Keywords: Host Identity Protocol (HIP), network mobility (NEMO), multihoming, nested mobile networks, security

I. INTRODUCTION

In the last decade, mobile telecommunication has faced an enormous evolution. The convergence of the Internet and the mobile communication technologies generated increasing demand for more widespread and more sophisticated support of mobility. 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. Thus, when considering mobility management in next generation 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. On the other hand, communication sessions within entire mobile networks moving between different subnets need to be maintained. To allow network mobility in practice, several protocols and methods were designed and evaluated. NEMO Basic Support [4] is the most widespread network mobility protocol located in the IP layer which inherits the benefits of Mobile IPv6 while keeping the problems of the main approach such as protocol overhead and inefficient routing. There are extensions of NEMO Basic Support in order to allow multihoming and nested mobile networking [5], and ongoing researches are trying to deal with the route optimization and security problems [6], [7], [21]. However several novel real-life demonstrations [8] and testbeds [9] started to prove the feasibility and usability of NEMO Basic Protocol and its extensions, the searching for new ways of creating an “all-in-one” solution has not stopped [10]. In this paper we also try to present a new approach for network mobility by proposing a HIP based protocol to provide secure and effective NEMO solution. In order to do this, first we give a short overview of HIP with its Base Exchange and mobility management procedures. Than we describe our solution in Section 3, while section 4 is devoted to conclude the paper and present our future work.

II. HIP OVERVIEW

The Host Identity Protocol (HIP) [11], [12] is a multi-addressing and mobility solution for the IPv4 and IPv6 Internet. HIP is also a security protocol that defines host identifiers for naming the endpoints and performs authentication and creation of IPSec security associations between them. A new protocol layer is added into the TCP/IP stack between the network and transport layers. The new layer maps the host identifiers to network addresses and vice versa. This achieves the main architectural goal of HIP: the separation of identifiers from locations. In the traditional TCP/IP architecture, IP addresses serve both as identifiers and locators, which create problems for mobility and multihoming. The host identity (HI) in HIP is a public-key. This kind of identifier is selfcertifying in the sense that it can be used to verify signatures without access to certificates or a public-key infrastructure. The host identity is usually represented by the host identity tag (HIT), which is a 128-bit hash of the HI. IPv4 and IPv6 addresses in HIP are purely locators. The protocol is composed of three major parts. The endpoints first establish session keys with the HIP Base Exchange [13], after which all packets are protected using IPSec ESP. Finally, there is a readdressing mechanism to support IP address changes with mobility and multihoming [14]. There are situations where the simple end-to-end readdressing functionality is not sufficient (e.g. the initial reachability of mobile nodes, simultaneous mobility of nodes). To solve this issue a new network entity called the HIP Rendezvous Server (RVS) was introduced in [15]. The RVS stores the HIT-IP bindings for mobile nodes registered to it.

III. HIP EXTENSION SUPPORTING NETWORK MOBILITY

A. Protocol basics

In our proposal we extend HIP protocol in order to provide network mobility in the Host Identity Layer by
fulfilling the needs of nested and multihomed NEMO scenarios and optimal routes, all in a secure way. Furthermore, the solution should reduce signaling and packet overhead as well. In [16] we presented a HIP based micromobility solution, where a new network entity, called the Local Rendezvous Server (LRVS) was introduced. This is a special, HIP enabled gateway router, which provides micromobility service for mobile nodes beneath it. Mobile nodes entering in such a subnet get ICMP Router Advertisement messages sent by the LRVS that inform mobile nodes about the HIT and IP address of the LRVS, and the network prefix of the subnet. This enables mobile nodes to configure their IP address, and to register themselves at the LRVS. During this registration process the LRVS assigns a different (i.e. unique), globally routable and topologically correct IP address (IPg), for every registering mobile. If the registration process is completed, the LRVS acts the following way: it changes the source address in the IP header of outgoing packets (i.e. packets traveling outwards the subnet) to the IPg address assigned to the corresponding mobile, i.e. which sent the packet. For incoming packets the destination address is changed to the actual address of the mobile node. Since the IPg address – assigned to every mobile node in the subnet – remains the same until the mobile node resides in the given subnet, the movements of mobile nodes within a subnet are transparent for the rest of the network. Location updates in case of intra- and inter domain handovers are also discussed in [16]. This is achieved by the normal HIP update process defined in [14].

This idea can be extended to serve moving networks. The following three issues have to be taken into account. Firstly we have to consider a hierarchical topology of mobility enabled LRVSs (mLRVS), where it is possible for an mLRVS to connect to another one, which is in a higher level of the hierarchy. Basically a hierarchical micromobility configuration has to be managed. Secondly the MNNs have to delegate their signaling rights to the mLRVS at which they register. This right can be further delegated by any mLRVS to a higher level one. Thirdly an mLRVS has to track the connections of MNNs under it. Connection tracking and signaling delegation enables mLRVSs to signal on behalf of MNNs if the whole moving network changes its point of attachment.

**B. Managing the hierarchy**

To build up the hierarchical topology of moving networks and to track changes in the topology, two separate functions have to be performed. The first one is used to deliver hierarchy information from the top to the bottom: mLRVSs use HIP service discovery [17] to inform MNNs and other mLRVSs directly (i.e. not through another mLRVS) connected to them about their reachability (i.e. their HIT and IP address). The HIP service discovery is similar to IPv6 Neighbor Discovery, as it consists of special advertisement (Service Announcement Packet, SAP) and solicitation (Service Discovery Packet, SDP) messages (Fig. 1).

The second function relies on the first. When a MNN or an mLRVS learns the parameters of the higher level mLRVS, it can perform a registration process with it. During this registration process, the lower level mLRVS not only registers itself, but all the nodes located under it (Fig.1). The higher level mLRVS assigns a different, unique IPg for every registered node. These addresses are assigned according to the subnet prefix advertised by the higher level mLRVS.

The registration information spread up in the hierarchy until it reaches the root mLRVS, e.g. the mLRVS that connects directly to the Internet. With a function described above, all the mLRVSs in the moving network store information about all the nodes under them even if they are in a nested moving network. If the node is directly connected to a given mLRVS, this information is the HIT, the actual IP address of the mobile node and the IP address assigned by the mLRVS to the corresponding MNN. If the mobile node is in a nested moving network, these three parameters appear as a sub-parameter of the next mLRVS on the path to the node (Fig. 2).

Finally every node inside the moving network builds up its own picture of the hierarchy. A simple MNN only knows about the mLRVS at which it is registered, but an mLRVS has information about the higher level mLRVS at which it is registered as well as about MNNs and mLRVSs under it.

The root mLRVS (mLRVSa in Fig. 1) stores the
information depicted in Fig. 2. As shown, mLRV Sa knows that there is one MNN (i.e. MNN1) directly attached to it. The HIT and the actual IP address (i.e. IP1aI) are stored. These records are bound to another IP address (i.e. IP1aE), which is assigned by mLRV Sa to MNN1. The source address of packets originating from MNN1 is changed by mLRV Sa to this address. When a packet arrives to MNN1, mLRV Sa changes the destination address (i.e. IP1aE) to the actual IP address of MNN1 (i.e. IP1aI). Figure 2 also shows that mLRV Sa knows the HIT and IP address of mLRV Sb, and it has information about MNN2, too. It knows MNN2’s IP address (IP2bE) assigned to it by mLRV Sb. As in case of MNN1, mLRV Sb assigns an IP address (IP2aE) to MNN2 as well.

As mentioned above, the further described functions can be used to manage topology changes too. If a new mLRV S appears in the network or an old one vanishes, the service discovery process informs the network about it. If a MNN or a whole nested moving network changes its point of attachment, it uses HIP update mechanism to refresh its registrations. As mLRV S entities provide micromobility service for nodes under them, topology changes can be managed inside the moving network. Furthermore, if a MNN or a nested moving network changes its point of attachment but it is served by the same mLRV S, the only thing to do is to update this mLRV S. If the MNN or a nested moving network arrives at a service area of a new mLRV S, the update information has to spread up the topology, until it reaches the crossover mLRV S of the new and the old route to the corresponding node or nested network.

C. Signaling delegation and connection tracking

During the registration process the MNNs delegate their rights of signaling to the mLRV S at which they are registered. Moreover, an mLRV S may further delegate these rights to a higher level one. As a result, the root mLRV S has the right to signal on behalf of all the nodes in the moving network and lower level mLRV S(s) has the right to signal on behalf of all the nodes beneath it. The delegation of signaling rights and considerations related to this issue are detailed in [18].

If the root mLRV S of the moving network changes its point of attachment, it has to inform the communication partners of the MNNs. Thus if a MNN establishes communication contexts, the root mLRV S stores information about the partners to be able to signal on behalf of the MNN. The root mLRV S stores the HIT and IP address of the correspondent nodes (Fig. 2). If a nested moving network leaves the service area of an mLRV S and connects directly to the Internet, the serving mLRV S of this moving network becomes the root mLRV S. Thus communication contexts established by MNNs have to be tracked by all the mLRV Ss on the communication path to be able to signal on behalf of the MNNs.

D. Communication with RVSs and between mLRV Ss

As mentioned earlier, the base HIP protocol defines a special network entity called the Rendezvous Server (RVS), which acts as an initial rendezvous point for nodes intend to communicate with each other. Beyond the further described modifications there is a need to define the mode of interaction with the RVS system. In general, every HIP-enabled mobile entity (i.e. MNNs and mLRV Ss in our context), has to register at least one RVS. During the registration process the RVS learns the HIT-IP binding of the corresponding nodes. After registration the RVS can redirect HIP connection establishment packets to the actual location of the destination node. The serving RVS of a given mobile node can be learned by a simple DNS lookup [19].

In our solution MNNs registering at a given RVS (RVS2 in Fig. 1) do not register their IP address but the HIT of the root mLRV S. Packets send to this RVS are redirected to the serving RVS of the root mLRV S (see the numbered arrows in Fig. 1). The latter RVS stores the correct HIT-IP binding for all MNNs under the root mLRV S. In this RVS the bindings of MNNs appear as the sub parameter of the binding of the root mLRV S. The root mLRV S is responsible for creating these bindings and keeping them up to date.

E. Security considerations

The security strength of this proposal is derived from the 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 cryptographical 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 endpoints. 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) mLRV S 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 updates are protected. Service discovery that is used by mLRV Ss to advertise
themselves for MNNs is the security bottleneck in the solution. When a HIP host 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. On the other hand, the decision of who to delegate my right of signaling becomes a more complicated problem in multihomed environments [18].

IV. CONCLUSIONS

In this paper we provided a new network mobility solution called HIP-NEMO based on hierarchical micromobility topology, signaling delegation and connection tracking 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.

Compared to existing NEMO proposals such as [4], [6], [10], [21], our solution provides the following advantages. As the proposal is based on HIP, all of its advantages are inherited [12]. The signaling delegation and the hierarchical micromobility architecture should provide much less signaling and packet overhead than the basic MIP6-NEMO [8] solution. However this needs to be proved by simulations and further evaluations. Moreover, there is no need to use tunneling or encapsulation, and data packets (except the first packet of the Base Exchange) are traveling always on the optimal route. Optimizations for MIP6-NEMO solve the problems of optimal routes and packet overhead [6], and even security problems [20], but today none of them provides such a complete framework to address all these issues like our proposal. In [21] the author shortly sketches a HIP based idea for NEMO issues, but this highly relies on the ESP transport format. Our proposal is completely independent of the underlying transport protocol.

The advantages of our solution are clear, but there are drawbacks as well: our method is not transparent to MNNs, they have to register at mLRVSs. Furthermore, if the whole moving network changes its point of attachment the root mLRVS has to update the CNs of all the MNNs inside.

In the future we plan to go ahead in making HIP-NEMO a fully functional network mobility protocol by doing further investigations concentrating on performance analysis and comparison to other NEMO proposals.

ACKNOWLEDGEMENTS

This work was supported by the European FP6 IST project ANEMONE and the Mobile Innovation Center Hungary. The authors would like to thank all participants and contributors who take part in the work.

REFERENCES