Design and Experimental Evaluation of a Route Optimization Solution for NEMO

María Calderón, Carlos J. Bernardos, Marcelo Bagnulo, Ignacio Soto, and Antonio de la Oliva

***Abstract*—An important requirement for Internet protocol (IP) networks to achieve the aim of ubiquitous connectivity is network mobility (NEMO). With NEMO support we can provide Internet access from mobile platforms, such as public transportation vehicles, to normal nodes that do not need to implement any special mobility protocol. The NEMO basic support protocol has been proposed in the IETF as a first solution to this problem, but this solution has severe performance limitations. This paper presents MIRON: Mobile IPv6 route optimization for NEMO, an approach to the problem of NEMO support that overcomes the limitations of the basic solution by combining two different modes of operation: a Proxy-MR and an address delegation with built-in routing mechanisms. This paper describes the design and rationale of the solution, with an experimental validation and performance evaluation based on an implementation.**

***Index Terms*—Computer network performance, mobile communication, mobile IPv6 (MIPv6), mobile router (MR), network mobility (NEMO), route optimization (RO).**

I. Introduction

THE Internet is evolving towards a more ubiquitous network, accessible anytime, anywhere. Forthcoming fourth-generation (4G) [1] networks are expected to make possible the access through different and heterogeneous technologies, enabling true mobility.

Triggered by these needs and the fact that deployed Internet protocols did not support mobility of any kind, the technical community designed several solutions that addressed the problem of mobility. Protocols such as dynamic host configuration protocol (DHCP) [2], [3] enabled the *portability* of terminals, but this was not enough to achieve real and transparent mobility, as it required ongoing transport sessions to be restarted after a change of the point of attachment. Terminal *mobility* support was first enabled by Mobile IP protocols [4], [5] and nowadays there are lots of proposals that extend and improve this support [6], [7] or address it in a different way [8]–[10].

Manuscript received June 3, 2005; revised February 2, 2006. The work described in this paper is based on results of IST FP6 Integrated Projects DAIDALOS I and II. DAIDALOS I and II receive research funding from the European Community's Sixth Framework Programme. Apart from this, the European Commission has no responsibility for the content of this paper. The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

The authors are with the Department of Telematics Engineering, Universidad Carlos III de Madrid, Leganés (Madrid) 28911, Spain (e-mail: maria@it.uc3m.es; cjbc@it.uc3m.es; marcelo@it.uc3m.es; isoto@it.uc3m.es; aoliva@it.uc3m.es).

Digital Object Identifier 10.1109/JSAC.2006.875109

As the Internet access becomes more and more ubiquitous, demands for mobility are not restricted to single terminals anymore. Supporting the roaming of networks that move as a whole is required in order to enable the transparent provision of Internet access in mobile platforms, such as trains, planes, buses, etc. [11]. The network mobility (NEMO) basic support protocol [12] enables complete networks to roam among different access networks, without disrupting network nodes' ongoing sessions and without requiring any specific mobility capability in the hosts. Nevertheless, it has some important limitations in terms of performance, due to the increased path length and the packet overhead that this solution introduces. Such limitations trigger the need for what has been called route optimization (RO) for NEMO. These approaches try to overcome some of the limitations of the basic solution currently defined for NEMO [12].

This paper presents a RO solution called Mobile IPv6 (MIPv6) route optimization for NEMO (MIRON). An initial version of MIRON was presented in ASWN 2004 [13]. This paper represents many refinements and extensions to our original work from ASWN 2004, extending the scope of the original solution and providing significant contributions to the work presented in [13], not only in the design and scope of the protocol, but also performing an important practical evaluation, based on an implementation. MIRON enables direct communication between nodes belonging to a mobile network and other nodes of the Internet. MIRON is composed of two main modes.

- For those nodes of the mobile network that do not have any mobility capability, the mobile router (MR) performs all the RO and mobility tasks on their behalf (what some authors [14] have called *Proxy-MR*).
- For those nodes and (mobile) routers with standard MIPv6 support, an address delegation mechanism, based on protocol for carrying authentication for network access (PANA) [15] and DHCP [3], provides these nodes with topologically meaningful addresses (i.e., addresses that are directly reachable without requiring special rendezvous points, such as home agents (HAs), to be deployed to reroute any packet towards the actual location of the node). This enables these nodes to manage their own mobility and to perform the RO by themselves.

These two different key modes of operation of MIRON combined give as a result a complete RO solution for mobile networks, enabling traffic from any kind of node (with and without mobility support), and network configuration (including nesting) to be optimized. This is achieved without requiring changes on the operation of any node except the MRs.

This paper is structured as follows. A brief summary of the basic concepts of NEMO and an introduction to PANA

are described in Section II, as well as the motivation for RO. Section III provides a detailed description of MIRON. Section IV presents a performance evaluation of MIRON and compares it with the NEMO basic support protocol, by means of real-life experiments, as well as analytical studies. In Section V, we explore different alternatives for RO in NEMO and compare them with MIRON. Finally, Section VI concludes this paper.

II. Background and Motivation

This section summarizes some of the concepts, terminology, and related protocols that are used along the paper, as well as the motivation for the necessity of RO solutions for NEMO. A brief description of network mobility and the NEMO basic support protocol [12] is provided first. A more detailed, but still summarized, description of PANA is provided afterwards, as this is a novel protocol that is used as part of our proposal.

A. Network Mobility

Users demand Internet access not only from fixed locations (e.g., at home, at work, in hotels, cafeterias, universities, etc.) but also in public transportation systems (e.g., planes, trains, and buses). In order to satisfy such demands, the technical community worked on the design of the required protocols to provide network mobility support. In particular, a working group called NEMO was created within the IETF[1] to extend the basic end-host mobility support protocol, Mobile IP [4], [5], to provide network mobility support [12].

In the IETF NEMO solution, a mobile network (known also as Network that Moves—NEMO[2]) is defined as a network whose attachment point to the Internet varies with time. The router within the NEMO that connects to the Internet is called the MR [16]. It is assumed that the NEMO has a home network where it resides when it is not moving. Since the NEMO is part of the home network, the mobile network has configured addresses belonging to one or more address blocks assigned to the Home Network: the mobile network prefixes (MNPs). These addresses remain assigned to the NEMO when it is away from home. Of course, these addresses only have topological meaning when the NEMO is at home. When the NEMO is away from home, packets addressed to the mobile network nodes (MNNs) will still be routed to the home network. Additionally, when the NEMO is away from home, i.e., it is in a visited network, the MR acquires an address from the visited network, called the care-of address (CoA), where the routing architecture can deliver packets without additional mechanisms.

The goal of the network mobility support mechanisms [17] is to preserve established communications between the MNNs and external correspondent nodes (CNs) despite movement. Packets of such communications will be addressed to the MNNs addresses, which belong to the MNP, so additional mechanisms to forward packets between the home network and the NEMO are needed. The basic solution for network mobility support [12] essentially creates a bidirectional tunnel between a special node located in the home network of the NEMO (the HA), and the CoA of the MR.

This solution is quite similar to the solution proposed for host mobility support, MIPv6 [5], without including the RO support. Actually, the protocol extends the existing binding update (BU) message to inform the HA of the IP address of the NEMO side of the tunnel (i.e., the CoA of the MR), through which the HA has to forward the packets addressed to the MNP. A new BU option is also defined to convey information about the MNPs.

[1]http://www.ietf.org/.

[2]NEMO can mean NEtwork MObility or NEtwork that MOves according to the context.

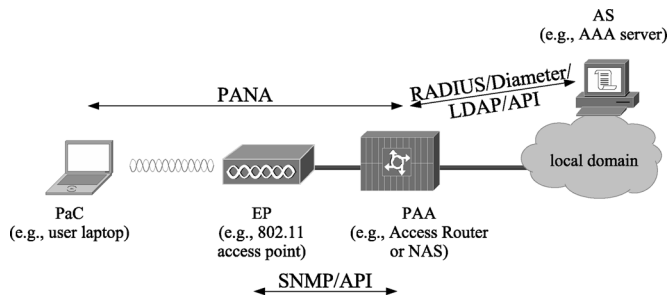

Fig. 1. PANA functional model overview. Some entities can be also collocated on a same physical node.

B. Network Authentication and Access Control: PANA

Nowadays, most of the public wireless access networks deploy some authentication and access control mechanisms in order to avoid unauthorized clients gaining access to the network. Nevertheless, these mechanisms are either limited to specific access media technologies (e.g., 802.1X for IEEE 802 links) or based on proprietary solutions (e.g., web access-based authentication methods) [18]. This fact, together with the expectation that future mobile devices will have several access technologies to gain network connectivity, triggered the creation of a new working group within the IETF, called PANA, aimed at the definition and specification of a standard network-layer solution for authenticating clients for network access.

The PANA protocol [15], [19] is designed to facilitate authentication and authorization of clients in access networks. Basically, it is a link-layer agnostic network access authentication protocol—encapsulating extensible authentication protocol (EAP) [20] authentication methods—that runs between an entity (called PANA Client, PaC) in a node that wants to gain access to the network and an agent (called PANA authentication agent, PAA) in a server on the network side [15]. PANA is responsible for enabling the authentication process between these two entities, but it is just a part of the overall process of authentication, authorization and accounting (AAA) and access control. The complete picture, with AAA and access control functions, comprises four entities (Fig. 1).

- PANA client (PaC). Entity residing in the node that requests network access and implements the client part of the PANA protocol.
- PANA authentication agent (PAA). Entity implementing the server part of the PANA protocol that interacts with the PaCs for authenticating and authorizing them to access the network. The PAA consults the authentication server (AS) in order to verify the credentials and rights of a PaC and

also updates the access control state, such as filters, in the Enforcement Points (EPs) in the network. The PAA usually resides in the network access server (NAS) node, but it can be hosted in any node that is in the same subnet (within one-hop distance) as the PaC.
- Authentication server (AS). Server-side entity in charge of verifying the credentials of a PaC requesting access (sent by the PAA on behalf of the PaCs).
- Enforcement point (EP). Entity implementing the access control function by allowing access to authorized clients and preventing access from others.

PANA is a UDP-based protocol [19], consisting of a series of requests and responses. Each message can carry zero or more attribute value pairs (AVPs) as payload. The main payload of PANA is EAP, which is responsible for performing authentication (PANA just helps the PaC and PAA establish an EAP session). Messages are sent between PaC and PAA as part of a PANA session, that consists of five different phases.

1) Discovery and handshake phase. This phase starts the PANA session. The PaC discovers the PAA(s) by either explicitly soliciting advertisements to the PAA(s) or receiving unsolicited advertisements. The PaC's answer, sent in response to an advertisement, starts a new session.
2) Authentication and authorization phase. EAP execution between the PAA and PaC, by carrying an EAP method inside the EAP payload.
3) Access phase. If the authentication and authorization phase is successful, the host gains access to the network and can send and receive IP data traffic through the EP(s).
4) Re-authentication phase. This phase is usually initiated by the PAA before the session lifetime expires (carrying EAP to perform authentication), although this phase may be triggered by either the PaC or PAA regardless of the session lifetime.
5) Termination phase. The PaC or the PAA may choose to discontinue the access service at any time, by sending an explicit disconnect message.

C. Route Optimization (RO)

The NEMO basic support protocol [12] has the following limitations, due to the fact that packets of MNNs' communications traverse—in both directions—the MR's HA, through the MR-HA bidirectional tunnel.

- It forces suboptimal routing (known as angular or triangular routing), i.e., packets are always forwarded through the HA following a suboptimal path and therefore adding a delay in the packet delivery.
- It introduces non-negligible packet overhead, reducing the path MTU (PMTU). Specifically, an additional IPv6 header (40 bytes) is added to every packet because of the MR-HA bidirectional tunnel.
- The HA becomes a bottleneck of the communication as well as a potential single point of failure. Even if a direct path is available between a MNN and a CN, if the HA (or the path between the CN and the HA or between the HA and the MR) is not available, the communication is disrupted.
- These problems are exacerbated when considering nested mobility (i.e., a mobile network gains connectivity through other mobile networks), since in this case the packets are forwarded through all the HAs of all the upper level mobile networks involved (known as multiangular or pinball routing). This is because each sub-NEMO obtains a CoA that belongs to the MNP of its parent NEMO. Such a CoA is not topologically meaningful in the current location, since the parent NEMO is also away from home, and packets addressed to the CoA are tunnelled—thus increasing packet overhead—to the HA of the parent NEMO.

Because of all the limitations identified above, it is highly desirable to provide RO support [14], [21], [22] for NEMO that enables direct packet exchange between a CN and a MNN without passing through any HA and without inserting extra IPv6 headers. In MIPv6 [5], the RO is achieved by allowing the mobile node (MN) to send BU messages also to the CNs. In this way the CN is also aware of the CoA address where the MN's home address (HoA) is currently reachable. The return routability (RR) procedure is defined to protect a CN to change the IPv6 destination address (using the MN's CoA) of packets addressed to the MN's HoA [23].

III. MIRON: MIPv6 RO for NEMO

In this section, we present a novel solution that provides RO for NEMO, enabling direct path communication between any kind of MNN and a CN in the Internet. An overview of the protocol is first provided, before describing in detail how the proposed solution works.

A. Protocol Overview

MIRON aims at improving the overall performance of communications involving nodes within a NEMO, by both avoiding data packets passing through the MR's HA and reducing the packet overhead due to the additional IPv6 headers introduced by the NEMO basic support protocol. MIRON does not introduce any change on the operation of the CNs and the MNNs, but only of the MRs.

Fig. 2 shows a possible RO target scenario for MIRON. It considers a mobile network deployed in a train, consisting of different types of MNNs.

- *Fixed nodes* in the train—without mobility support, called local fixed nodes (LFNs) [16]—, such as internal servers or passengers' laptops.
- *Mobile devices*—called visiting mobile nodes (VMNs)—such as passengers' laptops, running MIPv6, that keep using their Home IPv6 Addresses.
- Nested mobile networks, such as personal area networks (PANs), e.g., a passenger's laptop, acts as a MR of his devices and is connected to the train's MR.

All of these devices access the Internet through the train's MR. This scenario includes almost every possible mobile network communication, involving LFNs, VMNs, and nested NEMOs. Fig. 2 also shows the different components every entity is composed of. Both the components and the way they

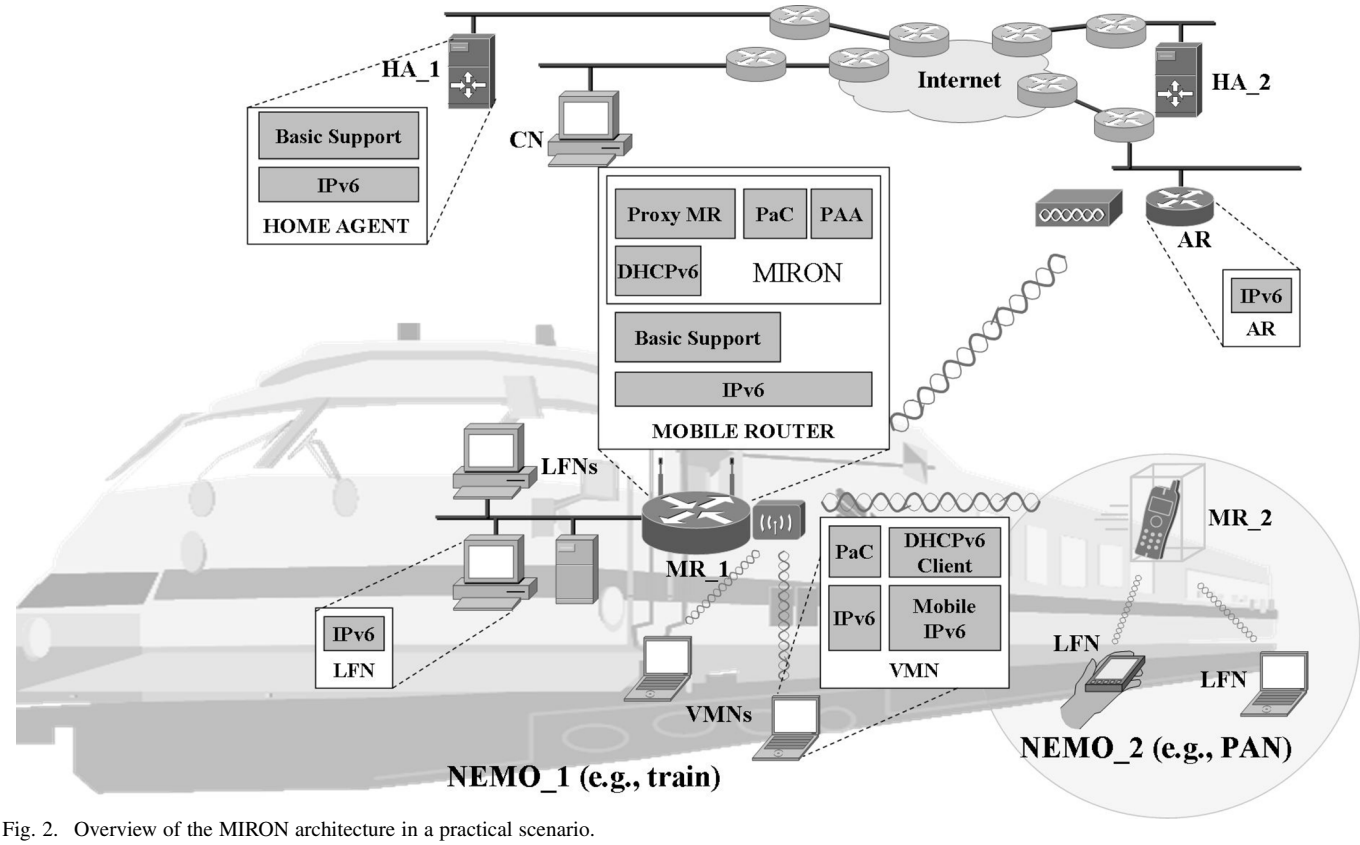

Fig. 2. Overview of the MIRON architecture in a practical scenario.

work together to construct a complete RO solution will be described in detail later in this section.

MIRON addresses two different RO aspects.

- *Angular routing*. Angular routing is caused by the MR-HA bidirectional tunnel introduced by the NEMO basic support protocol, since packets of a communication involving a MNN have to be forwarded through the HA of the NEMO. MIRON addresses this problem in two different ways, depending on whether the MNN that is communicating with a CN has mobility support or not. If the MNN has no MIPv6 capabilities (i.e., an LFN), the approach followed by MIRON consists in delegating the RO functionality to the MR, that performs all the RO signaling and packet handling on behalf of the LFNs. Therefore, the MR is a kind-of "Proxy-MR" [14] for the LFNs of the NEMO. On the other hand, if the MNN is a MIPv6 MN (i.e., a VMN) that is visiting the mobile network, MIRON takes advantage of the already available mobility support that the MN has. In this case, by using PANA and DHCPv6, the MR provides a topologically meaningful IPv6 address (that is, an address belonging to the network that the MR is visiting) to every VMN attached to the NEMO and updates it every time the NEMO moves. This, in addition to a routing mechanism that enables these addresses to be routed inside the NEMO, allows the VMN to make use of its own MIPv6 RO functionality, therefore avoiding traversing the HA and reducing the packet overhead.
- *Multiangular routing*. Multiangular routing is caused in nested NEMOs by the chain of nested MR-HA bidirectional tunnels that packets should traverse. MIRON addresses this problem by using PANA and DHCPv6 to provide topologically meaningful IPv6 addresses to every MR in the nested NEMO hierarchy. In this way, every MR has an IPv6 address belonging to the network that the root-MR (that is, the MR of the NEMO at the top of the hierarchy) is visiting. This, in addition to a routing mechanism that enables these addresses to be reachable, makes it possible to avoid traversing any HA.

The set of mechanisms of MIRON enables direct path communication between a MNN (LFN or VMN) and a CN, avoiding the suboptimal MR-HA path. The recursive tunneling due to nesting is also eliminated, therefore optimizing the traffic in every possible configuration of a mobile network. MIRON only introduces changes in the MR (see Fig. 2), while MNNs, HAs, and CNs remain unchanged, thus facilitating the deployment of the solution. The next sections provide a detailed protocol walkthrough of MIRON.

B. Angular RO

If no RO mechanism is used, all the traffic sent/directed to a MNN goes through the bidirectional tunnel set up between the MR and its HA. MIRON enables direct communication—without traversing the MR's HA—by following one of the next approaches, depending on the type of MNN.

- Local fixed node (LFN). LFNs do not have mobility support, so any mechanism that attempts to optimize their traffic should be implemented without requiring support from the LFN itself. The MIRON mechanism for LFNs is basically a Proxy-MR approach, in which the MR performs the MIPv6 RO [5] on behalf of the LFN.

- Visiting mobile node (VMN). VMNs are MNs that are visiting the mobile network, managing their own mobility. By default, the CoA obtained and used by a VMN attached to a NEMO belongs to the MNP of that NEMO, so although these MNs may be performing RO with the CNs they are communicating to, there still exists a tunnel—between the NEMO's MR and the MR's HA—introduced by the NEMO basic support protocol. In this case, our Proxy-MR approach is not feasible, therefore a different mechanism is used. MIRON takes advantage of the mobility support that VMNs already have. Basically, we propose a mechanism, using PANA and DHCPv6, that enables the VMNs to configure topologically valid IPv6 addresses (i.e., those addresses that belong to the address space of the foreign network the NEMO is visiting) as CoAs, and letting the VMNs manage their mobility and RO tasks.

1) Detection of the Type of Node: In order to apply the appropriate RO mechanism, the MR should first be able to determine which kind of node (LFN or VMN) every node that is communicating is. The MR performs such a task by looking for BU messages received at its ingress interfaces, since an MN right after gaining connectivity to a foreign network and configuring a new CoA (from the MNP), has to send a BU to its HA to inform it about its new location (i.e., MN's CoA).

2) RO Mechanism for LFNs: LFNs are nodes without any mobility support running, therefore a mechanism that optimizes their traffic cannot relay on any mobility function implemented by them. MIRON puts this LFN mobility support into the MR, that performs all the required mobility and RO tasks on behalf of the LFNs attached to it.

The mechanism basically consists in enabling a MR to behave as a proxy for the LFN, performing the MIPv6 RO signaling and packet handling [5] on behalf of the LFN. In order to do that, the MR first tracks the different communications that LFNs have established and decides which of those will be optimized, since optimizing a traffic flow involves a cost—in terms of signaling and computation resources at the MR—that may not be worth for some kinds of flows (e.g., DNS queries). This decision (that is, whether to perform RO for each flow or not) is out of the scope of this paper, although we are working on different algorithms and heuristics to evaluate their performance based on real tests.

For those LFN-CN pairs whose traffic is to be optimized, the MR starts to send the RO signaling described for standard MIPv6 in [5].

- The BU is sent by the MR.
- The BU contains the LFN's address as the HoA and the MR's CoA as the CoA (since the MR's CoA is the only topologically meaningful address available).

The RO mechanism defined by MIPv6 [5] requires an additional procedure to be performed before sending the BU message, in order to mitigate possible attacks [23]. Basically, this mechanism, called return routability (RR), verifies that the node that is reachable at the HoA is able to respond to packets sent to a given CoA (different to the HoA of the node). This mechanism can be deceived only if the routing infrastructure is compromised or if there is an attacker between the verifier and the addresses (that is, HoA and CoA) to be verified. With these exceptions, the test is used to ensure that the MN's HoA and MN's CoA are collocated.

In our solution, we adopt the procedure described above. For this purpose, the MR has to perform the MIPv6 RR procedure [5] on behalf of the LFN. Such procedure involves sending the home test init (HoTI) and care-of test init (CoTI) messages to the CN and processing the replies (home test message HoT—and care-of test message—CoT). These messages are sent as specified in [5], using the LFN's address as the source address in the HoTI message—which is sent encapsulated through the MR's HA, and the MR's CoA as the source address in the CoTI message. With the information contained in the HoT and CoT messages, sent by the CN in response to the HoTI and CoTI messages, respectively, the MR is able to build a BU message to be sent to the CN on behalf of the LFN. This message is sent using the MR's CoA as the packet source address and carries a HoA destination option set to the LFN's address.

Besides performing the RO signaling on behalf of the LFN, the MR has to process the packets sent by and directed to the LFN. Packets sent by the CN follow a direct path to the MR, not traversing the HA, as a result of the RO. These packets carry the MR's CoA as destination address, and also carry a Type 2 routing header with the LFN's address as next hop. The MR processes and removes the routing header of the packet, checking if the next hop address belongs to one of its LFNs and, if so, delivering the packet to the LFN. Current MIPv6 specification [5] defines that IPv6 nodes which process a Type 2 routing header must verify that the address contained within is the node's own HoA. This is done in order to prevent packets from being forwarded outside the node. In MIRON this has been changed and the MR verifies that the address contained in the routing header is the address of one of the LFNs that the MR is acting as Proxy-MR. In the opposite direction, the MR receives the packets sent by the LFN and performs the following actions on every packet.

- Set the MR's CoA as IPv6 source address.
- Insert an IPv6 HoA destination option, carrying the address of the LFN.

Fig. 3 shows the signaling and data flows of the proposed RO mechanism for LFNs, including at the top of the figure the NEMO basic support protocol data flow for comparison purposes.

From the security point of view, allowing the MR to perform some operations on behalf of the LFNs attached to it does not introduce any threat, because LFNs trust their MR for the routing of all their traffic. From the architectural point of view, the solution is also natural, as the RO support defined by MIPv6 [5] conceptually could be implemented in multiple boxes. MIRON just applies this mechanism, by dividing the functionalities among two different physical boxes, but actually the conceptual basis of the solution is the same as the one defined in [5].

It may be argued that an attacker may induce the MR to initiate the RO procedure with a large number of CNs at the same time, by sending to an LFN of the NEMO a spoofed IP packet (e.g., ping or TCP SYN packet) that appears to come from a new CN. MIRON shares this and others vulnerabilities of MIPv6 [23], but the solutions proposed to mitigate these attacks in [23] are also applicable to MIRON. For example, to

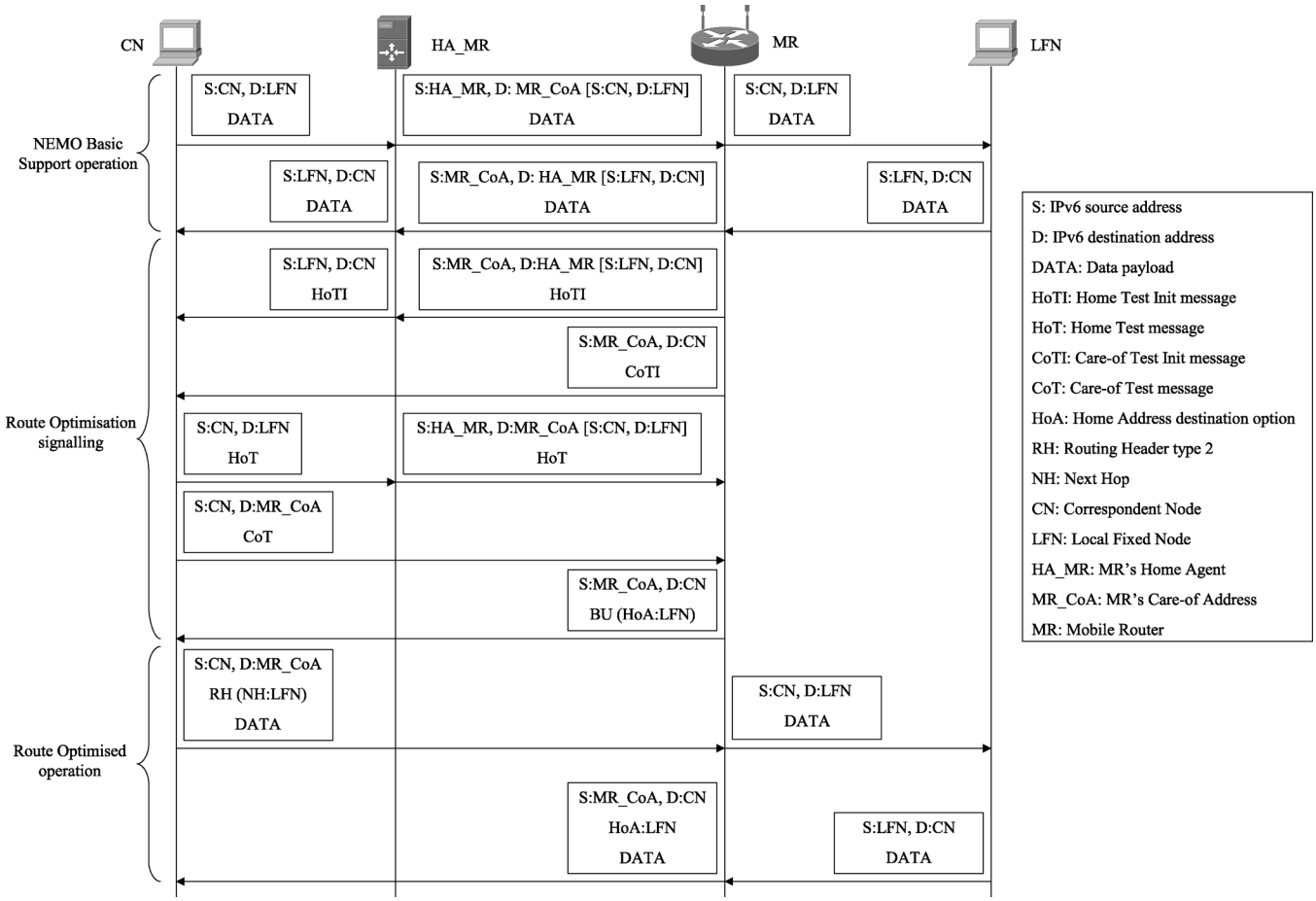

Fig. 3. RO mechanism for LFNs: Proxy-MR operation.

avoid bringing down the MR by making it send unnecessary BUs (after performing the complete RR procedure), the MR should apply some local policies [23], such as the following.

- Setting a limit on the amount of resources (i.e., processing time, memory, and communications bandwidth) that it uses for the *Proxy-MR* functionality. In this way, when the limit is exceeded, the MR may decide to stop initiating the RO procedure for new CN-LFN communications, following the plain NEMO basic support protocol operation for those.
- The MR may also recognize addresses with which an LFN had meaningful communication in the past and only start the RO procedure to those addresses.

Reference [23] proposes additional mechanisms for a MN to avoid attacks regarding to RO. Most of them may also be considered by a MR implementation that provides MIRON capabilities.

3) RO Mechanism for VMNs: VMNs are nodes that support mobility (that is, nodes running MIPv6 [5]) and are visiting a mobile network. Therefore, the VMN is attached to an access router that is the NEMO's MR, and the address that the VMN obtains and configures as CoA belongs to the MNP. In this case, our Proxy-MR mechanism used for LFNs cannot be used, as the VMN itself may generate RO signaling with its CNs. Besides, the MR cannot modify the RR and RO signaling sent by the VMN in order to make the MR's CoA the CoA that the CN uses to send the packets to the VMN, because part of the RR signaling is protected by IPsec (the HoTI message is sent through the VMN's HA protected by IPsec ESP).

The RO approach that MIRON defines for this type of node is based on taking advantage of the mobility support that these nodes already have, providing the means to the VMN to perform the RO. In order to allow the VMN to manage its own mobility and enable it to perform RO with the CNs (in a way that avoids the MR-HA bidirectional tunnel), we propose the following.

- Provide a topologically meaningful IPv6 address to the VMN. These addresses are those that belong to the network that the root-MR is visiting.
- Enable this address to be routable inside the NEMO, as it only has topological meaning in the visited network. The MR has to perform proxy neighbor discovery for this address in the egress interface that is attached to the network to which the address belongs. Besides, the MR has to insert a host route for this address to be able to route packets destined to it.
- Perform source address routing in the MR in order to send directly (that is, avoiding the bidirectional MR-HA tunnel that still exists and is used for nonoptimized traffic) packets sent by the VMN.
- Update the address of the VMN when the NEMO moves.

A mechanism that fulfils the previous goals should be able to allow VMNs, and only the VMNs—the mechanism must not affect other type of nodes—to obtain a new IPv6 address to be

used as the CoA, whenever the MR wants to, and in a secure way that does not introduce any new security threat.

The RO mechanism for VMNs that we propose in this section uses a particular functionality that is included in the PANA protocol, namely, the capability of telling a node that it must change its IPv6 address and how to get a new one.

This imposes the requirement that PaC software must be available in VMNs for providing them RO, and PaC and PAA software must be available in MRs. The PaC software in the MRs is needed to optimize nested NEMOs as will be described in next subsection. The PAA software in MRs is needed to support the RO for VMNs visiting the NEMO, and to support the RO of nested NEMOs. PANA support is not required by MIRON in the access network that the root-MR is visiting (in the infrastructure access network) nor in the LFNs in the NEMO.

The assumption of availability of PANA software in the MRs is not a problem, because MIRON is based on modifications in the MRs software, PANA is just an additional software to have. The assumption of PANA in VMNs can be more restrictive. The idea of the solution is that MIPv6 compliant MNs can visit the NEMO and optimize its routing just like when they visit an infrastructure access network. This will not be true if they do not have a PANA client installed.

Most of current access networks (such as hotspots deployed in airports and cafeterias) require users to authenticate to the network before gaining Internet access. As the number of hotspots continues growing in the coming years, authentication mechanisms will be more and more important in order to avoid nonauthorized users using and wasting the network resources. Using a standard protocol to perform such authorization and authentication tasks would help in the deployment of ubiquitous access "anytime anywhere" networks. Our RO protocol, MIRON, assumes that: 1) an authentication protocol will be used in public heterogeneous access networks and that 2) PANA [15], [18], [19] will be a standard protocol widely deployed and used, so PANA support will be available in VMNs.

We argue that assuming that VMNs will have PaC software does not limit the practical usability of MIRON for RO in VMNs, since, on one hand, it is not realistic to assume public access networks to be open and not to require any kind of authentication. On the other hand, we assume that PANA support will be available on VMN, because it is expected that PANA will become a standard authentication protocol once its specification is concluded within the IETF, finishing with the current status of multiple possible authentication mechanisms (e.g., IEEE 802.1X, proprietary web-based systems, etc.).

Even if that is not finally the case, and PANA does not turn to be the standard authentication protocol in heterogeneous networks, a different protocol that is able to provide IPv6 routable addresses to arriving VMNs and change them every time the NEMO moves, could be alternatively used. One example could be the use of the DHCPv6 *reconfigure* mechanism [3], using some authentication information between MR and VMN obtained from any other means to authorize the MR changing the IPv6 address used by the VMN.

Anyway, if nor PANA nor an alternative protocol is available in a VMN, this VMN—attached to a MIRON MR—will just not benefit from the RO mechanism provided by MIRON, and its traffic will follow the suboptimal path provided by the NEMO basic support protocol.

The mechanism to provide an IPv6 address to the VMN using PANA works as follows (see Fig. 4): when a VMN attaches to a NEMO, it initiates the PANA session (PANA discovery and handshake phases). Immediately after that, the actual authentication and authorization phase (by executing EAP between the PAA and PaC) takes place. The VMN is then authorized to access the network and it has an IPv6 address. This address is obtained by using the address autoconfiguration mechanism available at the NEMO. Initially, we assume that we are using stateless address configuration for addresses of the MNP, but later we will see that we can also use stateful address configuration within the NEMO. The VMN then sends a BU message to its HA, informing about its current location. Once that this BU is received at the MR, it then becomes aware that a new VMN is now attached to the NEMO. The MR discards this BU message and starts a PANA reauthentication phase.

During the PANA reauthentication phase, the PAA located in the MR tells the PaC located in the VMN that it should obtain and configure a new IPv6 address (post-PANA address, POPA) and how to obtain it, by including available configuration methods in a post-PANA-address-configuration (PPAC) AVP contained in a PANA message (PANA-bind-request). DHCPv6 is the only available configuration mechanism listed in the message, and upon the reception of that, the VMN requests an address using DHCPv6. There is a DHCPv6 component located at the MR that receives the DHCPv6 requests from the VMN and then obtains (using one of the available autoconfiguration mechanisms at the foreign network) an IPv6 address. The DHCPv6 component generates a DHCPv6 reply—including this address—that is delivered to the requesting VMN. This DHCPv6 component implements the client part of DHCPv6 and also some reduced functionalities of the server part (e.g., the generation of DHCPv6 responses), but it is not a DHCPv6 server (for example, the DHCPv6 component does not have a pool of available addresses, each time an address is needed, it obtains it from the foreign network), although the implementation of this DHCPv6 component can be very easily performed from the code of a normal DHCPv6 client and server implementation. Once the MR has sent the DHCPv6 reply—including the (/128) delegated address—to the VMN, the PaC in the VMN conveys this newly configured IPv6 address to the PAA in the MR by sending the PANA-update-request message.

The use of stateful address configuration (DHCPv6) within the NEMO (to configure addresses from the MNP) is also possible, but it requires the DHCPv6 component at the MR to implement the complete server functionality and to check, before providing an address, if the requesting node is an identified VMN or not, to know whether this address should belong to the MNP or to the visited network address space. Nodes are identified as VMNs at the MR according to the procedure described above.

In order to enable the VMNs' addresses reachability inside the NEMO, the MR has to add a host route for each VMN's address and perform proxy neighbor discovery on its egress interface (the interface that is connected to the link where the ad-

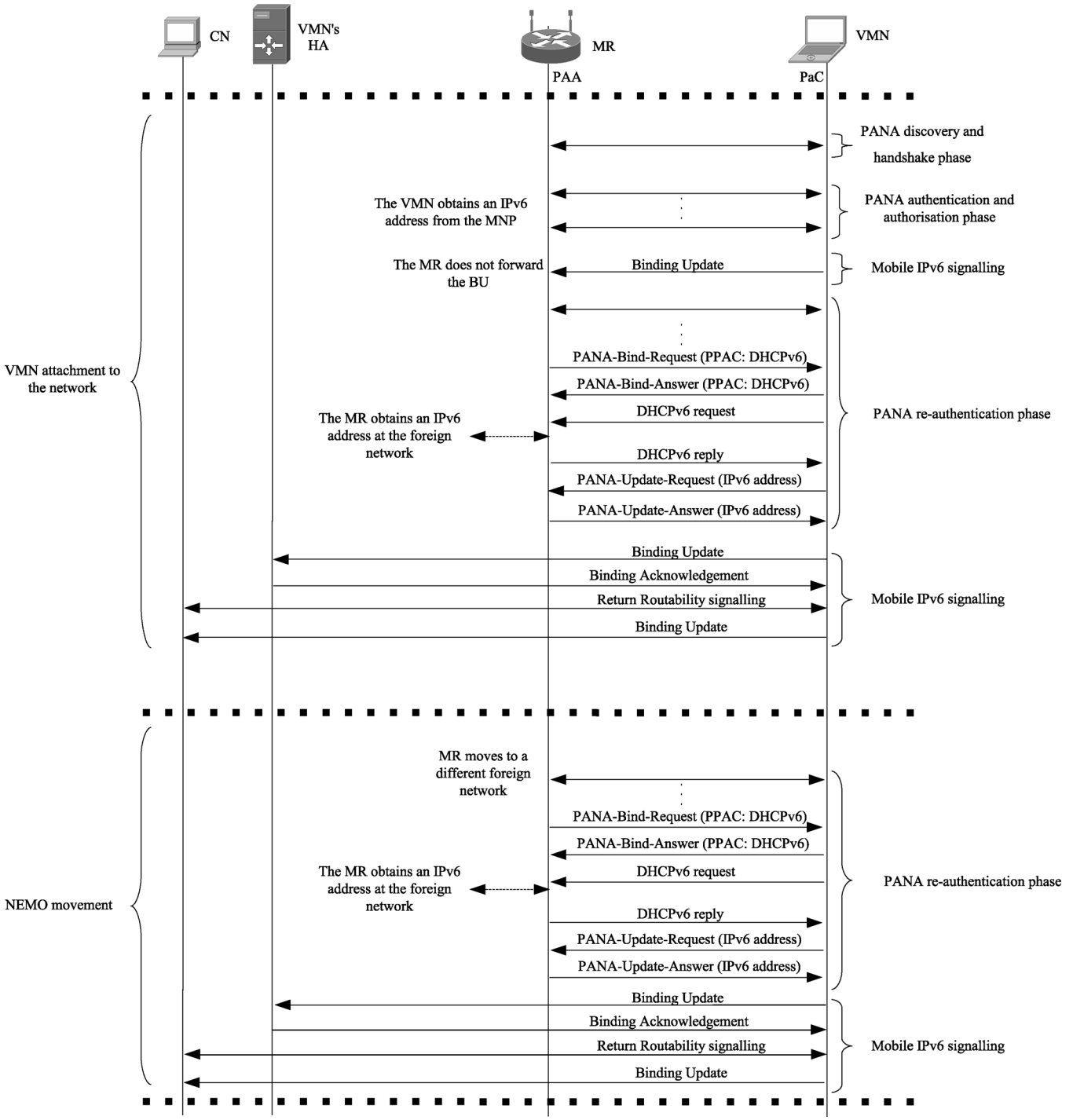

Fig. 4. RO mechanism for VMNs.

dress has topological meaning), allowing the MR to forward packets to their final destinations. Both the delegated IPv6 addresses and the host routes have a lifetime that prevents this state to remain in the network after a sub-NEMO or a node leaves a parent-NEMO (the value depends on the lifetime of the address obtained by the root-MR).

The VMN, triggered by the change of address, starts the MIPv6 location update process, sending first a BU message to its HA. The VMN may then update the location information in the CNs it is communicating with (if the VMN is running RO with its CNs). This process consists of the VMN performing the RR process [5] and sending a BU to every CN whose traffic is to be route optimized.

When the NEMO moves to a different foreign network, the MR requests new IPv6 addresses and provides them to the VMNs attached to the NEMO by starting a new PANA reauthentication phase. The MR requests VMNs to configure a new IPv6 address using DHCPv6.

Due to the PANA and DHCPv6 signaling, MIRON takes a longer time to finish its handover than that in NEMO basic sup-

port. Similarly to the case of MIPv6, micromobility solutions such as fast handovers for MIPv6 [6], may be designed/adapted to MIRON to alleviate the increase in the handover delay [24].

C. Multiangular RO

The routing inefficiencies due to the MR-HA bidirectional tunnel are exacerbated when NEMOs are attached to other NEMOs, forming a nested NEMO. Packets belonging to a communication between a MNN of a nested NEMO and a CN have an additional IPv6 header per nesting level and traverse the HAs of every MR of the nested NEMO.

The problem of enabling RO for nested NEMOs (i.e., MRs visiting a NEMO) is very similar to that of VMNs (i.e., MNs visiting a NEMO). Both VMNs and MRs are nodes that are mobile-capable and can manage their own mobility. Routing inefficiencies arise from the fact of not using topologically meaningful addresses (i.e., addresses belonging to the NEMO MNP) as CoAs. Section III-B3 describes an address delegation mechanism with a built-in routing system that is able to provide IPv6 addresses—belonging to the foreign network that the MR is visiting—to a VMN in a secure way, by using PANA facilities.

MIRON extends that solution, used for providing angular RO for VMNs, to enable multiangular RO in nested NEMOs. Basically, the solution consists in providing topologically meaningful addresses—that is, those that belong to the foreign network that the root-MR is visiting—to every MR in the nested NEMO. The same PANA-with-DHCPv6-based mechanism is used to provide an IPv6 address to a MR that attaches to a NEMO (and to change it when one of the parent NEMOs moves). MRs have both a PAA and a PaC component and also a DHCPv6 component, so when a MR connects to a mobile network, they are able to get and configure a new IPv6 address.

Providing topologically meaningful addresses is not the only required step to avoid the suboptimal multiangular routing in nested networks. Another requirement that needs to be met is that these addresses are globally reachable. To enable that, every MR in the nested NEMO keeps track of the address of the node requesting an IPv6 address using DHCPv6, so when the delegated address is received, it can insert a host route entry in its routing table that allows it to route packets destined to that address afterwards. This information is also used to perform source address based routing for the packets generated inside the NEMO, as every MR should know for each packet if it has to be sent directly to the router it is connected to (this way, avoiding the tunnel), or it has to be sent towards the HA, through the bidirectional tunnel (for traffic that is not being optimized).

This address delegation mechanism with built-in routing avoids the multiencapsulation and multiangular routing in nested networks. Besides, it enables angular MIRON ROs to work when applied to a NEMO located in any level of a nested NEMO.

IV. Evaluation of MIRON

This section provides both an experimental and analytical evaluation of MIRON. The main aim of this evaluation is to study the performance of MIRON and compare it with the NEMO basic support protocol.

A. Experimental Evaluation

1) MIRON Implementation: In order to be able to conduct real experiments that allowed us to evaluate the performance of the NEMO basic support protocol and the improvements provided by MIRON, we first implemented the NEMO basic support protocol [25]. A first prototype of MIRON was also implemented, providing all the RO mechanisms. Packets belonging to a communication flow optimized by MIRON must not traverse the bidirectional tunnel, so for outgoing traffic a host route towards the CN of the flow should be inserted at the MR to avoid the default route through the tunnel interface. Besides, there may be simultaneously communications in a NEMO—from different MNNs—with the same destination CN that are not all being optimized, thus source address based routing is necessary.

The required additional protocols and procedures (such as the RR and DHCPv6) were completely implemented, with the exception of PANA, that is currently being implemented and integrated. The fact of not having implemented the PANA signaling does not have an impact on the results obtained in the tests, as we have focused in the TCP throughput and PANA signaling is generated during handovers (and also periodically to renew the lifetime). In this paper, we have not been concerned about the performance of our solution during handovers as we address the problem of RO, just in the same way that the RO solution for MIPv6 does. Improvements in the handover latency (like the ones designed for MIPv6 [6], [7], [24]) requires further study and will be addressed in future works.

The NEMO basic support protocol [25] and MIRON were mostly implemented in user space, because in this way the development was easier and quicker than doing that in the kernel. The main software characteristics are: a Linux machine with Kernel Linux-2.6.x (tested with Linux-2.6.8.1) with support for IPv6-in-IPv6 tunnels (used for the HA-MR bidirectional tunnel) and Netlink sockets, and the *pcap* library (used for the capture and processing of the mobility related signaling).

2) Studied Scenarios: Two different scenarios (Fig. 5) were deployed to allow us to experimentally test the performance of MIRON and compare it with the NEMO basic support solution. The first one [Fig. 5(a)] was used to evaluate the performance in a non-nested case, whereas the second [Fig. 5(b)] is an extension of the former to include nesting.

We describe next the second scenario, as it is an extension of the first one. This scenario [Fig. 5(b)] consists of 13 Mandrake 10.0 Linux machines (all with Linux-2.6.8.1 kernels, except three routers that run Linux-2.4.22). Five of them act as *fixed* (i.e., nonmobile) routers (R1 to R5), two as home agents (HA1 and HA2), two as mobile routers (MR1 and MR2), one as CN, one as LFN and two as *fixed* nodes (fixed nodes 1 and 2). This is part of the IST Daidalos[3] project testbed at the Universidad Carlos III de Madrid.

All the mobility-aware nodes run the network mobility software, that is, the NEMO basic support protocol (at the HA and

[3]http://www.ist-daidalos.org/.

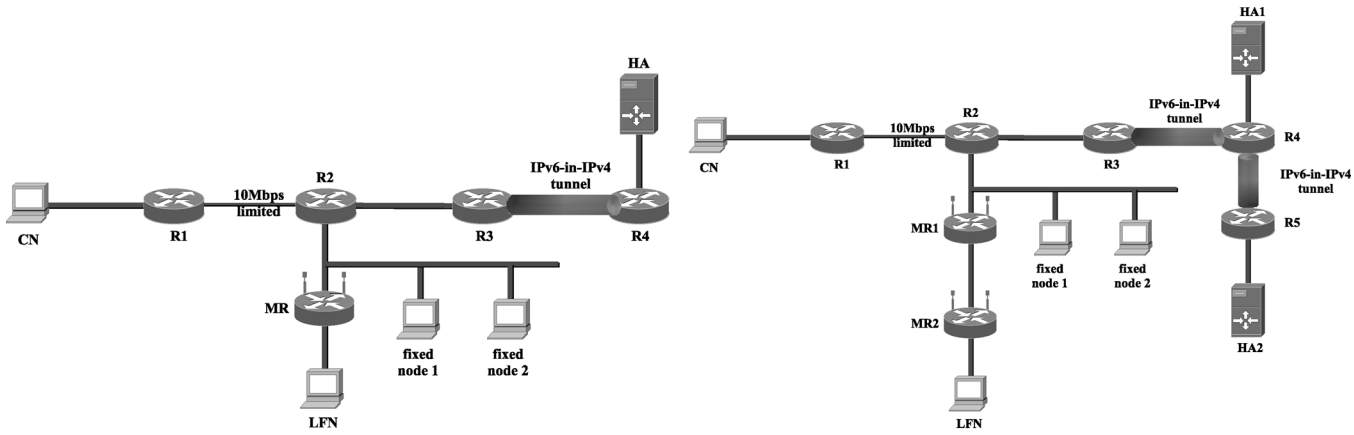

Fig. 5. Network mobility testbed employed during the experimental evaluation. (a) Non-nested scenario. (b) Nested scenario.

MR) and MIRON (at the MR only) developed by us. The CN runs MIPL[4] 2.0 RC2, with the support of RO enabled.

We need the ability to modify the delay in the path followed by packets of a communication between a CN and a MNN (that is, the path between the CN and the MNN's HA and/or the path between the MNN's HA and the foreign network the MR is currently attached to). This allows us evaluate how the performance of a particular network mobility solution is affected by network characteristics, such as the particular location of mobile networks, home networks and CNs. For this purpose, we used the NIST Net emulator.[5] NIST Net allows a single Linux PC, set up as a router, to emulate a wide variety of network conditions (e.g., latency, jitter, packet loss, ...).

We were interested in studying how the delay (and also the packet overhead) introduced by the MR-HA bidirectional tunnel affects the performance of applications. TCP performance is heavily dependent on the round-trip time (RTT) between the communication peers. Taking this into consideration and the fact that 85% of the traffic in the Internet is generated by TCP connections [26], the TCP study case becomes very interesting to be performed and analyzed. Therefore, we set up an scenario that allowed us to modify the delay in the CN-HA-MR path.

Other network characteristics, besides the delay, that do not have an special effect in the TCP performance and that are also present in nonmobile networks, were not modified.

NIST Net software runs only in IPv4 and with Linux-2.4.x kernels. Therefore, in order to use it in our testbed, we had to set up an IPv6-in-IPv4 tunnel—between R3 and R4 and between R3 and R5—for use in our IPv6 scenario. In the first, non-nested scenario setup [Fig. 5(a)], every packet in the CN-HA-MR path traverses the IPv6-in-IPv4 tunnel, which allows us to modify the network behavior by changing the parameters of the NIST Net emulator running in R3 and R4. In the rest of the path followed by packets, native IPv6 is used, so the tunnel inclusion does not affect the overall test performance except for the small added delay due to IPv6-in-IPv4 tunneling and the reduction of the PMTU (the situation is not different from having a change of the transport link technology in the path and it is transparent to the IPv6 behavior). Actually, the IPv4 tunnel clearly shows the current status of IPv6 networks in the Internet, with lots of IPv4 clouds connecting IPv6 native networks. In the second, nested scenario, a second IPv6-in-IPv4 tunnel was set up—between R4 and R5—to allow us to modify the network delay between the two different home networks (i.e., between HA1 and HA2).

To avoid the influence of the wireless media characteristics and interferences from other neighboring wireless networks, the performance tests were conducted using wired MRs, although experiments using wireless mobile networks were also performed to check the correctness of our solution in a more realistic scenario.

3) Impact of network mobility on the TCP Performance: The suboptimal routing introduced by the NEMO basic support protocol [12] makes packets not follow the direct CN-MR-MNN path, but the usually longer CN-HA-MR-MNN path. This adds a delay in the packet delivery that can significantly reduce the performance of certain applications. Furthermore, packets are encapsulated between the HA and the MR, thus reducing the PMTU. Both effects, increased delay and reduced PMTU, have an impact in the performance of applications.

TCP is the predominant type of traffic in the Internet nowadays [26], so analyzing how the network mobility support impacts the TCP throughput is important in order to evaluate the cost in terms of performance if users access the Internet through a mobile network. Both the NEMO basic support protocol and MIRON solution are tested for the purpose of comparing them and justifying the need for a RO solution that mitigates the poor performance of the basic solution.

The test consists of measuring the average TCP throughput of an MNN (in the tests, an LFN) downloading a file located at a CN, while two other nonmobile network hosts (fixed nodes 1 and 2), attached to the same network the NEMO is visiting, simultaneously download the same file, both in a non-nested and in a nested scenario [see Fig. 5(a) and (b)]. The available bandwidth between the CN and the network that the mobile network is visiting was limited to 10 Mb/s, by setting the R1–R2 link to 10 Mb/s half-duplex. The tool used for the download was *scp* (secure copy) and the size of the file was 50 MBytes.

Each average TCP throughput sample was calculated over a 20 s independent interval of download and at least 30 samples

[4]MIPv6 for Linux, available at http://www.mobile-ipv6.org/.

[5]http://www-x.antd.nist.gov/nistnet/.

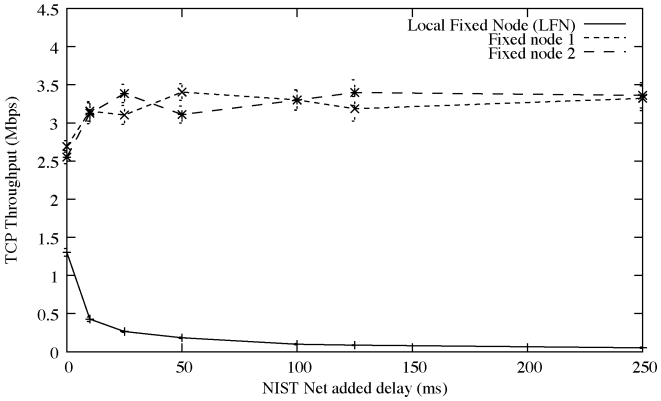

Fig. 6. Impact of NEMO basic support protocol on the TCP throughput.

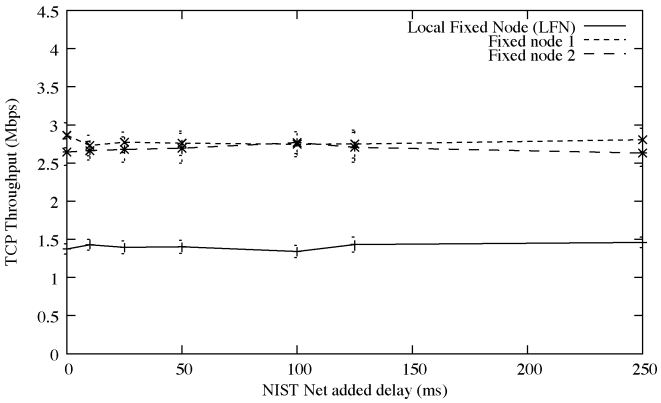

Fig. 7. Impact of MIRON on the TCP throughput.

were obtained for each test (to guarantee the statistical validity of the measurements).

For the non-nested scenario, the unidirectional NIST Net added delay of the link R3–R4—*delay1*—was varied between 0 ms (i.e., home network, visited network, and CN locate very close each other) and 250 ms (this value represents a high, but still common RTT value of 500 ms in the Internet nowadays). *Delay1* is part of the CN-HA and HA-MR delays, thus affects the overall delay in the CN-HA-MR-LFN path followed by packets of the CN-LFN communication. Results for the case of using the NEMO basic support protocol are shown in Fig. 6. Results for the case of using MIRON are shown in Fig. 7. Confidence limits (95%) are also shown in both figures.

If the NEMO basic support protocol is used, the effect of a higher value of *delay1* in the performance of TCP application is clear: the effective throughput decreases as the delay increases (Fig. 6). The LFN would obtain a much higher effective throughput if it was connected directly to the foreign network instead of the NEMO. This difference in the throughput increases with the delay in the CN-HA-MR-LFN path. Therefore, nodes of a mobile network located far from its home network and/or from the CN they are communicating with, would obtain extremely low TCP throughput when competing with other TCP flows, because of the suboptimal path introduced by the NEMO basic support protocol. Even for a value of *delay1* equal to 0 ms the throughput obtained by the MNN is almost a half of the one obtained by the non-MNs. Although *delay1* is 0 ms, the RTT

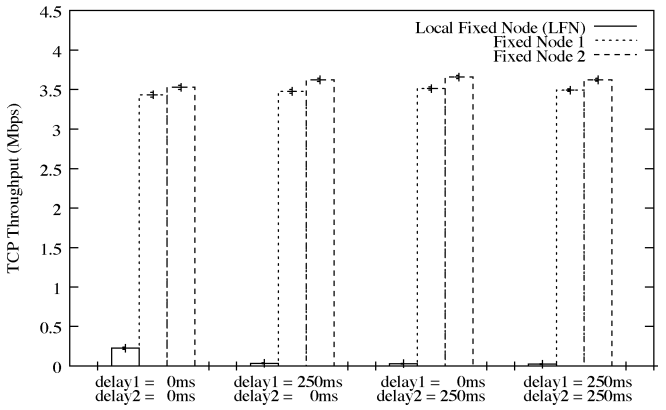

Fig. 8. Impact of NEMO basic support protocol on the TCP throughput in a two-level nested mobile network.

between CN and MNN is bigger than the RTT between CN and fixed nodes, because the path is not direct and there are more hops, and this difference, even though small, has an important effect on the TCP fairness. Moreover, there exists a difference in the PMTU because of the overhead that also has an influence in the TCP performance.

If MIRON is used, the performance improvement is substantial (see Fig. 7). The TCP throughput remains constant despite the value of *delay1*. This result is as expected, because with MIRON data packets do not follow the CN-HA-MR-LFN suboptimal path, but the direct CN-MR-LFN path. Part of the difference in the TCP throughput of the fixed nodes and the LFN is due to the packet overhead (MIRON introduces a 24-byte per packet overhead, because of the routing header type 2 and the HoA destination option). The performance of the MIRON prototype used during the tests (completely implemented in user space) may also have something to do with the obtained difference, although this difference could be reduced by improving the implementation (e.g., by implementing it in kernel space, or at least those tasks that have an strong impact in the overall performance).

For the nested scenario [Fig. 5(b)], besides evaluating the effect of the varying *delay1*, that is, the delay of the path CN-HA-MR-LFN, a second adjustable delay—*delay2*—was introduced between R4 and R5, allowing us to evaluate also the effect of the distance between the home networks of two different mobile networks that are nested. Fig. 8 shows the obtained throughput results for the NEMO basic support protocol and Fig. 9 for MIRON.

As in the non-nested test (see Fig. 9), the improvement achieved by MIRON is clear. The NEMO basic support protocol performs worse than in the non-nested scenario, even for the null added delay case. This is because the actual RTT is bigger for the LFN than for the fixed nodes due to the longer path that packets have to traverse (CN-HA2-HA1-MR1-MR2-LFN) and the reduced PMTU. On the other hand, the performance obtained with MIRON is the same as in the non-nested scenario, as packets follow the optimal direct path and the overhead remains the same, no matter what number of nesting levels the mobile network has. As in the non-nested scenario, the TCP throughput of the LFN is lower than the one achieved by

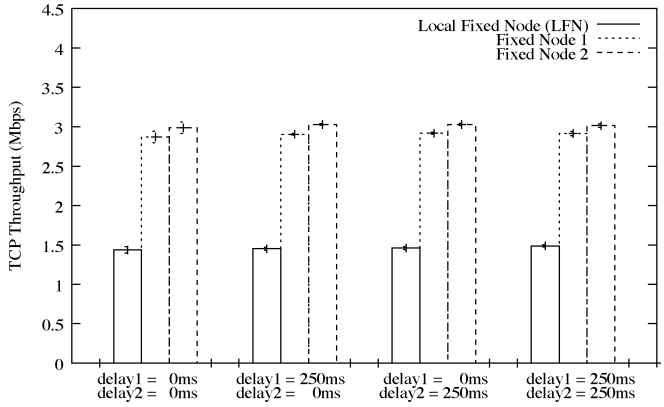

Fig. 9. Impact of MIRON on the TCP throughput in a two-level nested mobile network.

the fixed nodes because of higher RTT (packets go through more intermediate hops—MR1 and MR2) and the impact of implementing MIRON completely in user space.

B. Analytical Evaluation

We have analyzed how the added delay due to the suboptimal CN-HA-MR-MNN path introduced by the use of the NEMO basic support protocol affects the performance of TCP applications. In addition to the severe effect that the overall RTT has in the TCP performance, and the obvious effect that the delay itself has on real-time applications,[6] there is another effect that impacts performance: the packet overhead (and the associated PMTU reduction).

A 40-byte IPv6 header is added to every packet in the MR-HA bidirectional path due to the NEMO basic support protocol. Moreover, an IPv6 additional header is added per nesting level. The effect of this overhead can be negligible for nonreal-time applications, but it can be very important for real time ones, such as VoIP applications. In order to quantitatively evaluate this effect, we analyze next the effects of the NEMO basic support protocol and MIRON, comparing it with plain IPv4 and IPv6, in a VoIP communication using the widely utilized Skype[7] application. Skype uses the Internet low bit rate codec (iLBC) [28], which is a free speech codec suitable for robust voice communication over IP. The codec is designed for narrowband speech and results in a payload bit rate of 13.33 kb/s with an encoding frame length of 30 ms and 15.20 kb/s with an encoding length of 20 ms.

Table I shows the packet overhead and the bandwidth consumed by a VoIP communication using UDP/RTP and the iLBC codec, for plain IPv4, plain IPv6, the NEMO basic support protocol, and MIRON. The overhead of MIRON is less than the one introduced by the NEMO basic support protocol and remains constant though the number of nesting levels. The reader should notice that a nested mobile network connected to the Internet through a 64 kb/s connection would not be able to support this kind of VoIP traffic (VoIP applications are expected to be very important in forthcoming 4G networks). In [25], an additional analysis of the packet overhead in network mobility environments is presented.

[6]There are analytical studies [27] that say that the maximum tolerable delay in a voice communication is about 50 ms.

[7]http://www.skype.com/.

TABLE I
iLBC BITRATES AND PACKET OVERHEAD (20 ms ENCODING LENGTH)

Protocol	Bitrate (kb/s)	Packet Overhead (%)
IPv4	31.2	51.28
IPv6	39.2	61.22
NEMO (without nesting)	55.2	72.46
NEMO (2 nesting levels)	71.2	78.65
NEMO (3 nesting levels)	87.2	82.57
MIRON (without nesting)	48.8	68.85
MIRON (2 nesting levels)	48.8	68.85
MIRON (3 nesting levels)	48.8	68.85

C. Scalability Considerations

MIRON requires some additional operations to be performed in the MR. This section briefly analyzes the scalability of MIRON and provides some implementation considerations to ensure an scalable deployment.

Basically, there are three different aspects that may affect to the scalability of MIRON.

- *Signaling load*. In order to optimize a CN-LFN flow, the MR has to perform the MIPv6 RO signaling with the CN on behalf of the LFN. This signaling grows linearly with the number of CN-LFN pairs being route optimized. Similarly, to optimize the traffic of a VMN or a nested NEMO, the PANA and DHCPv6 signaling also grow linearly with the number of VMNs/MRs. This linearity is important, since it makes the required resources in a MR proportional to the size of the NEMO and it seems natural to expect MRs of large mobile networks (such the ones deployed in trains) to be powerful enough and not be resource-constrained. On the other hand, resource-limited devices, such as cellular phones and PDAs are not expected to be the MR of networks with more than a few attached nodes.
- *Memory consumption at the MR*. MIRON needs some additional information to be stored at the MR, such as host routes, extended binding cache entries (since state information regarding each LFN-CN optimized pair is required), and information about delegated addresses. The required memory to store a host route, a binding entry or the information about a delegated address is relatively small and grows linearly with the number of MNs (i.e., VMNs and MRs) being optimized and LFN-CN route optimized pairs.
- *Processing load at the MR*. MIRON requires the MR to perform some additional operations: inspection of every packet, special handling (that is, removal of the routing header in the CN to LFN direction and addition of the HoA destination option in the LFN to CN direction) of route optimized packets and source routing. Regarding packet inspection, MIRON just needs to look at the source and destination addresses of every packet to track LFN-CN flows and also to certain IPv6 headers to detect new arrived VMNs/MRs attached to the NEMO, so this inspection is quite similar to the normal inspection that a router does. Even if some local policies are implemented at the MR to enable smarter decisions about whether a certain flow should be optimized or not, requiring the MR to look also

at other fields in a packet (such as transport headers), this inspection is not much different than the inspection than typical firewall software does in an border (access) router. Besides, the amount of traffic being processed by a MR is, in general, related to the size of the NEMO, so the same reasoning about the size of the NEMO and the resources of its MR also applies here.

The special packet handling is performed by MIRON only to packets that belong to an LFN-CN communication that is being route optimized. Therefore, neither the optimized packets from VMNs or MRs, nor the packets of communications that are not being optimized, require such special packet handling. This special packet handling adds some delay in the packet processing time that depends on the MR capabilities and how this processing is implemented.

Finally, source routing at the MR is needed to avoid route optimized packets to be forwarded through the MR-HA bidirectional tunnel (instead of following the optimized direct path). Therefore, MIRON requires a different routing table per LFN that has traffic being optimized. Each of these routing tables has an entry per each CN the LFN is communicating with. Therefore, the amount of routing entries grows linearly with the number of different LFN-CN pairs being route optimized and it is independent of the nesting level.

We can conclude that MIRON required resources grow linearly with the number of optimizations being performed, independently of the nesting level. This allows practical deployments, since it is natural to expect that the capabilities and resources of a MR to be proportional to the size of the managed NEMO. Besides, a limit on the amount of resources (memory, processing power, etc.) used by MIRON can always be set, so the MR may stop starting new RO operations when that limit is exceeded.

V. Comparison With Previous Work

This section presents two different approaches of RO for NEMO and compares them with MIRON, in terms of performance, signaling load and complexity.

A possible approach to achieve RO for NEMO [11] is to allow the MR directly to inform the CN about the location of the MNP using the NEMO prefix option. So far, this is simply a direct extension of the MIPv6 RO procedure to the NEMO case. However, the security mechanism used for securing RO in MIPv6 cannot be directly applied to this case. In MIPv6, BU messages are secured through the RR procedure, that verifies the collocation of the HoA and the CoA. In the case of a prefix, it is unfeasible to verify that all the addresses contained in the prefix (2^{64} addresses) are collocated with the CoA contained in the BU message. In order to overcome this difficulty, a RR procedure for network prefix (RRNP) [29] is proposed, which consists of performing the MIPv6 RR procedure with a randomly selected address of the NEMO prefix.

We will next compare this proposal (hereafter BU for network prefixes) with MIRON. In particular, we will consider the benefits and the costs associated with each one of them. With respect to the costs, the main difference concerns the deployment effort associated with the different proposals. MIRON, as we have already mentioned, uses the existent MIPv6 protocol unchanged. This means that the deployment of MIRON only implies modifications to the MRs. CNs do not need any upgrade since they do not require any MIRON-specific mechanism. On the other hand, BU for network prefixes requires not only upgrading the MRs but also upgrading all the potential CNs, i.e., all the nodes in the Internet. This is a huge deployment cost, which may not be worth depending on the resulting benefits, which will be considered next.

The benefit resulting from the adoption of any of the proposals is the optimized path through which packets are routed between the MR and the CN. However, the approach based on BU for network prefixes requires less signaling than MIRON. We will next quantify the difference in order to evaluate if this overhead reduction can justify the deployment cost previously identified. Consider a moving network with N MNNs. Suppose that each MNN communicates simultaneously with M CNs in average. This means that with MIRON, $N \times M$ BUs messages will be required to optimize these communications. On the other hand, if the approach based in BU for network prefixes is used, the number of BU required depends only of the number of different CNs that are communicating with at least one MNN. This is so, because the BU message refers to the whole MNP, implying that if two or more MNNs are communicating with the same CN, only one BU message is needed. The net benefit resulting from the adoption of BU for network prefixes with respect to MIRON is a reduction in the amount of BU messages required proportional to the number of MNNs that are simultaneously communicating with a common CN. It should be noted that this only applies for those CNs that do not belong to the Home Network, since those nodes residing in the home network already benefit from a direct routing with the mobile network thanks to NEMO basic support protocol. So, the benefits provided by an approach based on BU for Network Prefixes heavily depend on the expected number of MNNs that will communicate with a common CN outside the Home Network. The costs, on the other hand, are objective and account for the upgrading of all the nodes of the Internet to support the new option. MIRON, on the other hand, is compatible with standard MIPv6 CNs.

The NEMO basic support protocol when applied to the case of nested mobile networks is quite inefficient as was mentioned in Section II-C. [30] proposes a solution to alleviate these inefficiencies. The proposal requires modifications in MRs and HAs, but not in LFNs, VMNs, or CNs.

The idea is the following: for packets going out of the nesting, the first MR in the path, in addition to tunneling the packet to its HA with a header with source address its own CoA and destination address its HA address, it also includes in the outer header of the packets a new type of routing header called reverse routing header (RRH), where it introduces its own HoA and empty slots where the rest of the MRs in the path can introduce their respective CoAs. This proposal requires the use of Tree Discovery [31] to allow the MRs to find out the level of hierarchy in the nesting (i.e., the number of slots required).

The rest of the MRs change the source address of the outer header and include their own CoA, but put the old source address (the CoA of the previous MR) in the RRH. When the

packets leave the nesting, they are forwarded to the HA of the first MR in the path. The HA decapsulates the packets and sends them to their destination (it uses the HoA included in the RRH to find out or create the right Binding Cache Entry), but also keeps associated to the respective Binding Cache Entry the information contained in the RRH. This information allows the HA to include in the outer header of the packets destined to a node in the nesting, a routing header indicating how the packet must be routed inside the nesting (the CoAs of the MRs in the nesting in the order that must be traversed). The final result is that the packets in each direction only go through one tunnel and one HA, although some processing is added in the HA and MRs plus the overhead of the information added to the packets.

This overhead can be quantified in one IPv6 header plus one routing header plus one IPv6 address per level of nesting of the mobile network, i.e., $(40 + 8 + n * 16)$ bytes $= (48 + n * 16)$ bytes, where n is the number of levels in the nesting (at least 2). This overhead is required in all the packets that go to and from the mobile network. It could be eliminated from some packets in the way out of the mobile network only at some cost in functionality (ability to detect changes in the nesting) and security. Notice that the solution of MIRON for nested mobile networks only requires the 40 bytes of the tunneling and even that is avoided when an end-to-end optimization of the path between the mobile network and the CN is used.

The additional need for using Tree Discovery [31] implies changes in MRs and routers included in the nesting, because Router Advertisements must support the functionality of Tree Discovery. This implies also an overhead in signaling because Router Advertisements in the nesting must have a minimum of 32 bytes more than normal Router Advertisements. This must be compared with the signaling load to distribute topological valid addresses to MRs in MIRON.

VI. Conclusion

The NEMO basic support protocol [12] enables whole networks to move and change their point of attachment, transparently to the nodes of the network. This solution introduces some limitations and problems in terms of performance (increased delay in packet delivery and packet overhead, decrease in available PMTU, the HA becoming a bottleneck, etc.). To overcome these limitations, we have designed and implemented a RO solution: MIRON, that enables direct path communication between a node of the mobile network—supporting any kind of node, with and without mobility capabilities—and a CN.

MIRON has two modes of operation: the MR performing all the RO tasks on behalf of those nodes that are not mobility capable—thus working as *Proxy-MR* [14]—and an additional mechanism, based on PANA and DHCP, enabling mobility-capable nodes (i.e., MNs attached to a NEMO) and routers (i.e., nested MRs) that actually have mobility and RO capabilities to manage their own RO.

To validate the design of the solution and evaluate the actual performance of it, a prototype of MIRON was implemented in Linux. The NEMO basic support was also implemented so we could compare the results obtained with MIRON with the basic solution for network mobility. Tests involving TCP applications showed that the increased RTT perceived by the nodes of a mobile network (due to the suboptimal path followed by packets) has a severe impact on the performance (in terms of effective throughput, when sharing some link with traffic from other active nonmobile TCP nodes). This effect is exacerbated when NEMOs are nested. On the other hand, the same tests conducted with MIRON showed a better performance, by obtaining much higher effective TCP throughput than in the case of the NEMO basic support, also in the case of nested networks.

The effect of packet overhead was described by means of a quantitative analytical study of the overhead that several protocols add to packets belonging to a VoIP application, such as Skype. These results show that the packet overhead introduced by the NEMO basic support protocol is significant for this kind of application, specially when there is nesting.

In conclusion, this paper proposes a RO for NEMO solution (MIRON), that provides significant performance improvements over the NEMO basic support protocol and that is implemented only modifying the software in the MRs. LFNs, VMNs, or CNs do not need to be modified for MIRON to work, which facilitates the deployability of the solution. The validity of the solution has been proven by making experiments and tests with an implementation for Linux.

We could also think in a solution to NEMO RO that could be developed without the constraints of no modifying CNs (i.e., any potential peer that a node in the mobile network may have). The problem with this type of solution is that it will only work with some nodes in the Internet (those that had upgraded their software to allow nodes of a NEMO to optimize their communications with them). We think that there is the need of working in the design of NEMO RO solutions that, by taking advantage of introducing some changes on CNs and/or MNNs, could be more efficient that the one presented in this paper. But both types of solutions will coexist, because a large installed base of legacy nodes will require a solution like MIRON.

Acknowledgment

The authors would like to thank Prof. A. Azcorra for his essential support to this work. They would also like to thank P. Thubert and E. Nordmark for their helpful comments that contributed to improve MIRON design. They also would like to thank A. Banchs, M. Urueña, H. Oliver, I. Martinez-Yelmo, and A. García-Martínez for reviewing and helping to improve this paper. Also, the authors would like to thank C. Izquierdo for the development of the DHCPv6 implementation used in the MIRON prototype. They also thank the anonymous reviewers of this paper for their valuable comments.

References

[1] D. Yi and K. H. Yeung, "Challenges in the migration to 4G mobile systems," *IEEE Commun. Mag.*, vol. 41, no. 12, pp. 54–59, Dec. 2003.

[2] R. Droms, "Dynamic host configuration protocol," IETF, RFC 2131, Mar. 1997.

[3] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, "Dynamic host configuration protocol for IPv6," IETF, RFC 3315, Jul. 2003.

[4] C. Perkins, "IP mobility support for IPv4," IETF, RFC 3344, Aug. 2002.

[5] D. Johnson, C. Perkins, and J. Arkko, "Mobility support in IPv6," IETF, RFC 3775, Jun. 2004.

[6] R. Koodli, "Fast handovers for mobile IPv6," IETF, RFC 4068, Jul. 2005.
[7] H. Soliman, C. Catelluccia, K. E. Malki, and L. Bellier, "Hierarchical mobile IPv6 mobility management (HMIPv6)," IETF, RFC 4140, Aug. 2005.
[8] R. Moskowitz and P. Nikander, "Host identity protocol architecture," IETF, draft-ietf-hip-arch-02.txt (work-in-progress), Jan. 2004.
[9] P. Nikander, J. Ylitalo, and J. Wall, "Integrating security, mobility and multi-homing in a HIP way," in *Proc. Netw. Distrib. Syst. Security Symp.*, Feb. 2003, pp. 87–99.
[10] T. R. Henderson, "Host mobility for IP networks: a comparison," *IEEE Network*, vol. 17, no. 6, pp. 18–26, Nov.–Dec. 2003.
[11] H.-Y. Lach, C. Janneteau, and A. Petrescu, "Network mobility in beyond-3G," *IEEE Commun. Mag.*, vol. 41, no. 7, pp. 52–57, Jul. 2003.
[12] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network mobility (NEMO) basic support protocol," IETF, RFC 3963, Jan. 2005.
[13] C. J. Bernardos, M. Bagnulo, and M. Calderón, "MIRON: mobile IPv6 route optimization for NEMO," in *Proc. 4th Workshop on Appl. Services in Wireless Netw.*, Aug. 2004, pp. 189–197.
[14] C. Ng, F. Zhao, M. Watari, and P. Thubert, "Network mobility route optimization solution space analysis," IETF, draft-ietf-nemo-ro-space-analysis-01.txt (work-in-progress), Dec. 2005.
[15] P. Jayaraman, R. Lopez, Y. Ohba, M. Parthasarathy, and A. Yegin, "PANA framework," IETF, draft-ietf-pana-framework-03.txt (work-in-progress), Dec. 2004.
[16] T. Ernst and H.-Y. Lach, "Network mobility support terminology," IETF, draft-ietf-nemo-terminology-02.txt (work-in-progress), Oct. 2004.
[17] T. Ernst, "Network mobility support goals and requirements," IETF, draft-ietf-nemo-requirements-03.txt (work-in-progress), Oct. 2004.
[18] A. Yegin, Y. Ohba, R. Penno, G. Tsirtsis, and C. Wang, "Protocol for carrying authentication for network access (PANA) requirements," IETF, draft-ietf-pana-requirements-09.txt (work-in-progress), Aug. 2004.
[19] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, and A. Yegin, "Protocol for carrying authentication for network access (PANA)," IETF, draftietf-pana-pana-07.txt (work-in-progress), Dec. 2004.
[20] L. Blunk and J. Vollbrecht, "PPP extensible authentication protocol (EAP)," IETF, RFC 2284, Mar. 1998.
[21] C. Ng, P. Thubert, M. Watari, and F. Zhao, "Network mobility route optimization problem statement," IETF, draft-ietf-nemo-ro-problem-statement-02.txt (work-in-progress), Dec. 2005.
[22] E. Perera, V. Sivaraman, and A. Seneviratne, "Survey on network mobility support," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 8, no. 2, pp. 7–19, Apr. 2004.
[23] P. Nikander, J. Arkko, T. Aura, G. Montenegro, and E. Nordmark, "Mobile IP version 6 route optimization security design background," IETF, RFC 4225, Dec. 2005.
[24] C. J. Bernardos, I. Soto, J. I. Moreno, T. Melia, M. Liebsch, and R. Schmitz, "Experimental evaluation of a handover optimization solution for multimedia applications in a mobile IPv6 network," *Eur. Trans. Telecommun.*, vol. 16, no. 4, pp. 317–328, Apr. 2005.
[25] A. de la Oliva, C. J. Bernardos, and M. Calderón, "Practical evaluation of a network mobility solution," in *Proc. 11th Open Eur. Summer School: Networked Applications*, Jul. 2005, pp. 60–66.
[26] S. McCreary and K. Claffy, "Trends in wide area IP traffic patterns—A view from Ames Internet exchange," CAIDA, Tech. Rep., 2000.
[27] M. J. Karam and F. A. Tobagi, "Analysis of the delay and jitter of voice traffic over the Internet," in *Proc. IEEE INFOCOM*, Apr. 2001, vol. 2, pp. 824–833.
[28] S. Andersen, A. D. Telio, H. Astrom, R. Hagen, W. Kleijn, and J. Linden, Internet low bitrate codec IETF, RFC 3951, Dec. 2004.
[29] C. Ng and J. Hirano, "Extending RR procedure for network prefix (RRNP) IETF, draft-ng-nemo-rrnp-00.txt (work-inprogress), Oct. 2004.
[30] P. Thubert and M. Molteni, "IPv6 reverse routing header and its application to mobile networks," IETF, draft-thubert-nemo-reverse-routing-header-05.txt (work-in-progress), Jun. 2004.
[31] P. Thubert and N. Montavont, "Nested Nemo tree discovery," IETF, draft-thubert-tree-discovery-01.txt (work-in-progress), Oct. 2004.

María Calderón received the Computer Science Engineering degree and the Ph.D. degree in computer science from the Universidad Politécnica de Madrid (UPM), Madrid, Spain, in 1991 and 1996, respectively.

She is an Associate Professor in the Telematic Engineering Department, Universidad Carlos III de Madrid. She has published over 20 papers in the fields of advanced communications, reliable multicast protocols, programmable networks, and IPv6 mobility, in outstanding magazines and conferences, such as *IEEE Network Magazine*, IWAN, and IEEE-PROMS-MMNET. Some of the recent European research projects in which she has participated are LONG, GCAP, DAIDALOS, COST-263, and E-NEXT.

Carlos J. Bernardos received the Telecommunication Engineering degree from the Universidad Carlos III de Madrid, Madrid, Spain, in 2003. He is currently working towards the Ph.D. degree in the Telematics Department, Universidad Carlos III de Madrid, where he has been working as a Research and Teaching Assistant of Telematic Engineering since 2003.

He has been involved in international research projects related with fourth-generation networks, like the IST MOBY DICK project, and currently IST DAIDALOS. He has published several papers in these topics in magazines and conferences. He is working now on IP-based mobile communication protocols.

Marcelo Bagnulo received the Electrical Engineering degree from the Universidad de la Republica Oriental del Uruguay in 1999 and the Ph.D. degree from the Universidad Carlos III de Madrid, Madrid, Spain, in 2005.

He is currently working as a Research and Teaching Assistant at the Universidad Carlos III de Madrid. He is involved in the design of the SHIM6 protocol, the IPv6 site multihoming solution currently being defined at the IETF.

Ignacio Soto received the Telecommunication Engineering degree and the Ph.D. degree in telecommunications from the Universidad de Vigo, Vigo, Spain, in 1993 and 2000, respectively.

He has been a Research and Teaching Assistant of Telematic Engineering at the Universidad de Valladolid from 1993 to 1999, and at the Universidad Carlos III de Madrid since that year. He is an Associate Professor at the Universidad Carlos III de Madrid since 2001. His research activities are focused in mobility support in packet networks and heterogeneous wireless access networks. He has been involved in international and national research projects related with these topics, including the EU IST Moby Dick and the EU IST Daidalos projects. He has published several papers in technical books, magazines and conferences.

Dr. Soto has served as Technical Program Committee member of INFOCOM.

Antonio de la Oliva received the Telecommunication Engineering degree from the Universidad Carlos III de Madrid, Madrid, Spain, in 2004. He is currently working towards the Ph.D. degree in the Telematics Department, Universidad Carlos III de Madrid, where he has been working as a Research and Teaching Assistant of Telematic Engineering since 2004.

He is currently involved in the European project IST DAIDALOS.