# Integration of Mobile-IPv6 and OLSR for Inter-MONET Communications

Ines b. Hamida[1], Hakim Badis[1,2], Lila Boukhatem [1] and Khaldoun Al Agha[1,2]
[1]LRI Laboratory, University of Paris XI, Orsay, France
[2]INRIA Laboratory, Rocquencourt, France
{badis, benhamida, boukhatem, alagha}@lri.fr
Phone: (33)(0)169156591, Fax: (33)(0)169156586

***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. MObile NETwork (MONET) is a group of mobile nodes moving together as a unit. Such groups are common characteristics of the vehicular environments, for example train and buses (which are attractive because of the high concentration of passengers on these vehicles). This paper investigates an ad hoc networking for Inter-MONET communications and interworking between MONETs and the global Internet. We propose a hierarchical architecture: (1) integrating Mobile IPv6 and OLSR, a routing protocol for ad hoc networks, to manage universal mobility; (2) connecting this ad hoc network to Internet. The heterogeneous communication is established with the help of specific access routers, which serve as gateways. We describe the network scenario, its basic protocol architecture and we discuss the different practical approaches for routing. A flat and hierarchical ad hoc routing comparison is studied and performance differentials are analyzed through simulation results using varying network load and mobility.

## I. INTRODUCTION

With the advances in wireless communication and mobile computing technologies, wireless multihop networking (ad hoc networking) is expected to play an important role in mobile communications beyond fourth generation systems. Because of its independence on pre-existing network infrastructure and its distributed organization, ad hoc networking enables the spontaneous establishment of communication between network-enabled electronic devices (e.g., mobile phones, personal digital assistants). Especially in applications where information must be distributed quickly and is only relevant in the area around the sender, ad hoc communications have major advantages compared to *conventional* wireless systems, such as GSM and UMTS. For example, cars involved in an accident can send warning messages back over a defined number of other vehicles, thus avoiding a motorway pileup [1]. In this vehicular scenario, we can also imagine transmission of information about bad traffic or street conditions (e.g., icy roads, obstacles), or wireless communication of closed user groups (e.g., emergency teams). A mobile ad-hoc network (MANET) [2] is a collection of nodes, which are able to connect on a wireless medium forming an arbitrary and dynamic network with *wireless links*. Implicit in this definition of a network is the fact that links, due to node mobility and other factors, may appear and disappear at any time. This in a MANET implies that the topology may be dynamic and that routing of traffic through a multi-hop path is necessary if all nodes are to be able to communicate.

A MObile NETwork (MONET) [3] is an entire network, moving as a unit, which changes its point of attachment to the Internet and thus its reachability in the topology. A MONET may be composed by one or more IP-subnets and is connected to the global Internet via one or more Mobile Routers (MR). Cases of mobile networks include networks attached to people (Personal Area Network or PAN, i.e., a network composed by all Internet appliances carried by people, like a PDA, a mobile phone, a digital camera, a laptop, etc.) and sensor networks deployed in aircrafts, boats, busses, cars, trains, etc. An airline company that provides permanent on-board Internet access is an example of a MONET. This allows passengers to use their laptops, PDA, or mobile phone to connect to remote hosts, download music or video and browse the web. Passengers could themselves carry a network with them (a PAN). Similarly, a bus, the metropolitan public transport, or the taxi company could allow passengers to connect their PAN to the Internet via the embarked network, therefore ensuring, while on-board, an alternative to the metropolitan cellular network, in terms of cost, available bandwidth or access control, etc. Traditional work on mobility support as conducted on Mobile IP working group is to provide continuous Internet connectivity to mobile hosts only (host mobility support) and enables to support network mobility. The NEMO [4] working group has therefore been created to

propose specific solutions for network mobility support.

This paper addresses the ad hoc networking for Inter-MONETs and interworking between MONETs and Inernet using ad hoc routing, where we restrict our view to IPv6 [5]. The wireless multihop access network is entirely based on IP, uses the optimized Link State Routing protocol (OLSR) [6] and meets the requirements of future *full-IP* wireless networks, such as providing high-rate video, voice and data services.

In the flat routing, the routing information may be maintained regularly (called proactive or table-driven routing) or computed when needed (called reactive or on-demand routing). In the hierarchical routing, the mobile nodes (MN) are clustered into several groups. The routing information is maintained separately within a group and among groups. A typical route can be found in the group-level granularity first and then in the node-level granularity. Extensive simulations are carried out to study performance comparison of flat and hierarchical ad hoc routing for Inter-MONET.

The remainder of this paper is organized as follows: in Section II, we give an overview of the MONET, terminology and the different Approaches for MONET mobility support. Section III describes wireless ad hoc networks, protocols, addressing and solution approaches for mobility using manet. We present in Section IV our proposed architecture for mobility management. Different routing and addressing mechanisms are discussed and compared in Section V. Performance results are presented in section VI. Finally, Section VII concludes this paper and defines topics for further research.

## II. Mobile Network (MONET)

### A. Terminology

Before discussing network mobility problems, we first give some useful definitions to introduce the MONET context. MONET is a network that changes its Internet access point. It is formed of mobile nodes called MNNs (Mobile Network Nodes) and one or more MRs (Mobile Routers). All these nodes move together as a single unit. The MR takes in charge the handover procedure. It has one or more interfaces and maintains the Internet connectivity for the entire mobile network. It gets access to the Internet through an AR (Access Router) which is an external router. A mobile network is said to be nested when another mobile network is getting attached to it. It is said multihomed when there are more then one active interface connected to the global Internet. The reader can refer to [7] for more details in terminology.

### B. MONET mobility approaches

Some solutions were proposed to enable support for network mobility [8], [9], [10], [11]. In [8], the authors proposed to extend Mobile-IPv6 protocol with *Prefix Scope Binding Updates*. These requests are Binding Updates that associate a CoA with the MONET prefix shared by all MNNs, instead of the full home address. The MONET prefix is carried in a new sub-option and requires a new flag (P) in the Mobile-IPv6 binding Update option. Then, a unique Prefix Scope Binding Update message allows registration of an entire MONET independently of the number of MNNs and transparently to them. Furthermore, at each subsequent point of attachement, the MR sends a Prefix Scope Binding Update to its home agent HA (special router on the home link), to its correspondant nodes CNs and to CNs of MNNs. Each recipient of this request adds an entry in its Binding Cache to do the binding between the MR's home address and the MR's care of address. Besides, if the bit (P) is set, it adds a second entry in its binding cache to do the binding between MONET prefix and MR's care of address. Consequently, before sending a packet, a correspondant node examines its Binding Cache for MNN's MONET prefix. If an entry is found, the CN sends the packet directly to MR's new location using a type 2 routing header. Otherwise, it sends the packet to the mobile node's home address.

## III. MANET Capabilities

Mobile ad hoc network (MANET) is self-organizing, rapidly deployable, and requires no fixed infrastructure. Nodes in an ad-hoc network may be highly mobile, or stationary, and may be very widely in terms of their capabilities and uses. The primary objectives of this new network architecture are to achieve increased flexibility, mobility and ease of management relative to infrastructured wireless networks. 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.

Several protocols exist, addressing the problem of routing in mobile ad hoc networks. We can classify the routing protocols on the basis of their control behavior in the following categories: proactive, reactive and hybrid.

Proactive protocols use an adaptive system of routing based on periodic exchange of control messages. There may be various kinds of control messages: those which are sent locally (broadcast to one-hop) to enable a node to discover its local neighborhood; and those which are

sent to be diffused in the network and which permit to distribute the topology information to all the nodes in the network. In a proactive approach, the routing protocol periodically updates the reach ability information in the nodes' routing table. Thereby a route is immediately available when needed. The cost for it is a use of substantial bandwidth for the periodic control traffic to acquire information, some of which may never be used. Proactive protocols include DSDV [12], OLSR [6] (an optimization of the link state algorithm OSPF [13]) and TBRPF [14].

Reactive protocols do not take any initiative for finding a route to a destination, before the information is needed. The protocol attempts to discover routes only *on demand* by flooding its query in the network. During route discovery, the data packet is put on wait until the route becomes available. The drawback of this technique is that the broad consumption of the bandwidth for its global search (flooding) process, as well as adding large delays before sending data packet. Examples of reactive protocols include AODV [15] and DSR [16].

Hybrid protocols as ZRP [17] and CBR [18], 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 on [19] 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 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 [16], with the Internet routing and Mobile-IP is presented in [20]. 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 the 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. 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.

In Mobile-IP for Mobile Ad hoc NETworks (MIPMANET) [21], nodes 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 using the AODV protocol in the ad hoc network. Moreover, MIPMANET uses a mechanism called MIPMANET Cell Switching (MMCS) that allows a mobile node to determine when is should register with another Foreign Agent.

In [22], authors have proposed an integrated architecture that manages 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, a routing protocol for ad hoc-networks, is used for micro-mobility management within the access network.

## IV. Proposed architecture for mobility management

### A. Hierarchical mobility management

The proposed architecture is depicted in Figure 1. An OLSR-IP access network constitutes an IP subnetwork and its interconnected to the Internet via an OLSR Access Router (OLSR-AR). The motion of a Mobile Router (MR) inside an OLSR-IP access network is managed by the OLSR protocol and the Mobile Node (MN) inside the MONET by a wireless LAN. Mobility between different OLSR-IP access networks or IP subnetworks is managed by Mobile-IPv6.

An OLSR-IP access network consists of a random topology of ad hoc moving networks. In our MONET, an OLSR Mobile Router (OLSR-MR) provides connectivity between MONETs and OLSR-ARs. We can find more then one OLSR-MR per MONET.

The architecture is composed of several functional entities:

- ☞ Home Agent (HA): a Router in the MN's home network.
- ☞ OLSR Mobile Router (OLSR-MR): a router which changes its point of attachment to the Internet. The OLSR-MR has one or more egress interface(s) and one or more ingress interface(s) and acts as the gateway between the mobile network and the rest of the Internet. The OLSR-MR implements the OLSR protocol.
- ☞ OLSR Access Router (OLSR-AR): any subsequent point of attachment of the OLSR-MR at the network layer. Basically, a router on the home link or the foreign link. It can also implement the role of a HA if the OLSR-IP access network is the home

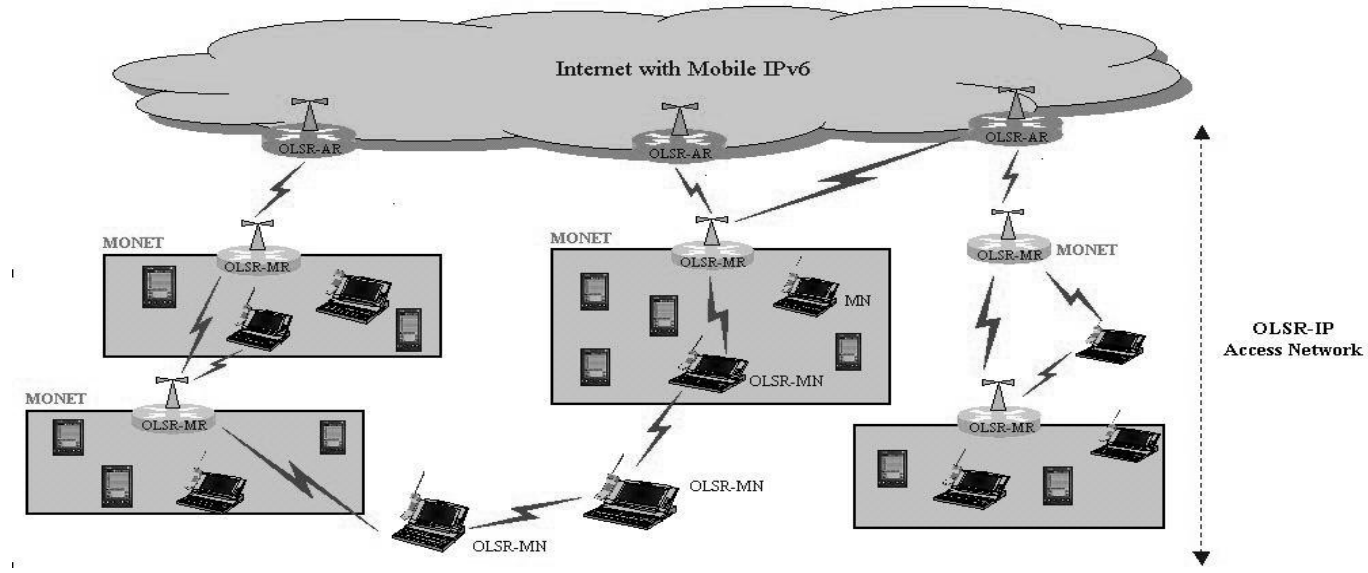



Fig. 1. Hierarchical mobility management

network. Furthermore, OLSR-AR implements the OLSR protocol.

- ☞ Mobile Node (MN): A node, either a host or a router located within the MONET. A MN could be any of OLSR-MR.
- ☞ OLSR Mobile Node (OLSR-MN): a MN that can implement the OLSR protocol.
- ☞ Ad hoc Mobile Node (ad hoc MNs): an OLSR-MR or OLSR-MN.
- ☞ Correspondent Node (CN): any node that is communicating with one or more MN.

In our architecture, OLSR-ARs and OLSR-MNs form an ad hoc network and use the OLSR routing protocol. MNs in the MONET implement a wireless LAN, and connected to the global Internet via its OLSR-MR. Some of MNs which are the OLSR-MNs implement the OLSR protocol and have a routing table. An OLSR-MR can exchange information directly with its OLSR-MRs neighbors. If an ad hoc MN has no OLSR-AR and OLSR-MR as neighbor, it can connect to the Internet by an OLSR-MN. Any OLSR-MN that belongs to the MONET, connects to its OLSR-MR using the OLSR protocol.

### *B. Access router discovery*

Upon initialization, a MN or should discover the existence of all access routers in its reachability and then select one access router out of these candidates. This problem is well-known for systems with only direct (single hop) connections between MNs and ARs, but the multihop environment makes the discovery algorithm more complicated.

In general, AR discovery can be initiated by the MN (active discovery) or the AR (passive discovery). In practice, both discovery methods can be combined and run in parallel. This leads to a hybrid method for AR discovery. The AR periodically sends out advertisements, and all nodes in its radio range store this information. An active *access router solicitation*, which was broadcasted by a MN that is not in the radio range of a gateway, can now be answered by an intermediate node with stored AR information, thus reducing the signaling traffic. Intermediate MNs cannot reply, if the active *access router advertisement* was sent to the Access Router Multicast Address. If an MN receives, within a certain time, more than one *access router advertisement* from different ARs, it selects one AR according to a certain metric (e.g., received signal level from AR, hop count, capacity, security issues, load of AR, or combination of this criteria). This is denoted as access router selection.

In our architecture, the ad hoc network is logically separated into MONETs. The OLSR-ARs and OLSR-MRs periodically send out advertisements. Each OLSR-MR selects one OLSR-AR as its default route according to a certain metric. If an OLSR-MR has no OLSR-AR in its radio range, it sends an *access router solicitation*. Any intermediate ad hoc MN can answer with its stored information AR. So, any OLSR-MR can obtain the prefix OLSR-AR information. Each MN selects one OLSR-MR (the MONET can contain more then one OLSR-MR) of its MONET as default route. Furthermore, each OLSR-MN stored information about an OLSR-AR selected by its OLSR-MR to answer to the ad hoc MNs's *access router solicitations*.

### C. Address Autoconfiguration

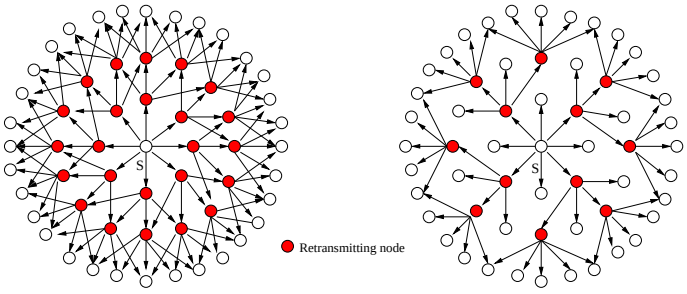
IPV6 defines two fundamental principles for autoconfiguration: stateful and stateless autoconfiguration. Stateful address autoconfiguration can be implemented by a DHCP server [23] residing in the OLSR-AR and OLSR-MR. It automatically assigns addresses to requesting MNs, and manages the address space. The MNs learn the IP address of the DHCP server from the OLSR-AR and OLSR-MR discovery respectively.

Let us now consider stateless autoconfiguration. In fixed IPv6 networks, a node first forms a link-local address to obtain IP-level connectivity with neighboring nodes [24]. This temporary address is a combination of the reserved link-local prefix FE80::0 and the node's equipment identifier (EUI). Using this initial address, the node learns the prefix of its router, and can then form a global or site-local address. This configuration method must be slightly modified to work in our multihop scenario betweenn OLSR-ARs and ad hoc MNs because link-local addresses may not be applicable for multihop communication. Instead of using the link-local prefix FE80::0, OLSR-MRs and OLSR-MNs must use a different reserved prefix (e.g., the MANET initial prefix [25]) to generate a temporary address. The uniqueness of the address can be validated by a protocol for Duplicate Address Detection (DAD), e.g., as described in [25]. After a successful DAD of this initial address, a node can communicate with other nodes in the ad hoc network and is therefore able to send and receive messages for OLSR-MR and OLSR-AR discovery. From received Access Router Advertisement and Response messages, it learns the prefix information that identifies each candidate OLSR-AR or OLSR-MR. After selecting one OLSR-AR for the OLSR-MRs and one OLSR-MR for the OLSR-MNs belong in the same MONET, the OLSR-MR and OLSR-MN combine the prefix of this OLSR-AR or OLSR-MR and the EUI to generate a globally routable IP address. The initial address should time out in all routing tables after a short period of time.

### D. Optimized Link State Routing Protocol (OLSR)

OLSR [6] is a proactive routing protocol, which inherits the stability of a link state algorithm [26] and has the advantage of having the routes immediately available when needed due to its proactive nature. In a pure link state protocol, all the links with neighbor nodes are declared and are flooded in the whole network. The OLSR protocol is an optimization of the pure link state protocol for the mobile ad hoc networks. First, it reduces the size of the control packets: instead of all links, it declares only a subset of links with its neighbors that are its multipoint relay selectors [27]. Secondly, it minimizes the flooding of its control traffic by using only the selected nodes, called multipoint relays, to broadcast its messages. Therefore, only the multipoint relays of a node retransmit the packets. This technique significantly reduces the number of retransmissions in a flooding or broadcast procedure [28], [29]. OLSR protocol performs hop by hop routing, i.e., each node uses its most recent information to route a packet.

*1) Multipoint Relay:* The idea of multipoint relays is to minimize the flooding of broadcast packets in the network by reducing duplicate retransmissions in the same region. Each node $S$ of the network independently selects a set of nodes in its one-hop neighbors, which retransmits its packets. This set of selected neighbor nodes, called the multipoint relay (MPRs) of $S$ and denoted $\mathrm{MPR}(S)$, is computed in the following manner: it is the smaller subset of one-hop neighbors with a symmetric link, such that all two-hop neighbors of $S$ have symmetric links with $\mathrm{MPR}(S)$. This means that the multipoint relays cover (in terms of radio range) all the two-hop neighbors. Figure 2 shows the multipoint relay selection by node $S$.




(a) Pure flooding. (b) Diffusion using multipoint relays.

Fig. 2. Multipoint relays of node $S$.

Only MPR nodes forward broadcast messages received from one of their MPR selectors.

*2) Neighbor Sensing:* Each node must detect the neighbor nodes with which it has a direct and bi-directional link. The uncertainties over radio propagation may make some links uni-directional. Consequently, all links must be checked in both directions in order to be considered valid. For this, each node periodically broadcasts its HELLO messages, containing the list of neighbors known to the node and their link status. HELLO messages are received by all one-hop neighbors, but are not forwarded. They are broadcast at a low frequency determined by the refreshing period *Hello Interval* (the default value is 2 seconds).

These HELLO messages permit each node to learn the knowledge of its neighbors up to two hops. On the basis of this information, each node performs the selection of

its multipoint relays. These selected multipoint relays are indicated in the $hello$ messages with link status MPR. On the reception of HELLO messages, each node can construct its MPR selectors table.

*3) Topology Information:* Each node with a non-empty MPR selector set periodically generates a Topology Control message (TC message). This TC message is diffused to all nodes in the network at least every *TC Interval*. A TC message contains the list of neighbors that have selected the sender node as a multipoint relay. The information diffused in the network by these TC messages will help each node to build its topology table. Based on this information, the routing table is calculated. The route entries in the routing table are computed with Dijkstra's shortest path algorithm [30]. Hence, they are optimal as concerns the number of hops.

The routing table is based on the information contained in the neighbor and the topology tables. Therefore, if any of these tables is changed, the routing table is re-calculated to update the route information about each known destination in the network.

## V. Routing and Addressing in OLSR-IP Access Network

This section describes and compares different approaches for flat and hierarchical routing in our heterogeneous scenario.

### A. Flat Routing

Let us first consider the case in which a flat routing protocol is used in our architecture (Figure 3). Such protocol regards the ad hoc network as a number of nodes without subnet partitioning. The communication in this environment can be categorized into two scenarios: (1) routing between an Internet host and a MN and (2) routing between two MNs with the same OLSR-AR or with different OLSR-ARs.

With the OLSR protocol, an ad hoc MN (OLSR-MR or OLSR-MN) senders should have an entry for the destination in its routing table, which is either a route in ad hoc network or a link to the default OLSR-AR if the destination is not reachable through the ad hoc network.

*1) Communication btw. An ad hoc MN and Internet host:* After obtaining a route to the destination, an ad hoc MN can tunnel IPv6 packets through the ad hoc network to the OLSR-AR, which then forwards them to the Internet host. There are two methods to realize this tunneling. One method is that the ad hoc MN encapsulates each IPv6 packet (i.e., they add an ad hoc header with the OLSR-AR as destination). Another method is possible, the sending ad hoc MN uses the IPv6 extension header.

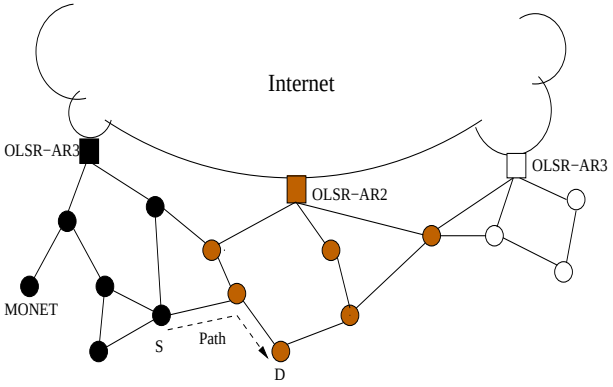



Fig. 3. Flat routing in the OLSR-IP access network

The routing extension of this header contains the final destination address, i.e., the address of the Internet host, and the destination field of the IPv6 header contains the final destination the OLSR-AR address. Only an ad hoc MN with an IP address mentioned in the destination field of the IPv6 header of an IPv6 packet can examine the routing header of this packet [5]. The home destination option of Mobile IPv6 is used to inform the correspondent IP host about the home address of the ad hoc MN. The OLSR-AR decapsulates the incoming packets from the ad hoc MN, or it reads the routing header and puts the address of the IP host into the destination field of the IPv6 header. The resulting packet is then routed through the Internet to the IP host.

We now consider traffic from the CN to the ad hoc MN. If the CN knows the care-of address of the ad hoc MN, it puts ad hoc MN's care-of address in the IPv6 destination address field and the ad hoc MN's home address in the routing header of the routing IP packet. If the CN has no binding information about the ad hoc MN, it sends a usual IPv6 packet the ad hoc MN's home address. The home agent intercepts this packet and must tunnel it to the ad hoc MN's current care-of address using IPv6 encapsulation. In the remaining routing process, we can distinguish two design options:

- All ad hoc MNs of a single subnet have been assigned the same care-of address from the OLSR-AR, e.g., by stateful autocongiguration. The OLSR-AR possesses two IP addresses: a home address the identifies the OLSR-AR uniquely and a second address that is given as care-of address to the ad hoc MNs. Both addresses have the same prefix. With this address assignment, incoming IP packets that are addressed to an MN's care-of address can be processed by the OLSR-AR, i.e., the OLSR-AR can decapsulate packets or examine the routing header, respectively. The home address of the MNs is used in routing, i.e., the OLSR-AR uses the MN's home

address as the destination address.

- Each ad hoc MN has been assigned a different care-of address with the prefix of the corresponding OLSR-AR using stateful or stateless autoconfiguration (this is in our case). This address or the home address can be used in ad hoc routing, where the location information of the care-of address is not used. The content of packets from the ad hoc MN to an IP host (outgoing traffic) is the same as in the previous case. In case of incoming traffic, the OLSR-AR does not decapsulate packets or examines routing headers that are addressed to the care-of address of ad hoc MNs.

*2) Communication btw. Ad hoc MNs:* In order to send an IPv6 packet to another ad hoc MN in the ad hoc network, the ad hoc MN originates an IPv6 packet with the address the destination ad hoc MN in the IPv6 header. No IPv6 routing header is required in this case.

### B. Hierarchical Routing with Care-of address

Using hierarchical routing, the ad hoc network is logically separated into subnets (i.e., cluster) (Figure 4). When an ad hoc MN receives a packet, it checks the destination address. If itself is the destination, it processes the packet for further operation. If the ad hoc MN is not the destination and the prefix of the source is different than its own prefix, the ad hoc MN ignores this packet. Inter-subnet information exchange is only possible via the OLSR-AR. In this case, a hierarchical address structure is also needed for routing in the ad hoc network, and therefore an ad hoc MN's care-of address is the right choice for addressing in the ad hoc routing protocol, since it contains the prefix of the OLSR-AR that a node is registered with. It is required that each ad hoc MN obtains a unique care-of address.

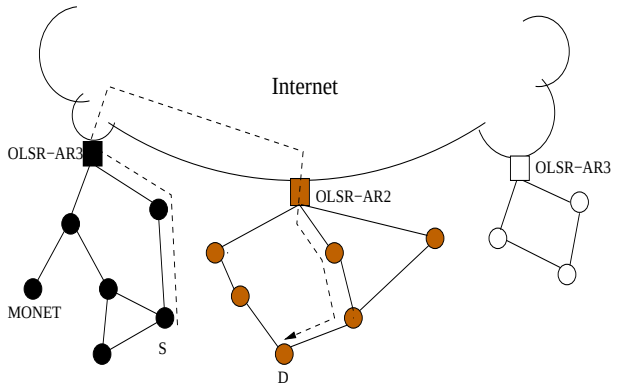



Fig. 4. Hierarchical routing in the OLSR-IP access network

If an ad hoc MN wants to send data packet to an Internet host, it knows from the prefix of the destination address that his host does not belong to its own subnet. Thus, it sends the data packets to the OLSR-AR using the OLSR protocol. Once the OLSR-AR receives the data packets, it forwards them to the Internet host.

*2) Communication btw. Ad hoc MNs in same subnet:* if an ad hoc MN wants to communicate with another ad hoc MN that has attached to the same OLSR-AR, the ending ad hoc MN learns from the prefix of the destination's care-of address, that the destination is located in the same IP subnet (from the routing table). If the sender knows only the home address of the destination, packets will be routed to the home agent of the destination.

*3) Communication btw. Ad hoc MNs in different subnets:* The sender learns from the IP prefix, that the destination is located in a different IP subnet. Thus, the packets are routed toward its serving OLSR-AR, and the source OLSR-AR routes the packets to the destination OLSR-AR via the fixed IP network. The destination OLSR-AR forwards the packets to the destination using the OLSR protocol.

### C. Comparison

A hierarchical approach in the ad hoc network continues the hierarchical architecture of the Internet. Moreover, it limits some signaling traffic to the subnet of an OLSR-AR. On the other hand, an advantage of the flat approach is that each node forms a care-of address.

For communication between ad hoc MNs and Internet hosts as well as between ad hoc MNs in the same subnet, the routing path optimality is similar for both approaches. For communication between ad hoc MNs in different IP subnets, the route optimality depends on the distance between two ad hoc MNs: In case the source and destination are close to each other, the optimal path is the flat wireless multihop path between them. In case the ad hoc MNs are far away from each other, the traffic between two IP subnets should be transported via a hierarchical routing path through the fixed network.

## VI. Simulations

### A. Simulation model

*1) Topology model:* In our simulation model, we generate a monet network as a collection of nodes moving together. Every monet network has at least one MR. The number of monets in the system and the number of mobiles inside a monet are specified as input parameters. The system contains a set of access routers, each of them covers a geographical area of random size. Every generated monet is placed in a region randomly selected. The region is represented by a subqueue with a profile

containing the co-ordinates x and y, the bandwidth, the latency time and the registration time of the access router of this region.

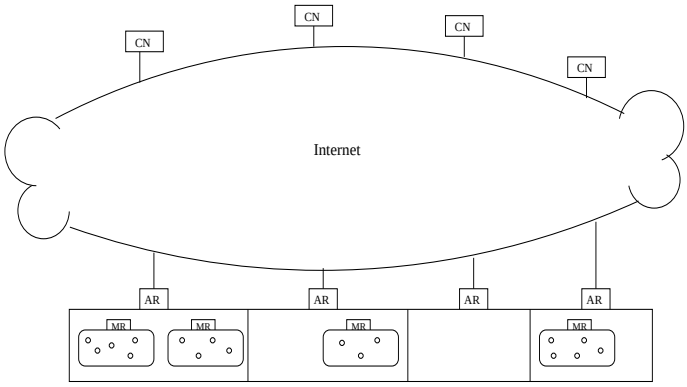



Fig. 5. Topology model

*2) Monet mobility model:* We have restricted the mobility of a monet network in a constant direction with a random varying speed. The monet speed model is a continuous time stochastic process. Each monet movement consists of a sequence of random length intervals during which a monet moves at a constant speed. To compute the position of a monet $n$ at time $t$ during an interval $i$ of duration $T_n^i$ and speed $V_n^i$, we calculate at the first time the distance $D$ covered by $n$, $D = V_n^i * T_n^i$, then we determine the global position by changing the scale.
Figure effig:mobilite illustrates the movement of monet $n$ over six intervals.

We have not considered a mobility inside a mobile network. All the nodes of the same etwork move at the same speed.

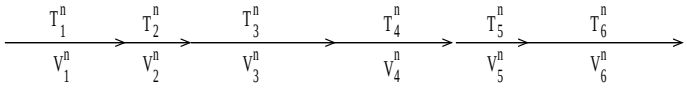



Fig. 6. Monet mobility model

To obtain the balance between the arrivals and departures in the coverage area of OLSR-ARs, all the OLSR-MRs leaving the last OLSR-AR zone are reinjected in the first OLSR-AR zone, thus eliminating the board's effects. Figure 7 shows the reinjection of monet.

There are three important parameters : $\lambda_n$, $speed_{max}$ and $speed_{min}$ for calculating the interval lengths and speed. The interval lengths are exponentially distributed with mean $1/\lambda_n$. The speed during each interval is uniformly distributed over($speed_{min}$, $speed_{max}$).

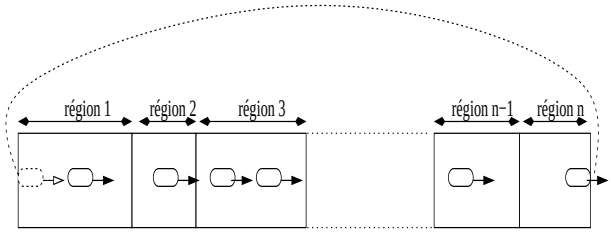



Fig. 7. Way-Round model

### B. Traffic model

Data packets are generated according to the Poisson distribution. The packet arrival rate is divided between all monet in the system. In our simulations, the destination for a data packet is randomly selected among all the destinations in the network, at each selection.

### C. Results

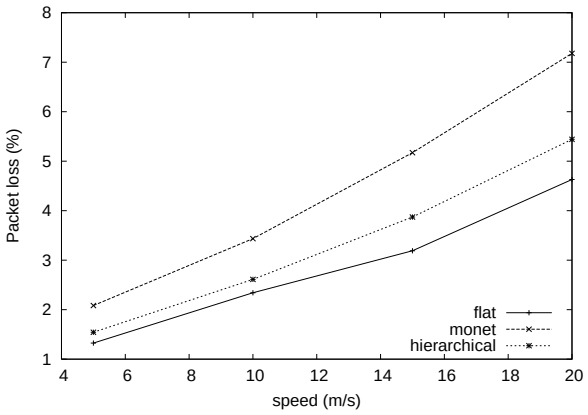



Fig. 8. Loss data packets versus mobility with 200ms as interarrival

Figure 8 shows the results of our simulation in which the data packets sent and lost plotted against the increasing speed. The OLSR-MR's speed is increased from $5meters/second$ ($18Km/hr$) up to $20meters/second$ ($72Km/hr$).

In this simulation, 5 OLSR-MRs move in the same direction using our mobility model. All the 5 OLSR-MRs are packet-generating sources using $200ms$ as interarrival and. Each OLSR-MR source selects randomly one of the remaining OLSR-MR as a destination. The OLSR-AR range is a uniform value between $1000m$ and $2000m$, the OLSR-MR area range is $200m$. Each OLSR-MR node selects its speed and direction which remains valid for next $60seconds$. We can see that when the mobility (or speed) increases, the number of packet loss increases. This can be explained by the fact that when a node moves, it goes out of the neighborhood (OLSR-AR in MONET or OLSR-MR in MANET) of a node

which may be sending it the data packets. There are about 2.1% of packets lost for monet classical routing at a mobility of $5meters/second$ (1.5% for hierarchical routing and 1.3% for flat routing). At a mobility of $20meters/second$, 7.2% of packets are lost for monet classical routing (5.4% for hierarchical routing and 4.6% for flat routing). The data packets are lost during the handover and Access router discovery latency. Flat routing has the highest packets delivered because during the OLSR-MR handover process, packets to this OLSR-MR are forwarded by one of its OLSR-MR neighbor. In Flat and Hierarchical routing mechanisms, the data packets are lost because the next-hop node is unreachable. A node keeps an entry about its neighbor in its neighbor table for about 6 seconds. If a neighbor moves which is the next-hop node in a route, the node continues to forward it the data packets considering it as a neighbor. Also, the next-hop is unreachable if there are interferences.

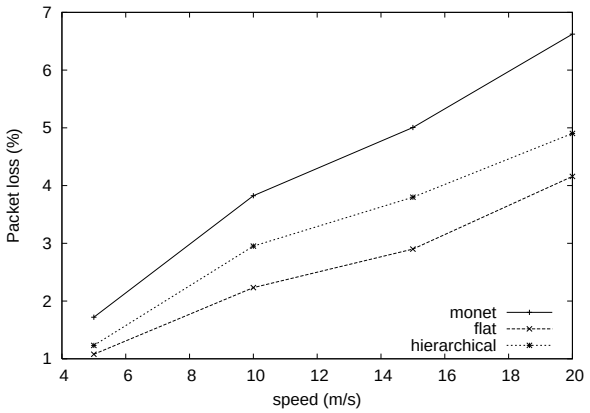



Fig. 9. Loss data packets versus mobility with 400ms as interarrival

In Figure 9, we show the packet loss versus the increasing speed. We modify only the packet arrival rate using $400ms$ as interarrival parameter. The loss packet has the same behavior as that of Figure 8. However, it is clear that the packet loss in figure 9 is less than that the figure 8 (packet arrival rate used to obtain Figure 9 is less than that the figure 8).

Fig. 10 and 11 show the data packets loss probability versus mobility and interarrival for flat and hierarchical routing respectively. As explained before, loss probability of data packets increases with increasing speed and decreases with increasing interarrival. The data packets are lost during handovers and access routers discovery latency. High values of interarrival imply less data packets in the OLSR-IP access network and leads to a less loss data packets. We note also, flat routing presents more performance than hierarchical routing in terms of loss probability.

Fig. 12 depicts end-to-end delay for both flat and

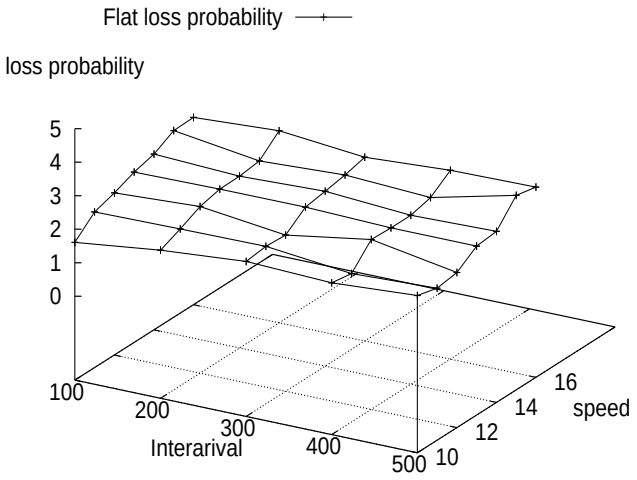



Fig. 10. Loss data packets versus mobility and interarrival for flat routing

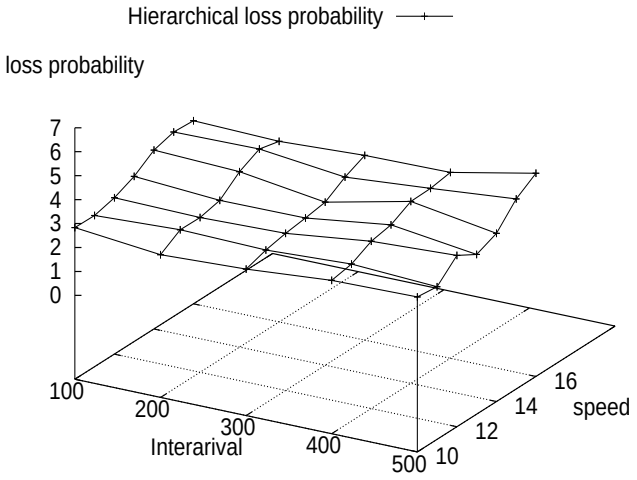



Fig. 11. Loss data packets versus mobility and interarrival for hierarchical routing

hierarchical routing. Flat routing has an average delay about 130 ms. However, hierarchical routing has 300 ms. This can be explained by the fact that in flat network, the hop count number between any two ad hoc MNs is less than in hierarchical network. A low variation can be detected with increasing interarrival and speed due to the high number of ad hoc MNs.

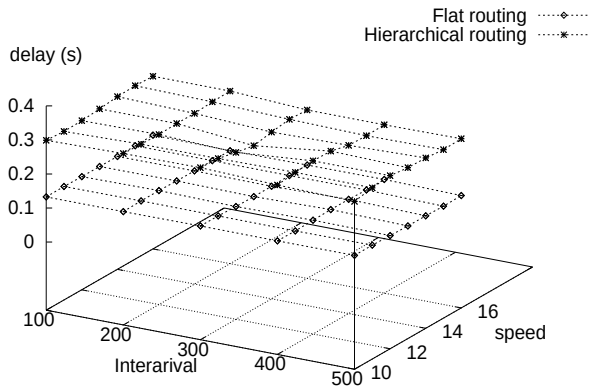



Fig. 12. Delay versus mobility and interarrival for flat and hierarchical routing

## VII. Conclusions

In this paper, we considered the Internet access of mobile devices in a wireless ad hoc network via specific access routers. We have described problems and our solution approach for access router discovery and routing. A new architecture is proposed to manage the MONET mobility using OLSR protocol. An OLSR-IP access network consists of a random topology of ad hoc moving networks. OLSR-ARs and OLSR-MNs form an ad hoc network and use the OLSR rouring protocol. Simulations are carried out using an efficient simulation model to study the performance of our proposed architecture. We have shown that flat routing achieves less data packet loss and end-to-end average delay.

Topics for further research include the investigation of proper methods for access router selection. Furthermore, *location updating* and *multihop handover* schemes must be designed and evaluated. Also, we will propose a smooth handover with reduced packet losses.

## References


[1] W. Kellerer, C. Bettstetter, C. Schwingenschlogl, P. Sties, K.E. Steinberg and H.J. Vogel, " (Auto)Mobile communication in a heterogeneous & converged world," *IEEE Personal Comm. Mag.*, December 2001.

[2] "http://www.ietf.org/html.charters/manet-charter.html."

[3] V. Devarapalli, R. Wakikawa, A. Petrescu and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol," *RFC 3963*, January 2005.

[4] "http://www.ietf.org/html.charters/nemo-charter.html."

[5] S. Deering and R. Hinden, "IPv6 Specification," *RFC 2460*, December 1998.

[6] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol," *RFC 3626*, October 2003.

[7] T. Ernst and H. Y. Lach, " Network Mobility Support Terminology," *In IETF Internet Draft*, 2002.

[8] T. Ernst, A. Olivereau, L. Bellier, C. Castelluccia and H. Y. Lach, " Mobile Networks Support in Mobile IPv6 (Prefixe Scope Binding Update)," *In IETF Internet Draft*, March 2002.

[9] T. Ernst, K. Uehara and K. Misuya, " Network Mobility from the internetCAR perspective," *17 th International Conference on Advanced Information Networking and Applications (AINA'03)*, March 2003.

[10] T. J. Kniveton, J. T. Malinen, V. Devarapalli, and C. Perkins, "Mobile Router Support with Mobile IPv6," *In IETF Internet Draft*, August 2001.

[11] H. Soliman and M. Pettersson, "MObile NETworks (MONET) problem statement and scope," *In IETF Internet Draft*, February 2002.

[12] C. Perkins and P. Bhagwat, " Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," *Association for Computing Machinery's Special Interest Group on Data Communication'94*, pp. 234–244, 1994.

[13] J. Moy, "Open Shortest Path First (OSPF) V2," no. 2328, January 1998.

[14] R. Ogier, F. Templin, M. Lewis, "Topology Dissemination Based on Reserved-Path Forwarding (TBRPF)," no. 3684, February 2004.

[15] C. Perkins, E. M. Royer and S. R. Das, "Ad Hoc On-Demand Distance Vector routing," *RFC 3561*, July 2003.

[16] D. Johnson and Al, "Dynamic Source Routing in Ad Hoc Wireless Networks," *In IETF Internet Draft, draft-ietf-manet-DSR-10.txt*, July 2004.

[17] Z. J. Hass, M. R. Pearlman and P. Samar, "The Zonr Routing Protocol (ZRP) for Ad Hoc Networks," *Internet draft*, July 2002.

[18] M. Jiang, J. Li, Y.C. Tay, "Cluster Based Routing Protocol (CBRP)," Jully 1999.

[19] C. Perkin and H. Lei, " Ad hoc Networking with Mobile IP," *Second European Personal Mobile Communication Conference*, pp. 197–202, October 1997.

[20] D. Johnson, D. A. Maltz and D. Johnson, "Supporting Hierarchy and Heterogeneous Interfaces in Multi-hop Wireless Ad hoc Networks," *IEEE International Symposium on Parallel Architectures, Algorithms and Networks*, pp. 75–85, June 1999.

[21] U. Jonsson, F. Alriksson, T. Larsson, P. Johansson and G. Maguire, " MIPMANAT - Mobile IP for Mobile Ad hoc Networks," *IEEE/ACM Workshop on mobile and ad hoc networking and computing*, pp. 75–85, August 2002.

[22] M. Benzaid, P. Minet, K. Alagha, C. Adjih and G. Allard, "Intergration of Mobile-IP and OLSR for Universal Mobility," *Wireless network journal*, July 2004.

[23] J. Bound, M. Carney, C.Perkins and R. Droms, "Dynamic host configuration protocol for IPv6 (DHCPv6)," *Internet draft, work in progress*, June 2001.

[24] S. Thomson and T. Narten, "IPv6 stateless address autocongiguration," *RFC 2462*.

[25] C. E. Perkins, J. T. Malinen, R. Wakikawa, E. M. Belding-Royer and Y. Sun , "IP address autoconfiguration for ad hoc networks," *Internet Draft*, November 2001.

[26] E. Streenstrup, "Routing in Communication Networks," *Prentice Hall International, Inc., Englewood Cliffs*, 1995.

[27] A. Qayyum, L. Viennot and A. Laouiti, "An efficient technique for flooding in mobile wireless networks," *Research Report RR-3898, INRIA*, February 2000.

[28] P. Jacquet, P. Muhletaler, A. Qayyum, A. Laouiti, T. Clausen and L. Viennot, "Optimization Link State Routing Protocol," *IEEE INMIC, Pakistan*, December 2001.

[29] A. Qayyum, L. Viennot and A. Laouiti, "Multipoint relaying technique for flooding broadcast message in mobile wireless networks," *HICSS: Hawaii International Conference on System Sciences. Hawaii, USA*, January 2002.

[30] A. S. Tanenbaum, "Computer Networks," *Printice Hall*, 1996.