

A HIP based Network Mobility Protocol

Szabolcs Nováczki, László Bokor, Sándor Imre

Budapest University of Technology and Economics, Budapest, Hungary

E-mail: {nszabi, goodzi, 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 (NEMO) is to provide continuous, optimal and secure Internet access to all nodes and even recursively nested mobile subnetworks inside a moving network. This paper describes a Host Identity Protocol (HIP) extension called HIP-NEMO, based on hierarchical topology, signaling delegation and connection tracking to enable secure and efficient network mobility support in the HIP layer.

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. Then 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

information depicted in Fig. 2. As shown, mLRVSA 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 record is bound to another IP address (i.e. IP1aE), which is assigned by mLRVSA to MNN1. The source address of packets originating from MNN1 is changed by mLRVSA to this address. When a packet arrives to MNN1, mLRVSA changes the destination address (i.e. IP1aE) to the actual IP address of MNN1 (i.e. IP1aI). Figure 2 also shows that mLRVSA knows the HIT and IP address of mLRVSB, and it has information about MNN2, too. It knows MNN2s IP address (IP2bE) assigned to it by mLRVSB. As in case of MNN1, mLRVSA 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 mLRVS 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 mLRVS 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 mLRVS, the only thing to do is to update this mLRVS. If the MNN or a nested moving network arrives at a service area of a new mLRVS, the update information has to spread up the topology, until it reaches the crossover mLRVS 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 mLRVS at which they are registered. Moreover, an mLRVS may further delegate these rights to a higher level one. As a result, the root mLRVS has the right to signal on behalf of all the nodes in the moving network and lower level mLRVS(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 mLRVS 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 mLRVS stores information about the partners to be able to signal on behalf of the MNN. The root mLRVS stores the HIT and IP address of the correspondent nodes (Fig. 2). If a nested moving network leaves the service area of an mLRVS and connects directly to the Internet, the serving mLRVS of this moving network becomes the root mLRVS. Thus communication contexts established by MNNs have to be tracked by all the mLRVSs on the communication path to be able to signal on behalf of the MNNs.

D. Communication with RVSs and between mLRVSs

As mentioned earlier, the base HIP protocol defines a special network entity called the Rendezvous Server (RVS), which acts like 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 mLRVSs 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 mLRVS. Packets send to this RVS are redirected to the serving RVS of the root mLRVS (see the numbered arrows in Fig. 1). The latter RVS stores the correct HIT-IP binding for all MNNs under the root mLRVS. In this RVS the bindings of MNNs appear as the sub parameter of the binding of the root mLRVS. The root mLRVS 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) mLRVS 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 mLRVSs 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 mLRVSSs. Furthermore, if the whole moving network changes its point of attachment the root mLRVSS 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

- [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, 111, 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] N. Montavont, T. Noel, T. Ernst: "Multihoming in Nested Mobile Networking", IEEE SAINTW'04, pp 184-189, 2004.
- [6] 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.
- [7] J. Bournelle, G. Valadon, D. Binet, S. Zrelli, M. Laurent-Maknavigius, J.-M. Combes: "AAA Considerations Within Several NEMO Deployment Scenarios", 1st WONEMO, Sendai, Japan, 2006.
- [8] R. Kuntz, K. Mitsuya, R. Wakikawa: "Performance Evaluation of NEMO Basic Support Implementations", 1st WONEMO, Sendai, Japan, January 2006.
- [9] 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.
- [10] 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.
- [11] R. Moskowitz and P. Nikander: "Host Identity Protocol (HIP) Architecture", RFC: 4423, May 2006.
- [12] Pekka Nikander, Jukka Ylitalo, and Jorma Wall: "Integrating Security, Mobility, and Multi-homing in a HIP Way", In Proceedings of NDSS'03, pages 87-99. Ericsson Research NomadicLab, February 2003.
- [13] R. Moskowitz, P. Nikander, P. Jokela and T. Henderson: "Host Identity Protocol", Internet-Draft, June 2006.
- [14] T. Henderson: "End-Host Mobility and Multihoming with the Host Identity Protocol", Internet-Draft, June 2006.
- [15] J. Laganier and L. Eggert: "Host Identity Protocol (HIP) Rendezvous Extension", Internet-Draft, June 2006.
- [16] Sz. Nováczki, L. Bokor, S. Imre: "Micromobility Support for HIP: Survey and Extension for Host Identity Protocol", MELECON 2006, Malaga, Spain, May 2006.
- [17] P. Jokela, J. Melen and J. Ylitalo, "HIP Service Discovery", Internet-Draft, June 2006.
- [18] P. Nikander and J. Arkko. "Delegation of Signaling Rights". In Proc. of the 10th IWSP, pp 203-212, Cambridge, UK, 2002.
- [19] P. Nikander, J. Laganier: "Host Identity Protocol (HIP) Domain Name System (DNS) Extensions", Internet-Draft, February 2006.
- [20] M. Calderon, C.J. Bernardos, M. Bagnulo, I. Soto, "Securing Route Optimisation in NEMO", WIOPT'05. pp 248-254, April 2005.
- [21] J. Ylitalo: "Re-thinking Security in Network Mobility", NDSS'05 Workshop, 2005.