Design and Evaluation of a Novel HIP-Based Network Mobility Protocol

Szabolcs Nováczki, László Bokor, Gábor Jeney, Sándor Imre
Budapest University of Technology and Economics, Department of Telecommunications
Mobile Communication and Computing Laboratory (MC^{2}L) – Mobile Innovation Center (MIK)
Magyar Tudósok krt.2, H-1117, Budapest, Hungary
Email: {nszabi, goodzi, jeneyg, imre}@mcl.hu

Abstract—The rapid growth of IP-based mobile telecommunication technologies in the past few years has revealed situations where not only a single node but an entire network moves and changes its point of attachment to the Internet. The main goal of any protocol supporting network mobility is to provide continuous, optimal and secure Internet access to all nodes and even recursively nested mobile subnetworks inside a moving network. For this purpose, the IETF (Internet Engineering Task Force) has developed the NEtwork MObility Basic Support (NEMO BS) protocol which extends the operation of Mobile IPv6 (MIPv6). In order to bypass the same problems suffered by MIPv6 and NEMO BS, a novel Host Identity Protocol (HIP) extension called HIP-NEMO is introduced, proposed and evaluated in this paper. Our proposal is based on hierarchical topology of mobile RVSs (mRVS), signaling delegation and inter-mRVS communication to enable secure and efficient network mobility support in the HIP layer. The method provides secure connectivity and reachability for every node and nested subnet in the moving network and supports multihomed scenarios as well. Moreover, HIP-NEMO reduces signaling and packet overhead during network mobility management by achieving route optimization inside any moving network even in nested scenarios. To evaluate the proposed scheme we present a simulation model implemented in OMNeT++ and discuss the results of our simulation based analysis to show the efficiency of the approach compared to the NEMO BS protocol formulated by the IETF.

Index Terms—Host Identity Protocol (HIP), NEtwork MObility (NEMO), multihoming, nested mobile networks, route optimization, security, HIP-NEMO.

I. INTRODUCTION

During the last decade, mobile telecommunications has faced an enormous evolution. Due the growth of wireless networking technology, wireless and mobile services and applications have become popular. The convergence of the Internet and the mobile communication technologies generated increasing demand for more widespread and more sophisticated support of mobility, thus services and applications are being extended from single wireless nodes to different moving and traveling networks. The Internet is evolving towards a more pervasive and ubiquitous architecture where users are expected to be able to access different heterogeneous technologies enabling accessibility anytime and anywhere. Trends in information technology show that heterogeneous, IP-based wireless networks will support mobility for the widest range of single end terminals (e.g. mobile phones, SmartPhones, PDAs), and even Personal Area Networks (PANs), Vehicle Area Networks (VANs) [1], Intelligent Transportation Systems (ITSs) [2], networks of RFID (Radio Frequency Identification) devices and sensors, and various mobile ad hoc networks [3] will have permanent Internet connectivity during movement. Hence, when considering mobility management in next generation wireless networks, at least two main types of mobility should be distinguished. On one hand single mobile entities changing their point of attachments have to be taken into account (host mobility). On the other hand, mobility could not be restricted to single wireless terminals anymore: communication sessions within entire mobile networks moving between different subnets need to be maintained as a whole (network mobility). The key difference between the above two approaches is the level of manageability. In case of host mobility, the movement of each mobile terminal is managed separately, on an individual basis. Contrarily, solutions for network mobility define at least one central entity in a moving network in order to hide the inside operation. This behaviour ensures several advantages. First, because all nodes inside a moving network connect to the Internet using a central entity of their moving domain, much less power should be emitted for the wireless communication, saving a considerable amount of power. Second, since mobile terminals move as a single object, location update messages of the inside nodes doesn't need to leave the domain thus reducing the complexity of the overall architecture. Third, when the central entity recovers its reachability after a handover, all mobile nodes connected to this moving network can also immediately access the outside network due to the previously presented structure. This characteristic reduces the number of executed handover procedures.

To apply the introduced advantages of network mobility in practice, several protocols and methods were designed and evaluated. The IETF NEMO Working Group defined the basic methodology for providing network mobility called NEMO Basic Support [4] which is considered the most widespread network mobility protocol nowadays. NEMO BS operates in the IP layer and inherits the benefits of Mobile IPv6 [5] by extending

the binding mechanism of the ancestor, but keeps all the problems of the main approach such as protocol overhead, inefficient routing, security and lack of multihoming support. All of these issues are under examination at the IETF with regard to the extended network mobility support and the relating drafts [6], [7], [8], [9], [10], but this work has not been completed yet. However, there are several extensions of NEMO Basic Support in order to allow multihoming and nested mobile networking [11], [12], [13], [14], and ongoing researches are trying to deal with the route optimization [15], [16], [17], [18], [19] and security problems [20], [21], [22], [23], [24]. Despite the fact that several novel real-life demonstrations [25], [26], [27] and testbeds [28], [29], [30] started to prove the feasibility and usability of NEMO Basic Support and its extensions, the searching for new ways of creating an "all-in-one" solution has not stopped [31], [32], [33].

In this paper we also present a new approach for network mobility by proposing a HIP based protocol called HIP-NEMO to provide secure and efficient NEMO solution in the Host Identity Layer. In order to do this, first we give a short overview of NEMO BS and HIP with its Base Exchange, mobility management procedures, signaling delegation capabilities and service discovery mechanisms in Section II. This is followed by our main motivations and design goals in Section III. Then we summarize previous work relating to different NEMO solutions, and route optimization / security extensions of network mobility supporting protocols together with our contributions in Section IV. Section V presents the terminology, the protocol overview and the detailed operation of our HIP-NEMO proposal while Section VI is devoted to introduce the simulation framework and the evaluation results regarding the comparison of NEMO BS and HIP-NEMO. In Section VII we present the open issues of our proposal. Finally we conclude the paper and present our future work.

II. BACKGROUND

In this section we survey the main concepts, terminology and base protocols which will be used in the paper. First we summarize the characteristics of NEMO BS protocol together with its main advantages and drawbacks and then a description of the Host Identity Protocol is provided as the basic protocol of our novel network mobility solution.

A. Network Mobility Basic Support

In order to fulfill the requirements of persistent connected moving networks (e.g. trains or buses full of wireless clients inside the passenger cab) to the Internet, an IETF Working Group called NEMO was created aiming to work on the design of the required standards. NEMO WG defines the network mobility protocols in two main parts. NEMO Extended Support is an ongoing, uncompleted research which will provide a complete framework for NEMO communication together with route optimization even for nested scenarios and other advanced functions such as multihoming and QoS.

NEMO Basic Support is an approved RFC [4] providing only the primary functions for supporting the basic network mobility demands by enhancing the operation of MIPv6. Thus the main goal of NEMO-BS is to preserve all established internal and external communication sessions of nodes attached to a moving network despite the network's movement.

In the IETF NEMO protocols a moving network (MNet) is defined as an entity handling several inside nodes and/or subnetworks as a whole whose Internet point of attachment changes in time. A moving network consists of one or more Mobile Routers (MR) and several Mobile Network Nodes (MNN). MR is the node that manages the tasks of internal routing within a NEMO and connects the whole MNet to the external network. MNNs can either be fixed or can be mobile while belonging to one particular MR. In the first case we are talking about Local Fixed Nodes (LFN), in the second case Local Mobile Nodes (LMN) are to be distinguished (Fig. 1). If MNNs can leave their MRs (i.e. MNNs are able to move to foreign mobile networks), then these nodes are referred to as Visited Mobile Nodes (VMN) from the foreign MNet's point of view. This architecture makes possible that only the MR must be involved in the handover operations on behalf of the whole moving network. Data traffic between MNNs and Correspondent Nodes (CNs) is managed by establishing bidirectional tunnels between the HA and the MR of the moving network to which the MNNs belong. The solution used by NEMO-BS is similar to Mobile IPv6 without routing optimization: when a MR leaves its home link, it configures a Care of Address (CoA) in the visited network and registers this CoA with its HA using the binding procedure. However, the Binding Update (BU) message in NEMO-BS is quite different from that in MIPv6. While a BU message in MIPv6 contains the Care-of and the Home Address (HoA) of a mobile node, till a BU of an MR contains additional information: the IP subnet prefix(es) of the moving network. These so called Mobile Network Prefixes (MNPs) in the BUs instruct the HA to create a binding cache entry linking the MNPs to the MR's CoA.
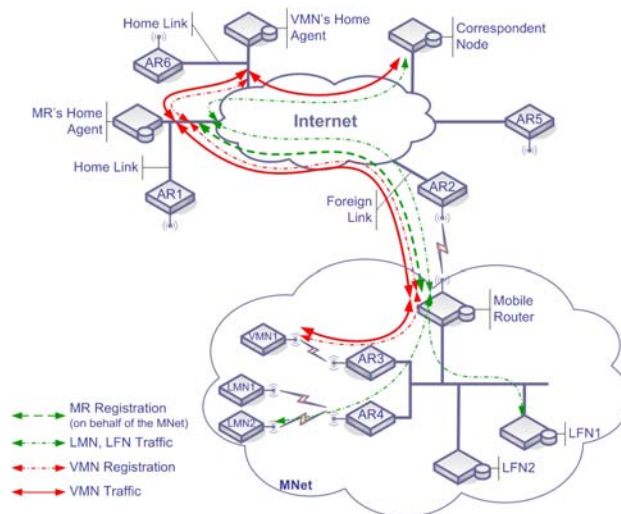

Figure 1. Overview of NEMO-BS

After a successful registration, the HA intercepts and forwards packets destined not only to MR, but also to any MNNs that have acquired an address from one of the MR's MNPs. When the moving network changes its actual network point of attachment, only the MR configures new CoA and sends Binding Update (containing the MNPs) to the HA. Observing that the MNNs don't need to configure and bind new CoA as long as they are inside the moving network, signaling overhead can be reduced but it has its cost. A CN usually sends packets to a mobile node using the MN's HoA. Since the HoAs of the LFNs and LMNs inside a moving network are associated with the MNPs registered in the HAs, the HA of the network's MR intercepts all the packets addressed to local nodes and forwards them towards the MR's CoA. If the CN addresses a VMN, the procedure is similar: data packets destined to a VMN first will be intercepted by the VMN's HA which tunnels all the packets to the VMN's CoA. The VMN's CoA belongs to the MNP, thus packets go towards the MR's HA which forwards to the MR's CoA. The MR decapsulates the packets (destined to both Local and Visited MNs) and forwards them on its appropriate ingress interfaces. Packets originated from inside the moving network will follow the same routes but in the reverse direction. It is obvious that the big number of encapsulations cause header overhead, and the fact that all the HAs should be involved in the communication path results using traffic routes far from the optimal ones.

NEMO-BS strongly relies on IPSec functions as its basic security protocol (similarly to MIPv6): IPSec Authentication Header (AH) and Encapsulation Security Payload (ESP) mechanisms are used for protecting the signaling messages and IPSec protected tunnels are offered for NEMO related traffics between communicating nodes.

Based on these procedures and modifications to the basic MIPv6 protocol, network mobility support can be achieved without the need of changing the addresses of MNNs, but with introducing a serious amount of header overhead and building tunnels on suboptimal routes.

B. The Host Identity Protocol

There are a big number of IP based frameworks today granting continuous mobile connectivity to single users or whole subnetworks of the Internet [4], [5], [34], [35]. However all of these protocols address the same basic problem: mobile entities are identified by IP addresses that depend on their actual topological location. IP addresses thus become overloaded in the sense that they are both identifiers and locators at the same time. This dual role of IP addresses makes mobility management very inconvenient because every time when a mobile entity leaves its actual location, it must tear down all its ongoing connections and must set them up again with the new IP address of the new location.

To meet the new requirements, the Host Identity Protocol (HIP) separates the dual role of IP addresses described above [36], [37]. By interposing the Host Identity Layer between the network and the transport layers, HIP takes off the identifier role from IP addresses,

which continue acting as locators only. HIP introduces a new, cryptographic namespace called the Host Identity where the members are represented by Host Identifiers (HIs, concrete bit patterns used in the protocol) and 128-bit long hashed encodings of HIs called Host Identity Tags (HIT). The Host Identifiers are self-certifying and statistically globally unique and static names of HIP-enabled hosts. In this architecture public keys of asymmetric key-pairs are used for HIs; accordingly a HIP-enabled host is defined as the entity holding the private key of the appropriate key-pair. Host Identity Layer maps HIs to IP addresses and vica versa thus transport layer connections are no more bound to IP addresses, and connections do not have to be broken if the location of hosts change.

1) The HIP Base Exchange

In order to establish end-to-end connection and set up keying material for the communication, HIP includes an initial four-packet handshake called the Base Exchange (BE). During the BE an IPSec Encapsulated Security Payload (ESP) and Security Association (SA) pair will be constructed [38] between the endpoints using a Diffie-Hellman authenticated key exchange (Fig. 2 shows the message sequence). The built-up ESP SAs are bound to HIs, but packets traveling in the network do not contain the actual HIT information after the BE is completed [37]. Instead, packets are identified and mapped to the correct SA using the Security Parameter Index (SPI) value in the IPSec header and the destination IP address in the IP header, thus subsequent packets do not require any additional HIP overhead (Fig. 2).
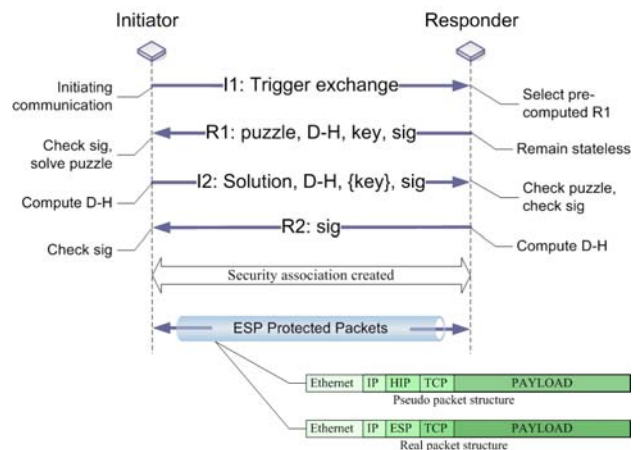

Figure 2.   The HIP Base Exchange

2) Mobility support in HIP

The HIP association of ESP protected SA pairs created by the BE manages a secure, point-to-point connection between two HIP enabled nodes. However, these nodes may be mobile, therefore the associations of moving endpoints may need to be updated over time to time. In such cases the mobility extension of HIP is used.

a) HIP Mobility with Single SA Pair

The Host Identity layer is responsible for mapping HIs to IP addresses, thus when a mobile node changes its

actual network point of attachment, the node must notify all of its Correspondent Nodes (CNs) about the new IP address. A new HIP parameter called LOCATOR was defined to make the protocol able to handle this situation by allowing a HIP node to update existing HIP associations (i.e. to report the new IP addresses to the CNs): if a HIP-enabled host changes its IP address it can send an UPDATE packet to all of its CNs. The UPDATE packet contains a LOCATOR parameter which holds the new location pointer (i.e. the new IP address) and some other information (e.g. the SPI associated with the new IP address and an ESP_INFO parameter to create a new inbound SA) [38]. A CN receiving an UPDATE packet simply corrects its HI – IP address mapping and communication can continue undisturbed (Fig. 3).

Since transport layer connections are bound to HIs the address changes in the IP layer are totally transparent to a HIP node. This property makes HIP mobility management and multihoming provisioning very convenient, simple and fast [39], [40]. Note that the concept of LOCATORs is not necessary limited to IP addresses. They can hold more complex information, e.g. IP-SPI pairs and even more than one LOCATOR can be included in one UPDATE packet. The different locators are distinguished by a type parameter assigned to them.
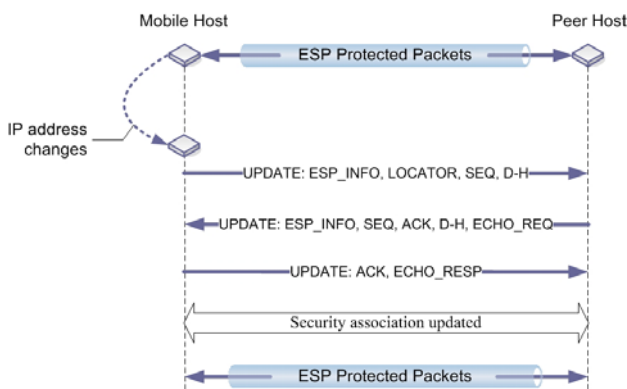

Figure 3.   HIP mobility with singe SA pair

b) Mobility with Rendezvous Mechanism

There are some complex but real-life scenarios where the above introduced simple end-to-end readdressing functionality and HIP architecture is not adequate (e.g. frequent location updates, the initial reachability of a mobile node (MN), simultaneous mobility of nodes). The handling of these situations needs extension of the basic HIP architecture: a new network entity was introduced to overcome the problems called the HIP Rendezvous Server (RVS) which maps HIs onto a set of IP addresses [41]. If a HIP enabled mobile node enters the network, it should register its IP address in a network directory, which is known by all the potential CNs. Basically this is a kind of DNS functionality. However, a traditional DNS is not prepared to handle frequent address changes. Therefore, using HIP Rendezvous Servers as a second global name resolution service is a better solution for tracking the frequent address changes of mobile nodes [42]. If we assume that the MN knows the IP address and HIT of at least one RVS, than in case of entering a new

network, the node updates its entry at the RVS and reports the IP address of the RVS at the DNS (the IP address of the RVS remains the same for relatively long time) (Fig. 4).
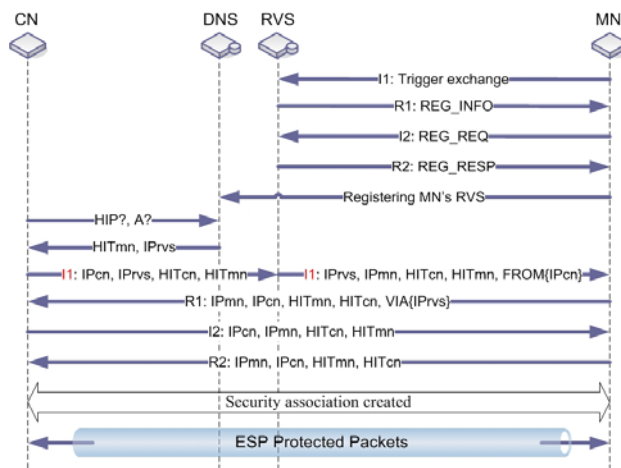

Figure 4.   HIP Rendezvous mechanism

Now if the MN moves to another attachment point while changing its IP address, the node should update only its entry at the RVS [41]. If a CN wants to reach the MN, it performs a lookup at the DNS for the IP address of the MN and the DNS answers with the IP address of the MN's RVS (Fig. 4). The CN now initiates the HIP connection by sending the I1 packet to the RVS with the HIT of the MN. The RVS – as a contact link – forwards the packet according to the containing HIT of the MN. In addition the RVS appends a FROM parameter to the packet representing the IP address of the CN. The MN answers with the R1 packet sending it directly to the CN. The MN adds a VIA_RVS parameter to the packet, which contains the IP address of the RVS. Finally the two nodes finish the BE in the regular way.

3) HIP Service Discovery

In [43] the authors describe a method for HIP enabled hosts to register themselves for a service to use which is provided by another HIP capable network entity, and [44] discusses the different HIP service discovery processes required by hosts depending on two distinguished scenarios.

In the first scenario (called *On-the-Path Service Discovery*) the service provider resides on the packet forwarding path and listens to traffic. Once a HIP host sends either I1, UPDATE or Service Discovery Packet (SDP) messages to the peer node, the service provider replies back to the HIP host a Service Announcement Packet (SAP). The destination IP address of the initiator packet is set to the IP address of the peer node towards which the service discovery is to be done. At first the HIP host sets the local IP_TTL value to one, and sets the TTL of the IP packets to this. When the initiator gets the ICMP Time Exceeded message, it increases the IP_TTL value by one, then sets the IP TTL to the new value, and resends the SDP. This procedure continues until the IP_TTL outruns the SDP_MAX_TTL value, or the HIP

host has successfully received SAP from a working service provider. There are cases where active queries of services are not needed. A good example for that is when a mobile host goes behind a mobile router. The host may not want to perform router discovery during every movement thus it is better to configure the mobile router to send the service announcement initiated by HIP packets traveling through the mobile router (e.g. I1 or UPDATE packets).

In the second scenario (called *Regional Service Discovery*) the HIP host may initiate the service discovery by injecting an SDP into the network, thus intending to detect services in a well-defined network area. The initiator creates and SDP with the appropriate REG_INFO parameter, fills the destination HIT field with zeros and selects the destination multicast/broadcast or even anycast IP address. This method makes it also possible to find service providers which are not located on the packet forwarding path.

4) Delegation of Signaling Rights

The basic idea behind the signaling delegation concept in general is as follows. An initiator node asks another node (usually a superior one) to send signaling messages on behalf of it. Using signaling delegation the usage of network resources and the number of signaling messages can be reduced. However in existing IP networks delegation of signaling rights raises many security threats. Solving these problems in current systems requires complex security management frameworks. However, in HIP-based networks there is a quite straightforward solution for the security issues: based on the HIP's self-certifying namespace, HIP-enabled hosts are able to authenticate each other, to protect the confidentiality and integrity of signaling messages and the payload. Furthermore, these identifiers can easily be used to create cryptographic certificates which is the basis of secure signaling delegation [45]. If a host has the right to signal on behalf of another host, it may further delegate this permission. In wireless environments this can lead to enormous resource savings on the air interface since the rest of the signaling overhead can be transferred from the wireless links to a signaling proxy in the wired domain [45].

III. MOTIVATIONS & DESIGN GOALS

Despite the fact that NEMO-BS answers the main questions of network mobility, it still has open issues regarding [8], [9]:

- Optimal routes: By reason of the subservient nation of the HA-MR (parent MR - child MR) liaisons and the encapsulation/tunneling procedures, the routing path in NEMO-BS is highly dependent on the level of nesting resulting suboptimal routes.
- Security: In order to provide security services, NEMO-BS adopts IPSec as its main security convention however it is highlighted that the

incorporation of IPSec is insufficient in several scenarios [10], [46].
- Fault-tolerant Home Agents: Since the active connections of a whole moving network are maintained by a single HA entity, the survivability of HAs is one of the critical issues of NEMO-BS.
- Multihoming: A multihomed MNet can benefit the advantages of having redundant links and connectivity gaining fault tolerance, seamless handovers and load sharing. NEMO-BS doesn't include specification for managing multihomed MNets, furthermore the solution is not trivial, especially in more complex nested scenarios.
- Header overhead: Encapsulating packets results in growing header overhead as the level of nesting increases because each packet must be encapsulated (by adding a new IP header) several times.
- Elimination of long delays due to the MR-HA (parent MR - child MR) bidirectional tunnels: The suboptimal routes easily can cause big RTTs thus long packet delays can be observed in several NEMO scenarios.

In order to give a compact solution for the aforementioned problems and shortcomings of NEMO-BS we propose a novel network mobility management framework based on the Host Identity Protocol.

Since HIP offers enhanced security features based on the cryptographic namespace of HIs, the benefits regarding the support of multihoming and advanced security capabilities can easily be inherited by HIP-NEMO.

As a result of analyzing the open issues of NEMO BS and the potential of HIP, we devised the main requirements of HIP-NEMO as our leading design goals:

- Global reachability: Every MNN should be reachable to every possible CN, independently of the MNet's actual location. The solution should provide uninterrupted Internet access for HIP capable mobile network nodes.
- Security: All implemented network mobility management functions should meet the requirements of the highest possible level of security.
- Transparency: In case of the MNet's movement the MNNs should not detect anything about the fact of possible handovers. In other words, there should not be applied any modification neither in the HIP stack of the MNNs, nor in the HIP stack of CNs.
- Optimized routes: The communication of MNNs should be handled by using optimal routes transparently to CNs and without introducing additional scalability, load balancing and security issues.
- Support of nested scenarios: The architecture should support any number of nested sublevels such assuring that no limitations will be imposed regarding the possible usage scenarios.

- Reduced signaling and header overhead: The protocol overhead should be minimized in order to improve the throughput of wireless channels.
- Compatibility: HIP-NEMO should be compatible with the current HIP architecture and its RVS subsystem as much as possible.

Besides of fulfilling the above goals our aim was to develop a new, effective and compact network mobility framework for HIP-enabled nodes and to prove the comprehensive abilities of the HIP protocol and its architecture even in the most complex scenarios.

IV. RELATED WORK & OUR CONTRIBUTION

Many efforts have already been made to provide a more efficient and secure NEMO protocol. Wide variety of different extensions, schemes and methods have been discussed at the IETF NEMO Working Group and at various conferences as well. In this section we give a short overview of the different approaches, in particular the ones which try to present an integrated solution for all the matters and issues of managing moving networks by searching novel paradigms.

Several approaches handle the problems of NEMO BS by extending the base protocol.

N. Montavont et al. [11] presented a new option in Router Advertisements that allows any receiving nodes discovering the hierarchy of MRs in different levels of nested MNets such helping the router selection for MNNs inside a multihomed nested NEMO environment.

Tat Kin Tan et al. [48] designed a secure hashing method for NEMO MR communication in order to bypass the typical weaknesses of IPSec protected moving networks.

K. Mihui et al. [24] introduced a fast defense mechanism against DoS attacks in NEMO BS. The defense mechanism includes agile detection, filtering of attack packets, identification of attack agents, isolation of attack agents and notification of neighboring routers.

M. Calderón et al. [18] proposed a routing optimization solution for NEMO BS called MIRON which enables direct path communication between any kind of MNN and CN based on two modes of operation: MR can work as a Proxy-MR performing all the RO tasks on behalf of non-mobile MNNs, and can operate using PANA protocol and DHCP enabling mobility-capable MNNs and MNs inside an MNet.

M. Watari et al. [17] published Optimized NEMO (ONEMO) in order to enhance the packet delivery with even in nested NEMO scenarios. The scheme is based on a new forwarding algorithm, a new signaling protocol (for dynamic peer-discovery), new Router Advertisement format and a new Binding Update mechanism.

M. Calderón et al. [22] analyzed the need of signaling delegation in environments where routing optimization for NEMO requires strong protection.

Extensions for NEMO BS solve the problems of multihoming, optimal routes and packet overhead, and even several security problems, but today none of them provides a complete, coherent, integrated framework to address all the issues of moving networks. In order to do this, novel architectures differing from the MIPv6 based NEMO schemes have also been published.

F. Teraoka et al. [31], [32] developed a novel architecture for network mobility management using Location Independent Networking for IPv6 (LIN6). LIN6-NEMO provides network mobility transparency by bringing in a so called Mapping Agent (MA) that manages the location of the MNNs and by performing a procedure in the root MR for overwriting the network prefix of the destination address of packets destined to the MNNs inside a MNet. Despite the fact that vLIN6 enhances the capabilities of the base LIN6-NEMO, several open issues remain open regarding the MA's functionality and the security.

H. Chung-Ming et al. [33] introduced a SIP-based network mobility protocol in order to avoid the problems inherited from MIPv6. The alternative approach of SIP-NEMO extends the SIP framework with three types of new entities called the SIP Home Server, SIP Network Mobility Server and SIP Foreign Server. Based on this new SIP architecture NEMO support can be achieved and even route optimization can be performed between SIP clients. However the solution doesn't handle all the security issues of managing NEMO scenarios.

J. Ylitalo [21] shortly sketches a HIP-based idea for NEMO issues, but this proposal highly relies on the ESP transport format and on the SPI-based NATs.

S. Herborn et al. [47] presented a HIP-based method for dual layered mobility management controlled by a dynamic context driven heuristics that is responsible for decisions regarding the scheme to be used. This proposal composes not a clean HIP architecture but a hybrid system because the authors assume that mobility will be supported via heterogeneous NEMO architectures created by mobile routers running MIPv6-based NEMO protocols, MNNs with HIP support and CNs also running HIP stack.

In this paper we introduce a complete network mobility framework called HIP-NEMO by classifying the mechanisms, defining the algorithms and evaluating the performance of the proposed NEMO solution designed to operate fully in the Host Identity Layer. We introduce a novel approach enabling a new application of the Host Identity Protocol to provide efficient and secure network mobility support for HIP-aware moving networks and its terminals even in multihomed and nested scenarios.

An initial version of HIP-NEMO was presented in WONEMO2007 [49]. This paper presents many elaborations, extensions and refinements to our original work: we have extended the proposal with significant contributions to the basic protocol exposed in WONEMO2007. The enhancements can be found almost in every aspect of the first study starting with the scope and operational design of our solution through formalized and detailed introduction of the system architecture till modeling HIP-NEMO in a discrete event simulation environment and performing extensive evaluations for analyzing the performance of our method compared with NEMO Basic Support.

V. HIP BASED NETWORK MOBILITY SUPPORT

In the former sections we summarized the most important issues related to network mobility. We also discussed the basic functions of the Host Identity Protocol. In this section we introduce our HIP-based network mobility solution, HIP-NEMO.

The solution is based on a new network entity called the mobile RVS (mRVS), which holds the role of Mobile Routers and provides certain HIP-based services for nodes in the mobile network. Before we start the detailed description of HIP-NEMO we define some terms that will be used in the rest of the paper. This is important since we use the NEMO BS terminology in a slightly different meaning. It is necessary to make this differentiation since most of the NEMO related terms were derived from definitions like home network, visited network or Home Agent, which have no real sense to use in a HIP environment.

- *Binding* is a HIP level IDENTIFIER – LOCATOR (i.e. HIT – IP address) couple as opposed to NEMO BS, where binding links two LOCATORs (IP addresses). In our term the *Binding* process is used by the Host Identity Layer to convert HITs to IP addresses and vice versa.

- *Local Fixed Node* (LFN) is a node in the mobile network with a permanent IP address. The node is called *local* as it uses mRVS as its primary Rendezvous Service (RS) provider. In NEMO BS LFN refers to a node, which is in the same home network as the Mobile Router.

- *Local Mobile Node* (LMN) uses mRVS to access the RS but its IP address may change from time to time. In NEMO BS the term refers to a mobile node in the mobile network, whose home network is the same as the one of the mobile router.

- *Visiting Mobile Node* (VMN) uses discrepant RVS as the mRVS to access HIP RS (in NEMO BS VMN is a mobile node in the mobile network, which is assigned to a home link that does not belong to the mobile network).

- *Mobile Network Node* (MNN) is used to refer to all kinds of nodes that may appear in a mobile network (i.e. LFN, LMN, VMN). In NEMO BS terminology MNN means nodes or routers that may appear in a mobile network. In this paper MNNs do not refer to mRVSs.

- *Mobile RVS* (mRVS) is a HIP enabled Mobile Router (MR). All the terms related to MR defined in NEMO terminology are applicable in case of mRVS. Here we mean terms like egress and ingress interfaces, nested mobility terms like root-mRVS (MR), parent-mRVS (MR) and sub-mRVS (MR).

- In NEMO terminology the abbreviation *NEMO* refers to either *NEtwork MObility*, as a networking scenario, and also *MObile NEtwork*, as a networking entity. In this paper we apply NEMO only for the networking scenario. We use MNet to refer to a mobile network, as a networking entity.

Introducing our approach first we highlight the main ideas behind our solution, after which we take a walkthrough over a simple NEMO scenario and explain how HIP-NEMO works in this case. Second, we discuss more complex situations such as the case of nested mobile networks. Finally the handover framework of the solution is explained.

A. Protocol Overview

Our first consideration was to define the roles and responsibilities of the entity, which will hold the function of mobile router. First, it obviously has to be a HIP-aware node since HIP enabled nodes and Host Identity specific connections have to be managed. Second, since all MNNs are reachable via this entity, it is a rendezvous point (RP) in a HIP aware context. Thus it is a practical choice to have an RVS-like entity in the role of HIP-aware mobile router. We defined a new network entity that meets these requirements, which we call mobile RVS (mRVS) in the rest of the paper.

The mRVS is a RP for MNNs, but not exactly in the same way as standard RVSs. The reason is that mRVS is mobile hence it can provide *mobile rendezvous point* services. This indicates that an mRVS itself must have a normal RVS for employing standard HIP RS. This can be considered as an abstraction of standard HIP RS because in HIP-NEMO we define a RP to another (mobile) RP while in HIP a RP is linked to a concrete HIP node.

The mRVS provides the following functions:

- Serves as the primary access point to HIP rendezvous service for LFNs and LMNs.

- Every mRVS acts like a signaling proxy for LFNs and LMNs. The service is offered to nodes directly connected to the particular mRVS, and not for nodes in a nested NEMO. Secure signaling on behalf of other nodes is achieved by HIP-based signaling right delegation [45].

- The standard RVS used by an mRVS is the permanent RP for LFNs and LMNs of the mRVS, which is responsible for registering these nodes at its RVS.

- Finally it communicates with other mRVSs to efficiently handle all the complex NEMO scenarios. On one hand this communication is based on HIP service discovery [44]. The mRVS frequently sends SAP packets on its ingress interfaces to inform other mRVS about its presence. On the other hand we defined a special inter-mRVS registration mechanism.

LFNs and LMNs can operate according to standard HIP in an mRVS-driven NEMO except that they have to be able to delegate their signaling rights to the mRVS. However, this shall be considered as a HIP-based service, rather than a modification of the base protocol. Thus HIP-NEMO can provide transparent network mobility support for LFNs and LMNs. The next subsection is devoted to explain how this is achieved in the simplest NEMO situation.

B. Simple NEMO Scenario

The simplest NEMO scenario consists of a single mobile network with one mRVS and a LFN as Fig. 5 shows. The figure also depicts the HIP layer binding of the entities with a number indicating the concrete step of the process, which resulted the particular binding.
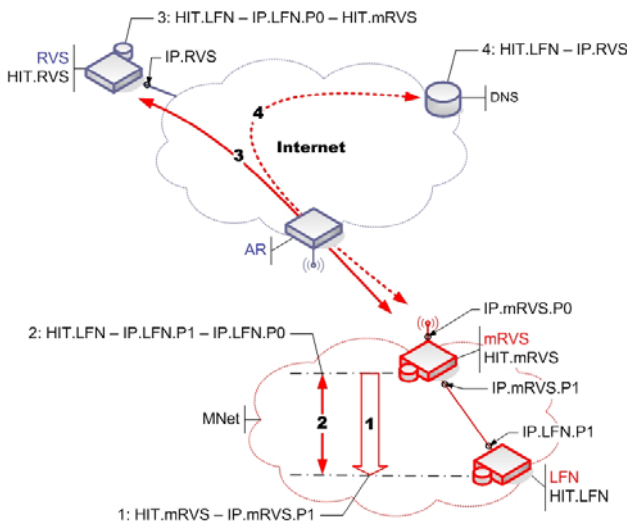

Figure 5. Initialization of a single NEMO scenario

Since the LFN is permanently connected to the mRVS it is an obvious choice to enable the mRVS to offer rendezvous service for the LFN. This can be a local policy setting (i.e. LFN knows the HIT and IP address of the mRVS) or can be announced with HIP service discovery mechanism (1). Either initiated by a local policy or by the reception of a SAP packet the LFN initiates the rendezvous registration mechanism with the mRVS. During the process the LFN also delegates its signaling rights to the mRVS. The main purpose of this registration is to get the mRVS to open a new HIT-IP binding entry in its database. Unlike standard RVS entities, which stores single {HIT – IP address} mapping records, the mRVS links this information with another IP address. This is a globally routable and topologically correct address, which is allocated and assigned by mRVS to the particular LFN. The role of this address is to provide global locator for LFN. As Fig. 5 depicts, mRVS assigned IP.LFN.P0 for LFN, while its actual IP address is IP.LFN.P1. One possible way to allocate a proper IP address for LFN is as follows. At registration LFN communicates on IP.LFN.P1. The mRVS simply changes the prefix (P1) of this address to P0, and leaves the remaining part of the address unchanged. Consider IP.LFN.P0 and IP.LFN.P1 as global unicast addresses, introduced in [50]. These addresses consist of two 64 bit long part, as Fig 6 shows.
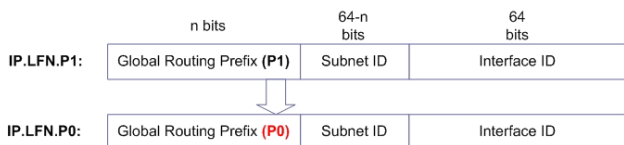

Figure 6. The address allocated by mRVS at LFN registration

The address assigned by mRVS to LFN should differ from the real address of LFN in the *Global Routing Prefix* (i.e.P1 and P0). The *Subnet ID* and the *Interface ID* remains the same.

As described above, LFN delegated its rights of signaling to mRVS. The first advantage of this process is that it enables mRVS to establish global reachability for the LFN. As Step 3 indicates, the mRVS registers the LFN at its standard RVS using the HIT of the LFN and the IP address assigned it. Moreover, the stored information is indexed by the HIT of mRVS. The role of this index is to enable mRVS to update bindings in RVS with sending only one UPDATE packet. The details are discussed in subsection D. Finally a DNS record has to be stored that links HIT.LFN to IP.RVS. This is also done by the mRVS and enables correspondent nodes to reach LFN (i.e. through the RVS).

Fig. 7 presents the process, in which a CN initiates a HIP association with an LFN. As [41] describes, if a HIP node wants to contact another one, it can initiate the connection in two different ways. If CN is aware of the IP address of its peer, CN can send I1 (i.e. the first packet of the Base Exchange) directly to this address. In case of unknown peer address CN should send the packet to the serving RVS of the peer.
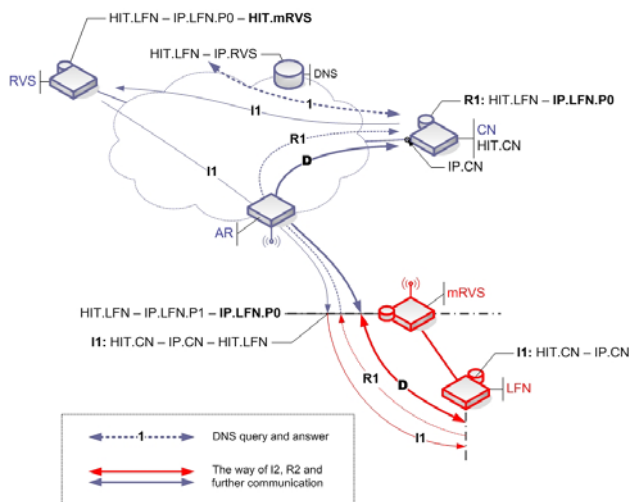

Figure 7. Connection establishment

Let's assume that in the scenario shown in Fig. 7 the CN initiates the connection through the RVS. As described above, the mRVS stored a {HIT.LFN – IP.RVS} record in the DNS thus, after a DNS query, I1 is sent to RVS. The server has the actual HIT – IP binding regarding LFN, according to which the RVS forwards I1 to the mobile network. As I1 reaches the mRVS it changes the destination address prefix (P0) to the actual prefix (P1) of LFN. Before forwarding I1 to LFN the mRVS learns the {HIT.CN – IP.CN} binding. This entry is indexed with the HIT of the LFN, which is used by the mRVS to perform necessary signaling functions (i.e. at sending updates). Finally LFN gets I1, learns the {HIT.CN – IP.CN} binding and continues the Base Exchange by sending R1, which source address is changed from IP.LFN.P1 to IP.LFN.P0 in the mRVS. The

R1 packet is routed directly to CN and at reception it obtains the {HIT.LFN – IP.LFN.P0} binding.

Finally the Base Exchange is finished and data is ready to transmit. Note that all the packets are routed between LFN and CN on the optimal path but all of them must be processed by the prefix changing function in mRVS. This provides seamless network mobility support for LFNs and ensures optimal routes. However, it has its prize, namely all HIT – IP address binding created at communication partners and at the RVS has to be updated if the whole mobile network changes its point of attachment. The mRVS is in charge to send these updates. On one hand mRVS has the right to do this (i.e. signaling delegation) and also ensures mobile network handovers transparent to LFNs. On the other hand, if large networks with lots of LFNs are in motion the mRVS might need considerable computational strength to fulfill all update needs. Note that here we mean large but not nested NEMOs because an mRVS is only responsible for nodes directly connected to it. For nodes in a nested subnet the mRVS of this subnet is responsible. The exact description of the handover management framework will be discussed under subsection D.

Concluding the protocol description introduced until now we feel worth to highlight the followings. There is a new network entity, mRVS, which is in charge to support seamless NEMO service for LFNs. The mRVS assigns a unique globally routable and topologically correct IP address different for each LFN This address appears in the source address field of the IP header of all packets traveling out of the mobile network. In the other direction a reversed change of the destination address is accomplished. Finally, mRVS stores information (HIT.CN – IP.CN) about LFNs' communication peers to be able to send the updates on behalf of the LFNs. This might be considered as a HIP level binding list entry.

For LMNs the same process is also applicable, and provides seamless NEMO management for them as well. In case of VMNs the solution can not provide transparency in means that every VMN has to inform the network about its presence and vice versa. Furthermore, VMNs have to delegate their signaling rights to the mRVS. A VMN might have active HIP connections and is already registered at an RVS. When it enters in the NEMO it receives SAP packets announcing the presence of the mRVS. In this case the VMN has to make a special registration at the mRVS, which is used to delegate signaling rights and to let mRVS to assign an IP address to the given VMN like it did in case of LFNs or LMNs. The information on CNs of a VMN shall be derived from the UPDATE packets that VMN sends to its CNs, when entering the NEMO. After this, VMNs can be handled in the same way as LMNs. Note that mRVS offers rendezvous service for VMNs (i.e. SAP), but they won't accept it since these nodes have been registered at another RVS before entering the NEMO.

C. Nested Mobile Networks

The most important issue in case of mobile networks is the management of nested mobile subnetworks. The appearance of such situations usually arise serious scalability issues. Thus an efficient NEMO solution has to cope with these scenarios in a scalable manner. In our proposal this is achieved as follows.

In HIP-NEMO nested subnetwork management is based on special inter mRVS signaling and a bidirectional tunneling between mRVSs. Inter mRVS communication manages introduction of new nested subnets in a MNet and nested subnet handover situations. The bidirectional tunnel is used for user data delivery between two mRVSs.

Fig. 8 depicts the simplest scenario. There are two initially individual mobile networks (MNet A, and MNet B). Both of them are assumed to have completed all necessary HIP-NEMO functions described above.
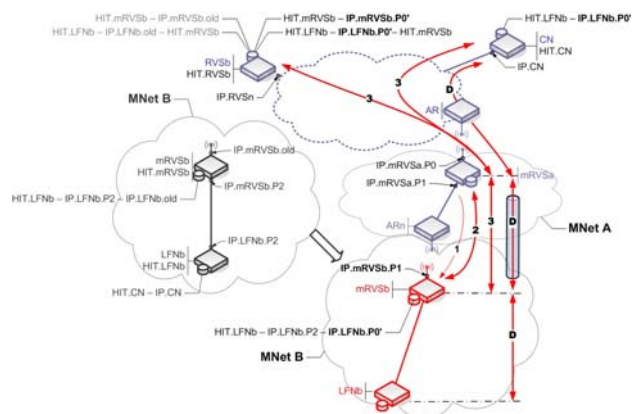

Figure 8.   Nested NEMO scenario

MNet B while in motion might enter the service area of MNet A and gets connection to the network through another mobile network itself. In case of situation shown in Fig. 8, mRVSb gets a P1 prefixed address (IP.mRVSb.P1) on its egress interface. In HIP-NEMO a nested subnetwork can realize the presence of a higher level mRVS (parent-mRVS) as this latter periodically sends SAP notifications (step 1). mRVSb (MNet B) sensing the presence of mRVS (MNet A), it initiates an inter mRVS registration (step 2). In this process the peers share information that helps efficient cooperation. The most important issue is that mRVS separates a part of the P0 address space (P0') and lends it to mRVSn to assign addresses to its MNNs (LFN, LMN, VMN). This enables mRVSa to decide weather the destination is in a nested subnet or not. Furthermore, mRVSa needs no further knowledge about nested subnets to be able to handle them. If a packet arrives form the public network holding a destination address that falls into that particular part of the P0 address space, which was given to mRVSb by mRVSa, the packet is forwarded towards mRVSb. This provides global reachability for nodes in nested subnets but have its prize as well. Packets traveling from and to the nested network would use invalid addresses as the network is using prefix P1 but these packets are addressed by P0 prefix addresses. That is why a bidirectional tunnel is needed to deliver P0-addressed packets in the P1 domain, to and from the nested subnet.

Finally mRVSb fulfills all update needs. The serving RVS and all CN of LFNb are updated (Step 3). The

complete discussion on handover framework can be found in the next subsection.

Note that in case of a lower level nested subnet that connects to MNet B, mRVSb would divide the P0' address space, and lend a P0" part of P0' to the mRVS of the lower level subnet (mRVSc). Furthermore, another bidirectional tunnel is created between mRVSc and mRVSb. Packets traveling between mRVSc and mRVSb are tunneled with P2 prefixed tunnel. This is modified to a P1 tunnel at mRVSb and packets are delivered on this to mRVSa rather than a new tunnel would be created. Thus there is no additional packet overhead if the level of nesting increases. Note that in NEMO BS this situation is handled with multiple tunnels, which degrades scalability.

D. Handover framework

In this section we describe some handover situations and how they are handled by HIP-NEMO.

Consider a situation when a single mobile network with one mRVS and a LFN connected to it moves away and connects to a new access point (Fig. 9). The egress interface of mRVS gets a new IP address. This also indicates that the mRVS has to assign a new IP address to the LFN. This is necessary since the IP address that the mRVS assigned to LFN needs to be topologically correct unless communication partners won't reach LFN.
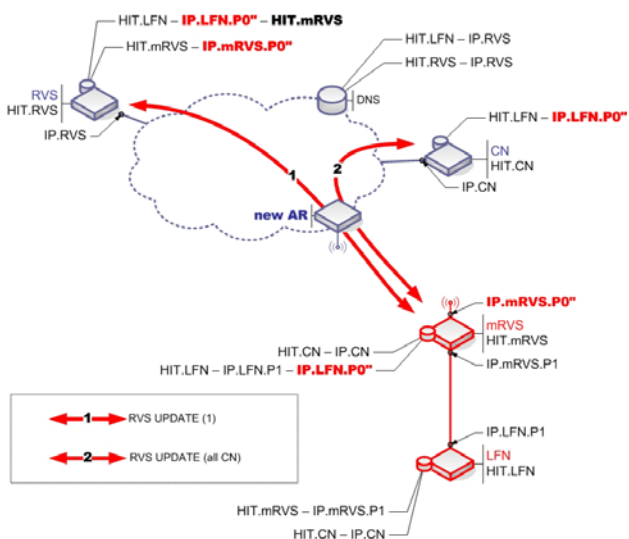

Figure 9.   A simple handover scenario

As mRVS has right to signal on behalf of LFN, it can send HIP UPDATE packets to the RVS and to all of the communication partners of LFN. The UPDATE packet sent to the RVS contains a LOCATOR parameter, which holds only the new prefix (P0") that mRVS uses on its new location. On reception of the UPDATE packet, the RVS will update the binding of the mRVS. Furthermore, all other bindings are updated that are indexed by the HIT of the mRVS. Note that only the prefix of the addresses in these bindings must be changed. This is applicable since only the prefix field is changed in the new IP address assigned by mRVS to LFNs, compared to the old address. The last 64 bits (assuming /64 networks) remains the same. Note that the "real" IP address of LFN is not

changed during the process and thus LFN is not included in the signaling mechanism. The same process can be used in case of LMNs existing in the mobile network.

It is a bit more complex scenario if there is a nested subnet in the mobile network. The nested mRVS have to be informed about the new address space it can use to assign globally routable and topologically correct IP addresses to its LFNs. Thus the root mRVS informs the nested one with an UPDATE packet, which holds a LOCATOR parameter that contains the new address range that can be used by the nested mRVS. On one hand, the nested mRVS send further UPDATE packets to lower level nested mRVSs. On the other hand it sends UPDATE packets to all communication partners of its LFNs. The serving RVS of the nested mRVS is also updated as the previous paragraph explains.

In the formerly described situations the whole mobile network changed its point of attachment. There are scenarios when *intra-NEMO* handovers have to be managed.

It is quite straightforward that if a nested mobile network changes its point of attachment, but still connects to the same mobile network, inter mRVS signaling is enough to handle the situation. The nested mRVS sends a single UPDATE packet to its higher level peer that holds the new locator of the nested mRVS. The tunnel used between the two mRVS is updated. Note that the handover is transparent to LFNs in the nested subnet.

Similar situation occurs if a LMN or a VMN changes its point of attachment to the same mobile network. However it raises some open issues. These will be discussed in Section VII.

VI.   EVALUATION

In order to evaluate our proposal we modeled, implemented and analyzed HIP-NEMO in a discrete event simulation system called OMNeT++ [51].

A. Metrics of Performance

To study the performance of HIP-NEMO and to compare it with NEMO Basic Support Protocol we used the following performance metrics:

- Handover latency (s) is defined as the time elapsed between the last packet arrived at the old access point and the first packet arrived at the new access point.
- Packet Loss (%) indicates the number of lost packets during a handover.
- Throughput (Kpacket/s) is defined as the amount of data received by the MNN during one second.

B. Scenarios and results

To examine how different environmental parameters which influence the performance of HIP-NEMO and NEMO Basic Support Protocol (NEMO BS) we used the simulation topology shown in Fig. 10. We defined one mobile network with one MNN. The mobile network is able to perform handovers between four different access points. In case of NEMO BS there is a Home Agent (HA) in the topology for the MR, and in case of HIP-NEMO

there is an RVS defined. This RVS acts as the standard RVS for all HIP nodes in the network including the mRVS as well. During the simulations the CN initiates a connection with the MNN, and than starts to send data packets to it. The MNN simply acknowledges the received packets.

In the first set of simulation runs we increased the delay between the HA/RVS and the central router (i.e. the delay of home link) and measured packet loss, handover latency and throughput.
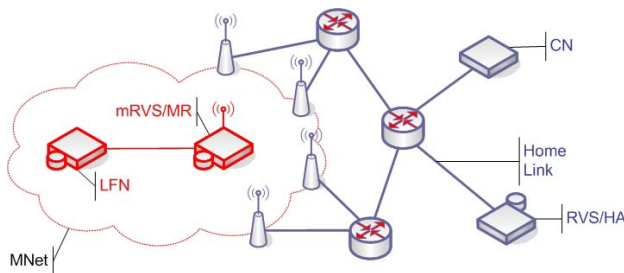

Figure 10. Simulation environment

Fig. 11 shows handover latency vs. home link delay for both NEMO BS and HIP-NEMO. The average of the handover latency and its maximum and minimum values are also depicted. Our goal was to prove that the distance of the RVS from the mobile network does not have impact on the performance of HIP-NEMO, while NEMO BS significantly increases handover latency . When using HIP-NEMO the traffic does not flow through the RVS thus the effect of increased home link delay on handover latency is minimal. NEMO BS is quite sensitive on home link delay as all data and signaling traffic bypasses the HA.
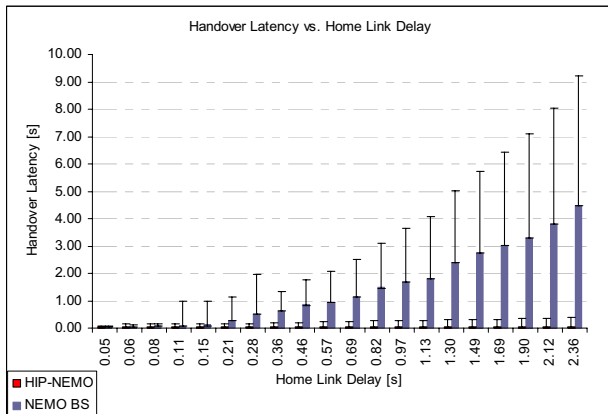

Figure 11. Impact of home link delay on handover latency

Fig 12 depicts packet loss vs. home link delay for both solutions. In these simulations the traffic rate was approximately 100 Kpackets/sec. The results are in relation with handover latency. The more the handover latency increases the more packets are lost during handovers. As handover latency was not much affected by home link delay in HIP-NEMO, the home link distance has no impact on packet loss as well. As shown, NEMO BS is far more sensitive on this.
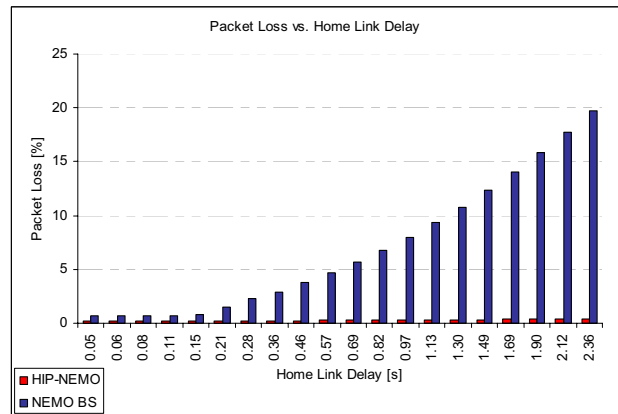

Figure 12. Impact of home link delay on packet loss rate

The second set of simulation runs was defined to examine the effects of handover frequency on the performance of HIP-NEMO and NEMO BS.

Fig. 13 depicts packet loss vs. handover frequency for both solutions. The result shows that the frequency of handovers (i.e. how often occurs a handoff) has significant impact on both solutions. The number of lost packets during handovers increases significantly with higher handover frequency. As in case of NEMO BS all signaling and data traffic flows through the HA, the rate of packet loss higher than it is when HIP-NEMO is used. Our solution builds optimal routes between communicating entities thus update information refresh bindings in CN earlier.
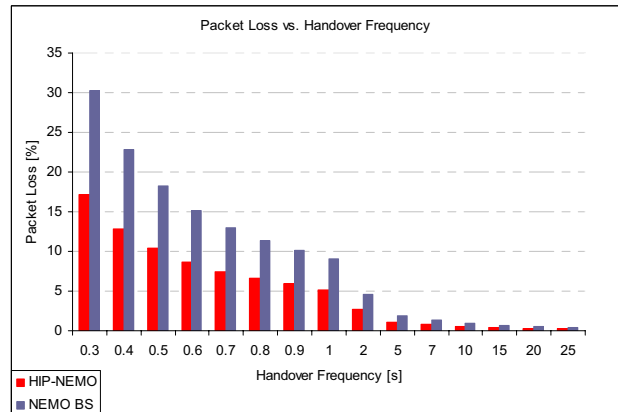

Figure 13. Impact of handover frequency on packet loss rate

On the last diagram (Fig. 14) we show that the relation between throughput and handover frequency reflects the results received in the latter analysis. We measured throughput for a given simulation term, during which no parameters were changed, after which we set up the simulation with decreased handover frequency. This iteration was repeated in case of some particular value of handover frequency. Fig. 14 shows how the average throughput, experienced during these simulation runs, relates to the parameter. The more packets lost during handovers the more the average throughput falls back.
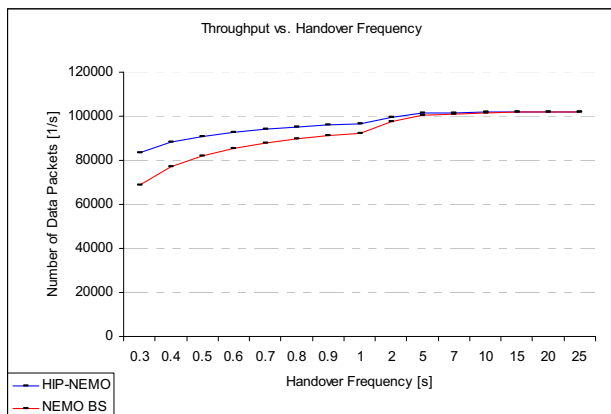
Figure 14. Impact of handover frequency on throughput

E. Security Considerations

The security strength of the proposal is derived from the generic security provided by HIP. In the current Internet where hosts are identified according to their IP addresses, the true advantage we get from HIP is a strong identification based on the cryptographic Host Identities. HIP enabled hosts can prove their identity by owning the private key part of their asymmetric Host Identity and signing data with it. With cryptographical identities, HIP enables authentication between end-points. Initialization of a HIP association is designed to protect the responder from Denial of Service (DoS) attacks. Communication confidentiality with HIP is established by encrypting the payload data.

Currently, the specified encryption format is ESP. Furthermore, HIP protects the integrity and confidentiality of payload data as well as integrity of control packets. HIP control packets can also be used to carry cryptographic certificates. Certificates can be used for authentication or authorization purposes by the peer host or intermediate entities. The latter property is a key issue, when considering secure signaling right delegation.

MNNs delegate their signaling rights to one (or more i.e. multihoming) mRVS in a secure way by sending registration packets that hold the correspondent certificate. Basic HIP security functions and secure delegation of signaling rights together provide secure location update.

Since signaling rights are delegated in a secure way and base HIP signaling messages are signed by the sender, location update signaling is protected. Service discovery that is used by mRVSs to advertise their presence and the rendezvous service they are offering for MNNs shall be considered as the security bottleneck of the solution. When a HIP host or a mRVS of a nested subnet receives a SAP packet from the network, either as a result of an active service discovery, or passively, it cannot know if the service provider is trustworthy or not. The SDP packet is unprotected, which makes it vulnerable. An attacker can modify the packet, or an attacker can send the packet using someone else's IP address and HIT. However, there are situations when nodes or moving networks have no other choice but to trust other nodes because there are no other means for

them to connect to the Internet. Note that MNNs delegate their signaling rights to the mRVS directly. In a singlehomed environment this is the only way for MNNs to connect to the public network. On the other hand, the decision of to whom shall I delegate my right of signaling becomes a more complex problem in multihomed environments.

VII.   OPEN ISSUES

In this section we discuss some open issues since there are some aspects, which we did not mention in the former sections. One is related to LMN and VMN handover management and the other is in connection with the division of the root address space.

A. Managing LMNs and VMNs

While providing NEMO services for LFNs is quite straightforward, the situation in which LMNs and VMNs has to be managed is a bit complicated.

The most important issue is related to mobility inside a mobile network. If a LMN or a VMN changes its point of attachment it starts to update all of its HIP associations. This generates unnecessary signaling load as these nodes are reachable through the same mRVS. Thus the nodes are reachable on the same address for their communication partners (i.e. the address the mRVS assigned to them). The only update that makes sense is the one performed with the mRVS. However, if we want to keep the transparency of the solution, these unnecessary updates are the prize to pay.

When mobile nodes inside a mobile network start to send updates to their nodes as a result of a handover inside the mobile network, the mRVS has no other choice but to let this signaling to get out of the mobile network. At reception of these updates the mRVS should also change the address, which it assigned to the sender mobile node. This is unavoidable thus sending updates with the same locator used before the update arrived might raise security problems.

A possible solution requires to give up some transparency, and to use a special micromobility service as in case of nested MNets. In order to achieve this there is a need for a mechanism that helps LMNs and VMNs to decide after a handover if they are in the service area of the same mRVS or not. HIP service discovery is a promising candidate for this function. On the other hand, handover management of LMNs and VMNs has to be modified to handle such situations.

B. Dividing the Root Address Space

There is a challenge in the solution that relates to nested subnet management, namely how to efficiently divide the base address space used by the root mRVS among nested subnets. There is a need for some dynamic method since NEMO environments are envisioned as temporary units changing their constellation quite often. A well designed solution must consider unlimited levels of nesting and number of MNNs. One possible solution is to enable the root mRVS to handle address space division management. However this centralized control obviously

provides an optimal solution, it generates huge amount of signaling in case of large and dynamic networks. On the other hand, a distributed control might provide only suboptimal results with lower signaling cost. Note that this is neither a HIP-NEMO nor a NEMO specific problem. This might arise in other networking scenarios, where a fixed IP address range has to be divided dynamically and/or on demand. Solving this problem is considered an interesting direction of future research and analysis.

VIII. CONCLUSIONS

In this paper we introduced a new approach to handle mobile networks based on HIP. All the major aspects of the idea have been introduced such as basic functions, management of nested subnetwork and handover framework. Concluding the paper we outline the main advantages and drawbacks of our proposal.

- The main advantage of HIP-NEMO is that it presents network mobility management integration to HIP by extending the usability of the base protocol. On the other hand HIP-NEMO benefits from being derived from HIP. Namely the effective security and mobility-multihoming framework of the base protocol is inherited.

- Focusing on network mobility management efficiency of HIP-NEMO, its primary advantage is that it uses direct routes between MNNs and their CNs. Furthermore, the proposal scales well with large and complex mobile networks. However, inter mRVS data flow needs to be tunneled, which introduces some packet overhead. Note that if the level of nesting increases the packet overhead stays constant in our proposal.

- One mRVS is responsible for MNNs directly connected (i.e. not through another mRVS) to it. In this sense the root RVS of nested mobile networks stores information about its own MNNs and manages their signaling needs. It has only one piece of information about nested subnets namely the HIT, the actual IP address and the address range that the nested mRVS uses to assign addresses to its MNNs. This indicates that the root mRVS of nested environments won't be overloaded by huge signaling process management.

- Our scheme provides a micromobility-like service for nested mobile networks. If a nested subnet moves inside a mobile network, it is enough to update the tunnel between the nested and the parent mRVS. This can be achieved so that the nested mRVS sends a single UPDATE to its parent networks mRVS. This reduces signaling overhead in certain NEMO scenarios.

Beyond the problems discussed as open issues in Section VII there are some further drawbacks of HIP-NEMO, and these are the following:

- The major disadvantage of the proposal is that it does not support completely seamless NEMO support for MNNs, as all kinds of these nodes need to delegate

their signaling rights to the actual mRVS. However, signaling delegation can be implemented as a HIP based service rather than as an extension or modification of the base protocol.

- An issue with the proposal's handover framework must be highlighted as well. If the whole MNet changes its point of attachment all the RVSs and CNs of all MNNs have to be updated, which generates serious amount of signaling in case of large MNets. Note that CNs must be updated individually. RVSs can be updated by a single UPDATE packet. However this can be considered as the cost of optimal routing.

The primary direction of our future work is to reduce the signaling overhead of our proposal by using bulk registrations, and extend the simulation evaluation and comparison study of HIP-NEMO. We are on the verge of implementing other network mobility supporting protocols (LIN6, SIP-NEMO) and NEMO-BS optimization extensions (ONEMO, MIRON, MoRaRo) in our simulation framework and compare them with HIP-NEMO. Furthermore, we are going to examine more complex NEMO scenarios like nested and/or multihomed environments to get more accurate results on the performance of our proposal. Finally we will start real implementation of HIP-NEMO, which will be deployed and analyzed in the ANEMONE testbed [29].

REFERENCES

[1] T. Ernst: "The Information Technology Era of the Vehicular Industry", ACM SIGCOMM Computer Communication Review (CCR), V36-I2, April 2006.

[2] T. Ernst, R. Kuntz, F. Leiber: "A Live Light-Weight IPv6 Demonstration Platform for ITS Usages", 5th ITST, Brest, France, June 2006.

[3] L.A. DaSilva, S.F. Midkiff, J.S. Park, G.C. Hadjichristofi, N.J. Davis, K.S. Phanse, Tao Lin: "Network Mobility and Protocol Interoperability in Ad Hoc Networks", IEEE Comm Mag., V42, I11, pp 88 - 96, November 2004.

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

[5] D. Johnson, C. Perkins, J. Arkko: "Mobility Support in IPv6", IETF RFC 3775, June 2004.

[6] E. Perera, R. Hsieh, A. Seneviratne: "Extended Network Mobility Support", IETF Internet draft <draft-perera-nemo-extended-00>, July 2003.

[7] C. Ng, E. Paik, T.Ernst, M. Bagnulo:"Analysis of multihoming in network mobility support", IETF Internet draft <draft-ietf-nemo-multihomingissues-06>, June 2006.

[8] C. Ng, P. Thubert, M. Watari, F. Zhao: "Network Mobility Route Optimization Problem Statement", IETF Internet draft <draft-ietf-nemo-ro-problem-statement-03>, Sept. 2006.

[9] C. Ng, F. Zhao, M. Watari,P. Thubert: "Network Mobility Route Optimization Solution Space Analysis", IETF Internet draft <draft-ietf-nemo-ro-space-analysis-03>, Sept. 2006.

[10] A. Petrescu, A. Olivereau, C. Janneteau: "Threats for Basic Network Mobility Support (NEMO threats)", IETF Internet draft <draft-petrescu-nemo-threats-01>, January 2004.

[11] N. Montavont, T. Noel, T. Ernst: "Multihoming in Nested Mobile Networking", IEEE SAINTW'04, pp 184-189, 2004.

[12] K. Park, S. Han, J Song: "Selective Handover Technique on Multihomed Mobile Network Environment", ICCS2006, Part II, LNCS 3992, pp. 1081-1088, 2006.

[13] R. Kuntz, J. Lorchat: "Building Fault Tolerant Networks Using a Multihomed Mobile Rouer: A Case Study", AINTEC2006, LNCS 4311, pp. 222-234, 2006.

[14] R. Han-Kyu, K. Do-Hyeon, C. You-Ze, L. Kang-Won, P. Hee-Dong: "Improved Handoff Scheme for Supporting Network Mobility in Nested Mobile Networks", ICCSA2005, LNCS 3480, pp. 378-387, 2005.

[15] S. H. Kim, Y. Y. Ahn, S. H. Kim, T. I. Kim: "Route Optimization Using RIPng Protocol in Nested Network Mobility", ICACT'06, February 2006.

[16] M.S Jeong, Y.-H. Cho, J.-T. Park: "Hierarchical Mobile Network Binding Scheme for Route Optimization in NEMO", Wireless Personal Communication, 10.1007/s11277-007-9257-4, 2007.

[17] M. Watari, T. Ernst, R. Wakikawa, J. Murai: "Routing Optimization for Nested Mobile Networks", IEICE Trans. Commun. Vol. E89-B, No. 10, Oct. 2006.

[18] M. Calderón, C. J. Bernardos, M. Bagnulo, I. Soto, A. de la Oliva: "Design and Experimental Evaluation of a Route Optimization Solution for NEMO", IEEE JSAC Vol. 24, No. 9., Sept. 2006.

[19] Ved P. Kafle, E. Kamioka, S. Yamada: "MoRaRo: Mobile Router-Assisted Route Optimization for Network Mobility (NEMO) Support", IEICE Trans. Inf. & Syst., Vol. E89-D, No. 1, January 2006.

[20] J. Bournelle, G. Valadon, D. Binet, S. Zrelli, M. Laurent-Maknavicius, J.-M. Combes: "AAA Considerations Within Several NEMO Deployment Scenarios", 1st WONEMO, Sendai, Japan, 2006.

[21] J. Ylitalo: "Re-thinking Security in Network Mobility", NDSS'05 Workshop, 2005.

[22] M. Calderon, C.J. Bernardos, M. Bagnulo, I. Soto, "Securing Route Optimisation in NEMO", WIOPT'05. pp 248-254, April 2005.

[23] S. Zrelli, T. Ernst, J. Bournelle, G. Valadon, D. Binet: "Access Control Architecture for Nested Mobile Environments in IPv6", SAR2005, Batz-sur-Mer, France, June 2005.

[24] K. Mihui, C. Kijoon: "A Fast Defense Mechanism Against IP Spoofing Traffic in a NEMO Environment", ICOIN2005, LNCS 3991, pp. 843-852, 2005.

[25] R. Kuntz, K. Mitsuya, R. Wakikawa: "Performance Evaluation of NEMO Basic Support Implementations", 1st WONEMO, Sendai, Japan, January 2006.

[26] M. Tsukada, T. Ernst: "Vehicle Communication Experiment Environment with MANET and NEMO", SAINTW2007, Hiroshima, Japan, January 2007.

[27] J. Montavont, J. Lorchat, T. Noel: "Deploying NEMO: A Practical Approach", 6th ITS Telecommunications 2006, pp. 1053-1056, June 2006.

[28] K. Lan, E. Perera, H. Petander, C. Dwertmann, L. Libman, M. Hassan: "MOBNET: The Design and Implementation of a Network Mobility Testbed for NEMO Protocol", LANMAN 2005, September 2005.

[29] T. Ernst, L. Bokor, A. Boutet, Y. Lopez: "An Open Network for Testing, Verification and Validation of IPv6-based ITS Components", ITST2007, Sophia Antipolis, France, June 2007.

[30] B. McCarthy, C. Edwards, M. Dunmore: "Applying NEMO to a Mountain Rescue Domain", ICOIN2006, LNCS 3961, pp. 10-20, 2006.

[31] T. Oiwa, M. Kunishi, M. Ishiyama, M. Kohno, F. Teraoka: "A network mobility protocol based on LIN6", VTC'03, V3, pp 1984 - 1988, October 2003.

[32] A. Banno, F. Teraoka: "vLIN6: An Efficient Network Mobility Protocol in IPv6", ICOIN2006, LNCS 3961, pp 3-10, 2006.

[33] H. Chung-Ming, L. Chao-Hsien, Z. Ji-Ren: "A Novel SIP-Based Route Optimization for Network Mobility", IEEE JSAC Vol. 24, No. 9., Sept. 2006.

[34] P. McCann: "Mobile IPv6 Fast Handovers for 802.11 Networks", IETF RFC 4260, November 2005.

[35] H. Soliman, C. Castelluccia, K. El Malki, L. Bellier: "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", IETF RFC 4140, August 2005.

[36] R. Moskowitz, P. Nikander: "Host Identity Protocol (HIP) Architecture", IETF RFC 4423, May 2006.

[37] R. Moskowitz, P. Nikander, P. Jokela, T. Henderson: "Host Identity Protocol", IETF Internet Draft <draft-ietf-hip-base-08>, June 2007.

[38] P. Jokela, R. Moskowitz, P. Nikander: "Using ESP transport format with HIP", IETF Internet Draft <draft-ietf-hip-esp-06>, June 2007.

[39] T. Henderson: "End-Host Mobility and Multihoming with the Host Identity Protocol", IETF Internet Draft <draft-ietf-hip-mm-05>, March 2007.

[40] T. R. Henderson, J. M. Ahrenholz, and J. H. Kim: "Experience with the Host Identity Protocol for Secure Host Mobility and Multihoming", IEEE Wireless Communications and Networking, V. 3, pp. 2120-2125 March 2003.

[41] J. Laganier, L. Eggert: "Host Identity Protocol (HIP) Rendezvous Extension", IETF Internet Draft <draft-ietf-hip-rvs-05>, Jun 2006.

[42] P. Nikander, J. Laganier: "Host Identity Protocol (HIP) Domain Name System (DNS) Extensions", IETF Internet Draft <draft-ietf-hip-dns-09>, April 2007.

[43] J. Laganier, T. Koponen, L. Eggert: "Host Identity Protocol (HIP) Registration Extension", IETF Internet Draft <draft-ietf-hip-registration-02>, June 2006.

[44] P. Jokela, J. Melen, J. Ylitalo: "HIP Service Discovery", IETF Internet Draft <draft-jokela-hip-service-discovery-00>, June 2006.

[45] P. Nikander and J. Arkko. "Delegation of Signaling Rights". Security Protocols 2002, LNCS 2845, pp 203-214, 2004.

[46] S. Jung, F. Zhao, S. F. Wu, H. G. Kim: "Threat Analysis on NEtwork MObility", ICICS2004, LNCS 3269, pp. 331-342, 2004.

[47] S. Herborn, L. Haslett, R. Boreli, A. Seneviratne: "HarMoNy - HIP Mobile Networks", Vehicular Technology Conference, 2006.

[48] Tat Kin Tan, Azman Samsudin: "Secure Hashing of the NEMO Mobile Router Communications", 2005.

[49] Sz. Nováczki, L. Bokor, S. Imre: „A HIP based Network Mobility Protocol", SAINT-WONEMO2007 (2007. 01.15-19.), Hiroshima, Japan, 2007.

[50] R. Hinden, S. Deering, E. Nordmark: "IPv6 Global Unicast Address Format", IETF RFC 3587, Aug. 2003.

[51] OMNeT++: A public-source, component-based, modular and open-architecture discrete event simulation environment. Official homepage: http://www.omnetpp.org/

Szabolcs Nováczki was born in Nagykanizsa, Hungary, in 9th February 1982. He received the M.Sc. degree in Electrical Engineering in 2006 from the Budapest University of Technology and Economics (BUTE), Hungary in the field of mobile communications and computer architectures.

He is currently a Ph.D. student at BUTE as the member of Mobile Communications and Computing Laboratory (MC2L) and Mobile Innovation Center Hungary (MIK). He is also a student member of IEEE.

His research interests include advanced network layer mobility solutions, new networking architectures, network simulation programming and network performance analysis.

László Bokor graduated with M.Sc. degree in Computer Engineering from the Budapest University of Technology and Economics (BME) at the Department of Telecommunicatons, in 2004. He also holds an M.Sc.+ Specialist of Bank Informatics degree from BME's Department of Information and Knowledge Management. He is a Ph.D. student at the same university, student member of the IEEE, member of Mobile

Communications and Computing Laboratory (MC^{2}L) and Mobile Innovation Center Hungary (MIK) where he participates in researches of wireless protocols and works on mobility management related projects (e.g. FP6-IST PHOENIX and ANEMONE). His research interests include IPv6 mobility, mobile computing, next generation networks, mobile broadband networking architectures, network performance analyzing, and heterogeneous networks.

Gábor Jeney received the M.Sc. degree in Electrical Engineering in 1998 from the Technical University of Budapest, Hungary in the field of mobile and optical communications. He received the Ph.D. degree in Electrical Engineering in 2005 from the same university, renamed meanwhile as Budapest University of Technology and Economics, Hungary in the field of multi-user detection. He also holds an M.Sc.+ Engineer-economist degree from the Budapest University of Economic Sciences and Public Administration, Hungary.
He is currently a Research Fellow at the Mobile Innovation Centre, Budapest University of Technology and Economics, Budapest, Hungary. He is involved in several national and European Commission funded project. His research interest includes neutral networks, mobile and wide-band communication systems, networking and transport protocols. He is a member of HTE (Scientific Association for Info-communications), Hungary since 1999, and he is a member of IEEE since 2000.

Sándor Imre is member of IEEE and HTE. He received the M.Sc. degree in Telecommunication Engineering from the Budapest University of Technology and Economics (BME) in 1993. In 1999 he obtained the Ph.D. degree in Electrical Engineering and D.Sc. in 2007. He is an Associate Professor at the Department of Telecommunications of BME and the R&D Director of the Mobile Innovation Center, Hungary. His research areas include IP mobility, routing, reliability; Wireless access; Software Defined Radio; Quantum Computing.