network uses its IP *home address* to establish and maintain routes.

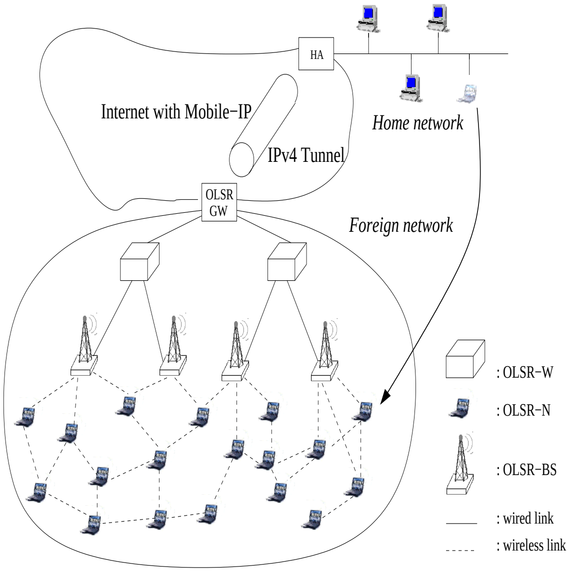


Fig. 4. An OLSR-IP Access Network Interconnected to a Mobile-IP enabled Internet.

The architecture is composed of several functional entities:

- *Home Agent* (*HA*): a router in the mobile node's home network.
- *OLSR-GW*: a router allowing an OLSR-IP access network to be connected to the Internet and implementing the role of a *Foreign Agent* in order to manage the visitor mobile nodes. It can also implement the role of a *Home Agent* if the OLSR-IP access network is the *home network*. Furthermore, *OLSR-GW* implements the OLSR protocol to contribute to micro-mobility management.
- *OLSR-BS*: a node having two interfaces: wireless and wired. In order to ensure routing between the two parts of the architecture, it implements the OLSR protocol on both interfaces.
- *OLSR-N*: a mobile node in the ad-hoc network having only a wireless interface. It implements

the OLSR protocol, which makes it possible to build its OLSR routing table to reach and maintain connectivity with all nodes inside the OLSR-IP access network. In addition, it uses the optimal default route via the *OLSR-GW* to reach a host outside the OLSR-IP access network. If this node can change its OLSR-IP access network, it implements Mobile-IP's registration procedures.
- *OLSR-W*: a wired node that serves as a traffic controller or supports micro-mobility management functions (i.e. it implements OLSR).

The operation of this architecture is as follows. When an *OLSR-N* is away from its *home network*, the *Home Agent* intercepts packets addressed to it and sends these packets through a tunnel up to the current mobile node's attachment OLSR-IP access network. The *OLSR-N* would previously have registered its *OLSR-GW care-of-address* with its *Home Agent*. The *Foreign Agent* decapsulates packets and forwards them to the visited *OLSR-N* according to the OLSR routing table. The motion of the *OLSR-N* inside the visited OLSR-IP access network is managed locally by the OLSR protocol and does not require informing or changing registered location information at the level of the *Home Agent*. Briefly, the *Home Agent* does not have to know the exact location of the *OLSR-N*, but in which OLSR-IP access network the *OLSR-N* is located. Micro-mobility inside the visited network is dealt with locally by updating the routing tables of each node in the network, according to neighborhood and topology changes.

The advantages of this architecture are the following:

- Increased bandwidth between *OLSR-GW* and the mobile nodes: due to having Base Stations connected by wired links to the *OLSR-GW*.
- Reduction in the amount of global location updates by Mobile-IP: avoiding Mobile-IP registration procedures when executing handoffs between the Base Stations. This is because the Base Stations are not directly connected to the Internet.
- Shared traffic load between Base Stations: the traffic to and from the outside of the OLSR-IP access network is distributed over all the Base Stations of the local network.
- Guaranteed use of the shortest route between *OLSR-GW* and a mobile node: because the OLSR protocol maintains the shortest routes regarding the number of hops.
- Micro-mobility is handled in a transparent manner for the *Home Agent*: when a mobile node moves inside the OLSR-IP access network, there is an automatic change of the Base Station that receives the packets from the *OLSR-GW* destined to a mobile node, without location updates on the *home network*. We can refer to this local change as a handoff at IP level (IP-handoff) between Base stations' cells.
- Preferential use of wired architecture to forward packets inside the access network. The wired paths are less vulnerable than the wireless ones, consequently the Base Stations can reduce the number of wireless hops and therefore the cost of the route.
- Support of nodes out of range of Base Stations: a mobile node can move out of the coverage area of a Base Station, and still be reached using ad-hoc OLSR routing.

B. Optimized Link State Routing Protocol (OLSR)

OLSR [17], [24] is a proactive routing protocol, providing the advantage of having routes immediately available in each node for all destinations in the network. It is an optimization of a pure Link State routing protocol. This optimization is based on the concept of *multipoint relays* (*MPRs*) [25]. First, using *multipoint relays* reduces the size of the control messages: rather than declaring all links, a node declares only the set of links with its neighbors that are its "*multipoint relays*". The use of *multipoint relays* also minimizes flooding of control traffic. Indeed only the *MPRs* of a node forward control messages received from this node. This technique significantly reduces the number of retransmissions of broadcast control messages [26]. OLSR is characterized by two types of control messages: neighborhood and topology messages, called respectively *Hello* messages and *Topology Control* (*TC*) messages. Indeed OLSR provides two main functionalities: Neighbor Discovery and Topology Dissemination.

1) Neighbor Discovery: Each node must detect the neighbor nodes with which it has a direct link. Due to the uncertainties in radio propagation, a link between neighboring nodes may enable the transmission of data in either one or both directions over the link. For this, each node periodically broadcasts *Hello* messages, containing the list of neighbors known to the node and their link status. The link status can be either *symmetric* (if communication is possible in both directions), *asymmetric* (if communication is only possible in one direction), *mpr* (if the link is symmetric and the sender node of the *Hello* message has selected this node as a *multipoint relay*), or *lost* (if the link has been lost). The *Hello* messages are received by all one-hop neighbors, but are not forwarded.

Thus, *Hello* messages enable each node to discover its one-hop neighbors, as well as it two-hop neighbors (the neighbors of its neighbors). Each node m of the network independently selects its *multipoint relays* among its one-hop neighbors to cover, in terms of radio range, all its two-hop neighbors. Figure 5 shows the *MPRs* selection by node m. One possible algorithm for selecting these *MPRs* is described in [25]. Each node m maintains the set of its "*multipoint relay selectors*" (*MPR selectors*). This set contains the nodes which have selected m as a *multipoint relay*. Node m forwards at most once a broadcast message and only if this message has been received from one of its *MPR selectors*.

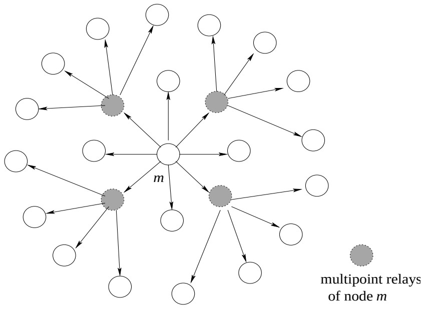


Fig. 5. Multipoint relays of node m.

2) Topology Dissemination: Each node of the network maintains topological information about the network obtained by means of *TC* messages. Each node m selected as a *multipoint relay*, broadcasts a *TC* message advertising its *MPR selectors*. The *TC* messages are flooded to all nodes in the network and take advantage of *MPRs* to reduce the number of retransmissions.

The neighbor information and the topology information are refreshed periodically, and they enable each node to compute the routes to all known destinations. These routes are computed with Dijkstra's shortest path algorithm [12]. Hence, they are optimal as concerns the number of hops. Moreover, for any route, any intermediate node on this route is a *multipoint relay* of the next node. The routing table is computed whenever there is a change in neighborhood information or in topology information.

IV. INTEGRATION OF MOBILE-IP AND OLSR

To achieve integration of Mobile-IP and OLSR we propose the architecture depicted in Figure 6. The ad-hoc routing protocol is implemented by an *OLSRd* daemon, while Mobile-IP is implemented by three specific daemons: *HAd*, *FAd* and *MNd*, corresponding respectively to *Home Agent*, *Foreign Agent* and *Mobile Node* functionalities. Each node in the ad-hoc network needing mobility services, such as a visiting *OLSR-N*, runs the two daemons *OLSRd* and *MNd*. An *OLSR-N* that never changes its OLSR-IP access network only implements the *OLSRd* daemon. The *OLSR-GW* has two daemons *OLSRd* and *FAd*; it can also implement *HAd* if it plays the role of the *Home Agent*. To ensure transparency, the two daemons *OLSRd* and *MIPd* (i.e. *HAd*, *FAd* or *MNd*) run independently without requiring any change to their behavior.

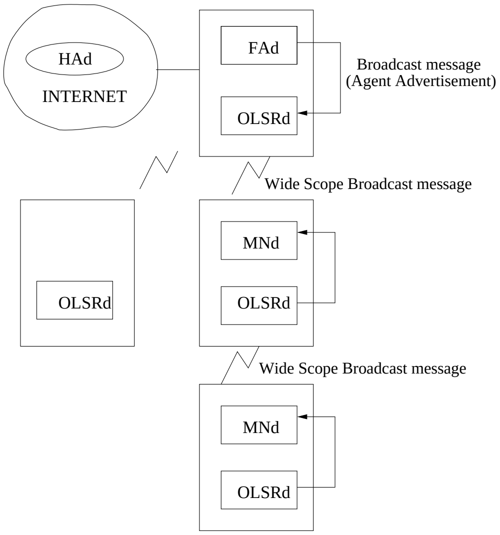


Fig. 6. Integration model.

The *OLSR-GW* periodically broadcasts *Agent Advertisement* messages targeting the limited broadcast address "255.255.255.255". So, these Advertisements would only be received by nodes within the transmission range of *GW-OLSR* (i.e. one-hop neighbors). In order to enable all nodes in the access network to receive advertisements we propose *MPR*- based flooding. In *MPR*-based flooding, a node forwards a broadcast packet at most once, and only if this packet has been received from one of its *MPR selectors*. The solution we propose works as follows: the *Agent Advertisement* of the *OLSR-GW* is captured by *OLSRd* before leaving the node. It is then encapsulated in a new message called a "*Wide Scope Broadcast message*" (*WSB*). Hence, this broadcast packet reaches all the nodes in the OLSR-IP access network and takes advantage of *MPRs*, which significantly reduces the number of retransmissions, in contrast to a purely classical flooding. When an *OLSRd* receives a *WSB* message, it decapsulates the packet and sends the original advertisement to the *MNd* (if present) on the local interface, as if it had been sent directly by a *Foreign Agent*. This is illustrated by Figure 6. Furthermore, to forward the WSB message at most once, *OLSRd* maintains a “Duplicate table”.

Moreover, as *MNd* thinks it is one-hop away from *FAd*, it is necessary to prevent *MNd* from changing routes established by the *OLSRd* within the ad-hoc network. Inside an OLSR-IP access network, the mobility management contains two procedures: an attachment procedure and a micro-mobility handling procedure, that are described below.

A. Attachment procedure

When a mobile node m powers up or moves to an IP-OLSR access network, it triggers the attachment procedure in order to have connectivity with its correspondents. To do so, first it must establish connection with the IP-OLSR access network, and then perform registration with the *home network*. Figure 7 illustrates the messages exchange during m’s attachment.

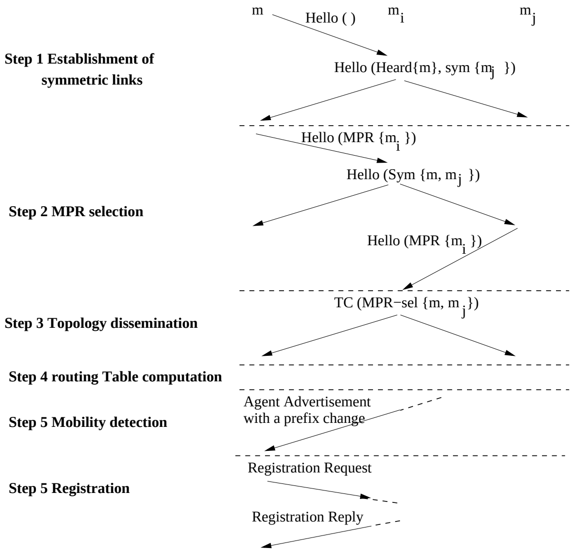


Fig. 7. Exemple of m’s attachment.

Briefly, m’s attachment consists of the following steps :

1) **Establishment of symmetric links:**
   - m starts by sending an empty *Hello* message announcing its IP *home address* in order to establish links with its neighbors.
   - a neighbor node receiving an empty *Hello* from node m, replies with a *Hello* containing the address of m. This allows m to validate the link in both directions.
2) **Multipoint relay selection:** among the neighbors’ replies, m selects its *multipoint relays* (i.e. neighbors with a “*symmetric*” link, that cover all two-hop neighbors). These *MPRs* are declared in the next *Hello* (i.e, the *Hello* message contains the IP addresses of those neighbors with the link type “*mpr*”).
3) **Topology dissemination:** the declared nodes will then broadcast *TC* messages to all the nodes in the network declaring that they are *MPRs* of m and thus m can be reached through them (i.e. a *MPR* of m is the last hop in a route to m).
4) **Routing table construction:** all the nodes in the network (including *OLSR-GW*) that receive *TC* messages, have a global vision of the network topology, and thus calculate routes to reach m.
5) **Mobility detection:**
   - m may send Mobile-IP’s *Agent Solicitation* message to request a Mobile-IP’s *Agent Advertisement* message.
   - m receives either an *Agent Advertisement* from *OLSR-GW* in response to its *Agent Solicitation* or a periodic *Agent Advertisement*.
   - therefore, m can detect if it has moved away from its *home network* (if the network prefix of m’s home IP address differs from the prefix network of *OLSR-GW*’s IP address) or has moved to another access network (if the network prefix of the advertised *care-of-address* differs from the current network prefix of the registered *OLSR-GW*).
6) **Registration:**
   - if m is away from its *home network* or has moved to another access network, it sends a Mobile-IP’s *registration request* message to its *Home Agent* via the *OLSR-GW*.
   - m receives Mobile-IP’s *registration reply* message from its *Home Agent*, via the *OLSR-GW*.

Once m has been registered, it is attached to the OLSR-IP access network and can send and receive data packets to/from its correspondent nodes in the Internet.

B. Micro-mobility handling procedure

As mentioned above, inside the OLSR-IP access network, mobility is naturally handled by the OLSR protocol. It is implemented by all the nodes within the access network. The operation scheme as executed by a node while moving within the access network can be summed up as follows:

- The node periodically broadcasts *Hello* Messages to its one-hop neighborhood.
- It selects its *multipoint relays* whenever its one-hop or two-hop neighborhood changes.

- It periodically broadcasts *TC* messages over the whole network, to announce the set of its *multipoint relays selectors*.
- It establishes and keeps topological information updated, which gives for each node in the network its *multipoint relays*.
- It constructs the routing table from the neighborhood and topology information: routes to all nodes in the network.

V. DESCRIPTION OF THE IMPLEMENTATION

A. *Choice of the implementation plateform*

Several implementations of Mobile-IP have been developed: e.g. [27], [28], [29], [30]. The Linux Mobile code of Helsinki University of Technology (HUT) Dynamics project [28] is used as a basis for our implementation. Dynamics - HUT Mobile IP is a scalable, dynamic and hierarchical Open Source Mobile IPv4 system for the Linux operating system. The *FAd*, *HAd* and *MNd* run on a priviliged UDP port: 434. The *registration requests* and *replies* are received and sent on this port. On the other hand, the ICMP *Agent Advertisement* and *Solicitation* are periodically sent as link layer broadcast messages. These messages, only received by the one-hop neighbors, are not adapted to ad-hoc networking, because the mobility agents (*FAd*, *HAd*) and a visiting node might not necessarily have link layer connectivity. Also, we have implemented the OLSR version 7 [17]. The code of the OLSR daemon (*OLSRd*) is enhanced to support the *WSB* format message and related processing. The *OLSRd* runs on a priviliged UDP port: 698.

B. *Communication between OLSR and Mobile IP daemons*

To resolve the broadcasting problem while providing transparency between Mobile-IP and *OLSRd* daemons described in section IV, we have developed a tool called “ifaceFilter” that makes possible to filter all packets sent by *MIPd*. ifaceFilter uses a local tunnel device called Universal TUN/TAP [31] to create a virtual interface (e.g. tap0, tap1,etc.) that operates above a physical (ethernet/wireless) interface (e.g., eth1). TUN/TAP was designed as a low level kernel support that provides user space programs with packet reception and transmission through the /dev/net/tun device. As described in Figure 8, we run *MIPd* (*MNd*, *FAd* and *HAd*) on the virtual interface.

All the unicast IP packets that are sent to the virtual interface are forwarded to the physical interface and vice-versa. Only the broadcast IP packets that have a destination address “255.255.255.255” (for example, *Agent Advertisements*) and come from *MIPd*, are encapsulated (using UDP packets) into OLSR version 7 format messages with message type set to “WSB”. They are then sent to the loopback IP address, on the OLSR port.

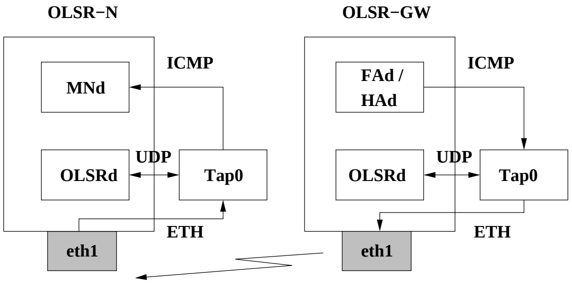


Fig. 8. Linux implementation of Agent Advertisement Broadcast in Ad-hoc network.

The messages are forwarded by *OLSRd* to all nodes in the ad-hoc network using MPR-based flooding. Thus, upon receiving a WSB message, the *OLSRd* checks if there is an internal *MNd* running on the UDP port 434. If so, it decapsulates the OLSR header and delivers an UDP packet to ifaceFilter. The ifaceFilter takes charge of delivering the original IP packet with an ethernet header to the internal *MNd*. Therefore *MIPd* running on this virtual interface will receive the original IP packets (with no UDP header) as they come directly from another daemon attached to the same link. Moreover, if the sender of the message is a *MPR* selector of this node and if it is the first receipt, then *OLSRd* forwards this OLSR message.

C. *Updating the routing table*

We have adapted the mobile-IP source code to an ad-hoc network environment, by introducing some changes in the route manipulation process of the *MIPd*. The *FAd* (respectively, the *HAd*) is not allowed to add an entry in the routing table for a visiting *mobile node* (respectively, a *mobile node* inside the OLSR-IP access network). Only *OLSRd* is allowed to manipulate the routing table for nodes inside the OLSR-IP access network. The *FAd* and the *HAd* only take charge of establishing the Mobile IP tunnel for *mobile nodes* moving from the *home network* to the *foreign network*. Also, the *MNd* cannot have a direct link to the *FAd* (respectively, the *HAd*) if it is several hops away from the *FAd* (respectively, the *HAd*), and so doesn’t use the *FAd* (respectively, the *HAd*) as the one-hop default router.

An *OLSR-GW* advertises the associated hosts and subnetworks it is connected to by means of “*Host and Network Association*” (*HNA*) messages. When a *OLSR node* receives a *HNA* message whose originator is an *OLSR-GW*, it can establish the default route via this *OLSR-GW* to reach the advertised destinations.

VI. TESTS AND MEASUREMENTS

The goal of the experiments is to evaluate the impact of mobility on the available throughput. We consider the following scenario: a mobile node successively performs domain changes by visiting different OLSR-IP access networks. Mobile-IP manages these domain changes and OLSR manages multi-hop routing within an OLSR-IP access network. For the sake of simplicity, we refer to this scenario as Mobile-IP handoffs.

A. Testbed setup

The experimental results are based on measurements taken from the Mobile-IP handoff testbed illustrated in Figure 9. The Mobile-IP handoff testbed consists of 3 OLSR-IP access networks interconnected by a router:

- ***home network***: comprises (i) the OLSR-GW0 (193.51.193.1) that serves as a *Home Agent* and a correspondent node; and (ii) the mobile node, manet2 (193.51.193.2).
- ***foreign network1***: comprises (i) the OLSR-GW1 (172.27.0.1) that serves as a *Foreign Agent1* and (ii) a mobile node, manet1 (172.27.0.2) that serves as a relay between the OLSR-GW1 and manet2.
- ***foreign network 2***: comprises (i) the OLSR-GW2 (193.51.192.46) that serves as a *Foreign Agent2* and (ii) a mobile node, manet3 (193.51.192.4) that serves as a relay between the OLSR-GW2 and manet2.

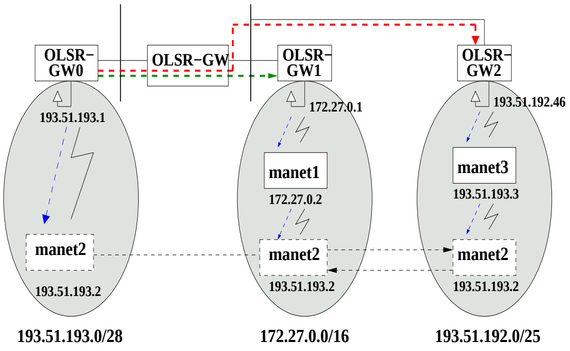


Fig. 9. Mobile-IP Handoff Testbed.

The wireless links are configured in ad-hoc mode. In the testbed the OLSR-GW0, OLSR-GW1,OLSR-GW2, manet1 and manet3 have statically assigned frequencies while manet2 can dynamically change frequency to perform IP-based handoffs between *foreign network1* and *foreign network2*. When manet2 is in one of the *foreign networks*, it is never in the coverage area of the OLSR-GW and an intermediate node (for instance, manet1 or manet3) ensures the communication between manet2 and the OLSR-GW.

B. Parameters and mobility model

The parameters of our experiments are summarized in table I. During the experiments UDP traffic is transmitted from a correspondent node (OLSR-GW0) to manet2. Throughout the Mobile-IP handoff experiments manet2 was moved between *foreign network1* and *foreign network2* as shown in Figure 9. manet2 spends the same amount of time in each *foreign network*.

Table I. Experiment parameters.

Input parameter	Values
Traffic model parameters	
Traffic type	UDP
Packet size[Byte]	1400
Packet burst size	1
Inter-arrival time [msec]	20
Socket buffer size [Byte]	65535
Direction of data flow	Downlink
Link parameters	
Wireless link (IEEE802.11)	11Mbps
WAN interconnection (FA, HA, MN)	ad-hoc mode
Mobile-IP specific parameters	
Advertisement frequency[N/s]	1 AA/5s
Handoff initiation policies	3 AA
Tunneling type	Triangular Routing
FA packet encapsulation	Enabled
OLSR specific parameters	
HELLO_INTERVAL	2s
TC_INTERVAL	5s
HNA_INTERVAL	5s
NEIGHBOR_HOLD_TIME	6s
TOP_HOLD_TIME	15s
Measurement specific parameters	
Test length (Δ)	960s
Number of iterations	15

C. Experimental results

We compute the impact of handoffs on the available throughput. We first evaluate the available throughput without Mobile-IP handoffs Th_{no_H}, then we evaluate the available throughput with

Mobile-IP handoffs Th_H. The number of Mobile-IP handoffs ranges from 3 to 31. The available throughput rate is equal to $\frac{Th_H}{Th_{no_H}}$.

The measurements results are plotted in Figure 10. The graph depicts the available throughput rate versus the number of Mobile-IP handoffs.

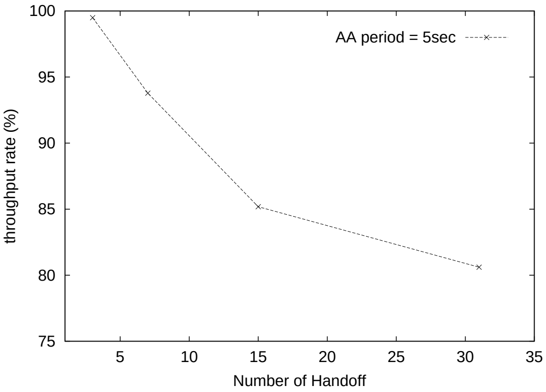


Fig. 10. Throughput rate versus Mobile-IP handoffs.

The curve was obtained with a sending period of Agent Advertisement of 5 seconds. Each point on the graph was obtained by averaging 15 throughput measurements. As the curve shows, when the number of handoffs increases, the throughput rate decreases. As long as the number of handoffs does not exceed 31, the throughput Th_H is higher than 80% of the throughput without handoffs Th_{no_H}. Notice that, in this testbed the Round Trip Time (RTT) is less than 20 ms. This value does not reflect the real Internet configuration, where the RTT is about 5 seconds. In the latter case, we would obtain smaller throughputs.

VII. CONCLUSION

4G wireless networks, in addition to incorporating all the services currently provided by 3G wireless networks, will integrate *full-IP* based core and access networks. In this way, universal mobility management will be possible through heterogeneous wireless and wired networks on the Internet. In this paper, we have discussed some limitations of existing mobility solutions on the Internet (e.g. Mobile-IP). We have proposed and implemented an integrated architecture that manages this universal mobility both for large scale macro-mobility and local scale micro-mobility. This architecture extends a wireless access network's micro-mobility management to an ad-hoc access network and connects an ad-hoc network to the Internet. It is based on a hierarchy of OLSR-IP access networks: the Mobile-IP standard is used for macro-mobility management between access networks and the OLSR protocol is used for micro-mobility management within the access network. We have shown how to integrate Mobile-IP with the OLSR protocol in this architecture. The measurements we have performed show that less than 31 handoffs do not decrease the available throughput lower than 80%.

On the other hand, work [32] has been carried out on the new OLSR extension, denoted Fast-OLSR. The Fast-OLSR proposes integrating fast mobility routing in the OLSR protocol in order to account for fast micro-mobility within an OLSR-IP access network. While the OLSR protocol currently supports best effort traffic only, in further work we will study how to integrate Quality of Service (e.g. in terms of bandwidth) to mobile nodes, using an admission control mechanism.

REFERENCES

[1] C. Perkins, "IP Mobility Support for IPv4," RFC 3220, IETF, http://www.ietf.org, January 2002.
[2] A.T. Campell, J. Gomez, A. Valko, "An overview of Cellular IP," *IEEE Wireless communications and Networking Conference*, vol. 2, pp. 606–610, September 1999, New Orleans.
[3] R. Ramjee, T.L. Porta, S. Thuel, K. Varadhan, S.Y. Wang, "HAWAII: a Domain-based Approach for supporting Mobility in Wide-area Wireless Networks," *IEEE international Conference on Network Protocols*, November 1999, Toronto.
[4] C. Perkins, *Ad Hoc Networking*. Addison Wesley, 2000.
[5] C.K. Toh, *Ad Hoc Mobile Wireless Networks protocols and Systems*. Prentice Hall, 2002.
[6] IP Routing for Wireless/Mobile Hosts (mobileip), *mobileip-charter*. http://www.ietf.org/html.charters/mobileip-charter.html, 2002.
[7] R. Droms, "Dynamic Host Configuration Protocol," RFC 2131, IETF, http://www.ietf.org, March 1997.
[8] R. Caceres, V.N. Padmanabhan, "Fast and Scalable Handoffs for Wireless Internetworks," *ACM International Conference on Mobile Computing and Networking*, pp. 56–66, November 1996, New York, USA.
[9] S. Das, A. Misra, P. Agrawal, "TeleMIP: Telecommunication Enhanced Mobile IP Architecture for Fast Intra-Domain Mobility," *IEEE Personal Communications*, vol. 7, pp. 50–58, August 2000.
[10] A. O'Neill, G. Tsirtsis, S.Corson, "Edge Mobility Architecture," draft-oneill-ema-01.txt, IETF, March 2000.
[11] Mobile Ad-hoc Networks (MANET), *manet-charter*. http://www.ietf.org/html.charters/manet-charter.html, 2002.
[12] A.S. Tanenbaum, *Computer Networks*. Prentice Hall, 1996.
[13] C. Perkins, E. Royer, S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," draft-ietf-manet-aodv-08.txt, IETF, March 2001.
[14] J. Broch, D. Johnson, D. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," draft-ietf-manet-dsr-01.txt, IETF, December 1998.
[15] C. Perkins, P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," in *ACM SIGCOMM'94*, August 1994, London, UK.
[16] J. Malkin, "Routing Information Protocol (RIP) V2," RFC 1388, IETF, January 1993.
[17] T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot, "Optimized link state routing protocol," draft-ietf-manet-olsr-07.txt, IETF, July 2002.

[18] J. Moy, “Open Shortest Path First (OSPF) V2,” RFC 2328, IETF, January 1998.

[19] R.G. Ogier, F.L. Templin, B. Bellur, M.G. Lewis, “Topology broadcast based on reverse-path forwarding (TBRPF),” draft-ietf-manet-tbrpf-05.txt, IETF, March 2002.

[20] Z.J. Haas, M.R. Pearlman, P. Samar, “The Zone Routing Protocol (ZRP) for Ad Hoc Networks,” draft-ietf-manet-zone-zrp-02.txt, IETF, July 2000.

[21] C. Perkins, H.Lei, “Ad hoc Networking with Mobile IP,” *Second European Personal Mobile Communication Conference*, pp. 197–202, October 1997.

[22] J. Broch, D.A. Maltz, D.B. Johnson, “Supporting Hieararchy and Heterogenous Interfaces in Multi-hop Wireless Ad Hoc Networks,” *Workshop on Mobile Computing, IEEE International Symposium on Parallel Architectures, algorithms and Networks*, pp. 75–85, June 1999, Australia.

[23] U. Jonsson, F. Alriksson, T. Larsson, P. Johansson, G.Q. Maguire, “MIPMANET - Mobile IP for Mobile Ad Hoc Networks,” *IEEE/ACM Workshop on Mobile and Ad hoc Networking and Computing*, pp. 75–85, August 2000, Boston MA USA.

[24] P. Jacquet, P. Muhletaler, A. Qayyum, A. Laouiti, T. Clausen, L. Viennot, “Optimized Link State Routing Protocol,” in *IEEE INMIC*, December 2001, Pakistan.

[25] A. Qayyum, L. Viennot, A. Laouiti, “Multipoint Relaying: An Efficient Technique for flooding in Mobile Wireless Networks,” Tech. Rep. 3898, INRIA, http://www.inria.fr, February 2000.

[26] A. Qayyum, A. Laouiti, L. Viennot, “Multipoint relaying technique for flooding broadcast messages in mobile wireless networks,” in *HICSS: Hawaii International Conference On System Sciences*, January 2002, Hawai, USA.

[27] MosquitoNet Project, “Mobile IP ressources,” tech. rep., http://www.cs.hut.fi/Research/Dynamics/mailinglist.html, 1998.

[28] Helsinki University of Technology (HUT), “Dynamics-Hut Mobile IP,” tech. rep., http://www.cs.hut.fi/Research/Dynamics/mailinglist.html, 1999.

[29] SUN Microsystems, “Mobile IP for Solaris/Linux,” tech. rep., http://playground.sun.com/mobile-ip/sunlabs/, 1999.

[30] Monarch Project, “Mobile IPv4 for BSD-based Unix systems,” tech. rep., http://www.monarch.cs.rice.edu/mobileipv4.html, 1998.

[31] Universal TUN/TAP driver, *Virtual Point-to-point (TUN) and Ethernet (TAP) devices*. http://vtun.sourceforge.net/tun/, 2002.

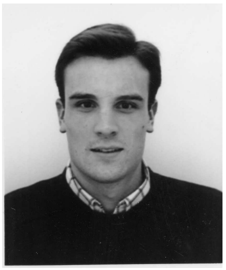
[32] M. Benzaid, P.Minet, K.Al. Agha, “Integrating fast mobility in the OLSR routing protocol,” *Fourth IEEE Conference on Mobile and Wireless Communications Networks*, September 2002, Stockholm, Sweden.

Mounir Benzaid received his Engineering Degree from the University of Science and Technology of Algiers, Algeria, 1998, and the Master’s Degree in Networking and Distributed Systems from the university of Nice, France, 2000. He is currently working on his PhD at the university of Paris XI and the INRIA research center, in the Hipercom (High Performance Communication) team. His reseach interests are: routing in mobile ad-hoc networks and integration to fixed networks; optimization of IP mobility (macro and micro mobility).

Pascale Minet is Senior Researcher with project Hipercom at INRIA. In 1998, she qualified from the University of Versailles (France) in advising PhD students. She is interested in mobile ad-hoc networks, networks providing quality of service, multimedia systems and more generally distributed real-time systems. She is co-author of the OLSR (Optimized Link State Routing) protocol, submitted at the IETF in the MANET group. Previously, she actively contributed to the ETSI Hiperlan standard, a radio ethernet with mobile stations.

Khaldoun AL AGHA received the HDR (Habilitation diriger des recherches) from the Paris XI University, France in 2002 and the PhD from Versailles University, France, in 1998. He obtained the Master’s Degree from the University of Versailles in 1995. He received the State Engineering Degree from Ecole Supérieure d’Électricité, Paris, France in 1993. He is currently Associate Professor at the University of Paris XI in France. His research interests are on resource allocation and IP Mobility for cellular and ad-hoc networks.

Cedric Adjih was born in France in 1971. He worked on his PhD diploma at INRIA in France, and received it in 2001 from University of Versailles-Saint-Quentin-en-Yvelines in France. He is currently a researcher at INRIA in the Hipercom team.



Graud Allard received a Master’s Degree in computer science from the University of Paris XI in France and a Postgraduate Degree in networking from University of Paris VI, France. He is currently working on a PhD thesis related to quality of service on large ad-hoc networks at INRIA in the Hipercom team.