International Journal of Wireless Networks and Broadband Technologies

January-March 2014, Vol. 3, No. 1

Table of Contents

Research Articles

The *International Journal of Wireless Networks and Broadband Technologies* is indexed or listed in the following: ACM Digital Library; Bacon's Media Directory; Cabell's Directories; DBLP; Google Scholar; INSPEC; JournalTOCs; MediaFinder; ProQuest Advanced Technologies & Aerospace Journals; ProQuest Computer Science Journals; ProQuest Illustrata: Technology; ProQuest SciTech Journals; ProQuest Technology Journals; The Standard Periodical Directory; Ulrich's Periodicals Directory

IGI PUBLISHING
WWW.IGI-GLOBAL.COM

Survey and Evaluation of Advanced Mobility Management Schemes in the Host Identity Layer

László Bokor, Inter-University Centre for Telecommunications and Informatics (ETIK), Debrecen, Hungary

Zoltán Faigl, Department of Networked Systems and Services (HIT), Budapest University of Technology and Economics (BME), Budapest, Hungary

Sándor Imre, Department of Networked Systems and Services (HIT), Budapest University of Technology and Economics (BME), Budapest, Hungary

ABSTRACT

This paper is committed to give an overview of the Host Identity Protocol (HIP), to introduce the basic ideas and the main paradigms behind it, and to make an exhaustive survey of mobility management schemes in the Host Identity Layer. The authors' goal is to show how HIP emerges from the list of potential alternatives with its wild range of possible usability, complex feature set and power to create a novel framework for future Mobile Internet architectures. In order to achieve this, the authors also perform an extensive simulation evaluation of four selected mobility solutions in the Host Identity Layer: the standard HIP mobility/multihoming (RFC5206), a micromobility solution (μHIP), a network mobility management scheme (HIP-NEMO) and a proactive, cross-layer optimized, distributed proposal designed for flat architectures (UFA-HIP).

Keywords: *Distributed and Dynamic Mobility Management (DMM), Handover Performance Evaluation, Host Identity Protocol (HIP), Host Identity Protocol Simulation Framework (HIPSim++), INET Notification Board (INET/OMNeT++), Micromobility, Network Mobility (NEMO)*

INTRODUCTION

Actual trends in mobile telecommunication show rapid growth of Internet related applications, and ever growing demand for them. The phenomenon of convergence in means of communication protocols, services and terminals accelerates this process: mobile applications are able to become more and more popular; users are willing to access Internet resources from their portable devices seamlessly, anytime and anywhere. The continuously growing number

DOI: 10.4018/ijwnbt.2014010103

of mobile users generates an increasing demand for more widespread and more sophisticated support of mobility, such creating serious challenges for the today's Internet architecture, which is the TCP/IP stack.

The Internet Protocol (IP) itself was designed in the 1970's, when all hosts of the early Internet were connected using wires: they were fixed hosts, not able to change their network point of attachment. That is why the basics of TCP/IP systems were not designed with any kind of mobility in mind. However, nowadays users are much rarely interconnected by wires: a remarkable mass of modern Internet devices are mobile and thus require the support of frequent changes in their network point of attachment. The shortcomings which make this support hard to provide come from the early days of the Internet. The most important one is the double role of IP addresses. On one hand an IP address identifies the host on the global network: all communication sessions initiated from or terminated at a given terminal is identified by its IP address. On the other hand, IP addresses have a topological locator role: a special network identifier belongs to IP addresses telling the position of the node on the Internet. In other words IP addresses have dual significance (i.e., being identifier and locator at the same time), thus becoming semantically overloaded. These two roles make things complicated and inconvenient when the host starts to move: if the node changes its network point of attachment (and thus its IP address), active communication sessions (which are mostly connected to the TCP/IP numbers) are interrupted and even lost in many cases. Obviously users want ubiquitous connection with seamless handovers and uninterrupted sessions, so engineers started to find an answer here.

One of the solutions for the above introduced problem space is a brand new protocol, which is called Host Identity Protocol (Moskowitz & Nikander, Host Identity Protocol (HIP) Architecture, 2006). HIP is a novel approach which decouples IP addresses from applications by proposing a new, cryptographic namespace to identify hosts or other network entities while IP addresses will remain to act as pure locators. In this architecture a novel layer (called the Host Identity Layer) provides separation of identifier (ID) and locator (Loc) roles of IP addresses (i.e., ID/Loc split): transport level connections are no more bound to IP addresses but to permanent IDs, which remain the same for the lifetime of the host. HIP such provides sophisticated and secure mobility/multihoming support, and creates a powerful toolset as the basis of several advanced mobility management schemes and extensions.

Our goal in this paper is to provide a broad survey of the existing HIP-based mobility management solutions and also to perform extensive simulation-based evaluation of key performance indicators related to handover events. Within this survey and evaluation we focus on four scenarios and extensions of HIP: the basic HIP mobility solution, and one of the earliest micro-mobility, network mobility and proactive distributed solutions (μHIP, HIP-NEMO, UFA-HIP, respectively). All of the three HIP extensions were developed by us in our previous works but this is the first time they are studied in complex simulation models and well-detailed handover scenarios focusing on the most important handover performance indicators.

The rest of this paper is organized as follows. The next section gives a general overview of the ID/Loc splitting paradigm together with the introduction of HIP, its fundamentals and main instruments. This is followed by the discussion of HIP's built-in mobility/multihoming support and the introduction of several enhancements, improvements and applications designed to extend the main standard with advanced capabilities in different topics of mobility management. Here we try to give a complete survey of existing HIP mobility solutions, but the focus will be on our previous works in the area of HIP-based handover management and optimization. We continue with the introduction

of our evaluation framework implemented in the INET/OMNeT++ discreet event simulation system which is followed by the introduction of our simulation scenarios, parameter settings and the analysis of the collected results. At the end of the paper we present our concluding remarks and discuss the expected future work.

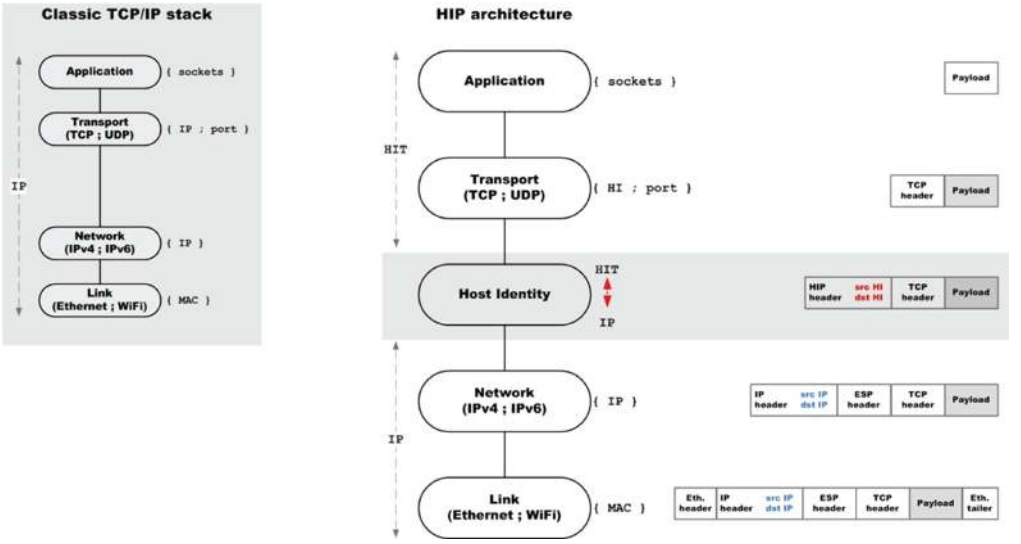
BACKGROUND

Current IP networks are based on two basic kinds of namespaces. On one hand there are human readable domain names which can be resolved to IP addresses by Internet applications via Domain Name System (DNS) lookups. DNS provides fast queries but it is not designed for fast updates and quick retrieval of dynamic information. On the other hand there are IP addresses used in the network layer as locator for packet routing purposes and also used as identifier in upper layers to refer to the host or a particular communication session. The inseparable bond between the locator and identifier functions of IP address makes it inconvenient or even impossible to design efficient and scalable mobility, multihoming, traffic engineering, routing and security solutions. Supporting heterogeneous network layer protocols or different locator families is also limited because of the same reason. The general concept of ID/Loc separation aims to eliminate the above problems and limitations by splitting the two roles of IP addresses and such allowing network layer to change locators without interfering with upper layer procedures. This separation makes the routing infrastructure more scalable, and by introducing a mapping function between IDs and Locs a natural and effective support of mobility and multihoming can be provided.

The concept gains more and more popularity: several different approaches exist for ID/Loc separation and it also has recently been introduced in the standardization activities of the ITU Telecommunication Standardization Sector (ITU-T) for integration in future network architectures (Y.ipsplit, 2009; Y.ipv6split, 2009). The common in all the existing standards, drafts and recommendations is the separation of identifiers from locators and applying a dynamic mapping mechanism between them, making the duplicate role of IP addresses disappear. They either use distinct namespaces for both functions (i.e., ID and Loc) or provide an architecture where the nature of the split is operational.

Host Identity Protocol uses the first approach: IP addresses continue to act as pure locators, while the identification role is handled by a newly introduced, globally unique namespace (the Host Identity namespace), that is a special pool of identity representations called Host Identifiers (HIs). The elements of the Host Identity namespace are public keys of asymmetric key pairs (i.e., self-certifying cryptographic names) used to identify nodes and to integrate strong security features such as authentication, confidentiality, integrity and protection against certain kind of Denial-of-Service (DoS) and Man-in-the-Middle (MitM) attacks. Furthermore, based on the cryptographic HIs special certificates can be generated by the nodes for secure signaling (Nikander & Arkko, Delegation of Signaling Rights, 2004) or even identity delegation (Herborn, Huber, Boreli, & Seneviratne, 2007), offering enormous resource savings, effective session mobility and other promising application possibilities in wireless and mobile environments. However, HIs are rarely used in actual HIP protocol packets, instead hash representations called the Host Identity Tag (128 bit long for global, IPv6-based communication) and Local Scope Identifier (32 bit long for local usage and IPv4 compatibility) are applied. HIP related signaling information is conveyed within HIP headers having a form of a standard IPv6 extension header. Every HIP compatible node has at least one HI and implements the functions required to handle the new namespace and the relevant mechanisms. Therefore the scope of the protocol includes the modifications and new methods designed to integrate the concepts of HIP into the existing Internet architecture. As Figure 1 shows,

Figure 1. The host identity layer

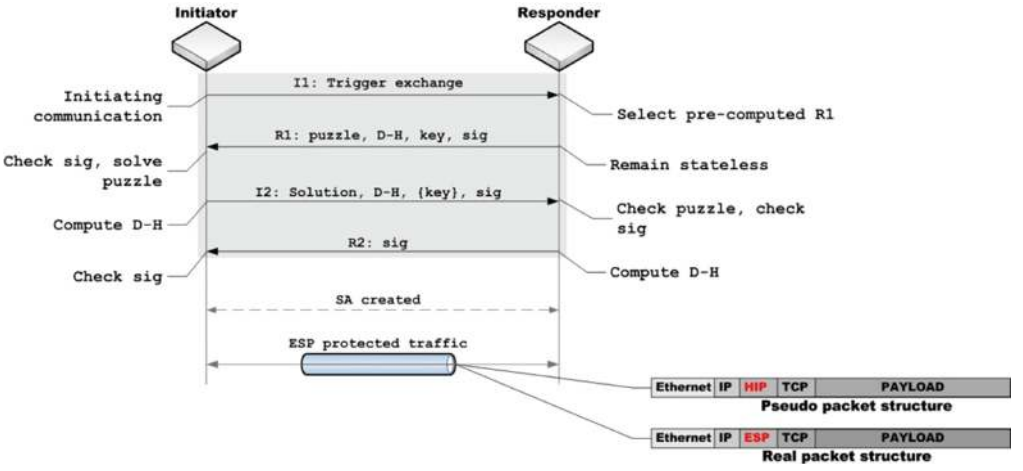


these functions and TCP/IP extensions form a new protocol layer, which resides between the transport and network layer in the TCP/IP reference model (Moskowitz & Nikander, Host Identity Protocol (HIP) Architecture, 2006).

The basic function of HIP is to set up Host Identifier based connections between nodes and to map HIs to IP addresses and vice versa. A HIP association can be established between two nodes (i.e., an Initiator and a Responder) by a four way end-to-end security handshake called the Base Exchange (BEX) (see Figure 2).

The BEX performs mutual authentication based on the peers' asymmetric keys and

Figure 2. HIP base exchange



implements a Diffie-Hellman key exchange to create symmetric keys for later payload encryption. Additionally, a special puzzle-solution mechanism is applied to protect the responder against certain DoS attacks. As a result of a successful HIP Base Exchange an IPsec Security Association pair is created between the peers where SAs are bound to HIs instead of IP addresses (Moskowitz, Nikander, Jokela, & Henderson, 2008). After the BEX, payload data is passed between the peers using the Encapsulating Security Payload (ESP) through a special ESP tunnel. A new transport mode of ESP was designed especially for HIP (Jokela, Moskowitz, & Nikander, Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP), 2008). This so called Bound-End-to-End-Tunnel (BEET) mode integrates the ESP tunnel mode with the low overhead transport mode. Using BEET mode the outer IP header of the ESP packet holds the IP addresses of the peers but the inner header is missing. Instead the Security Parameter Index (SPI) is used to identify the correspondent HIP association by reception at the destination. Thanks to the BEET mechanisms HIP related signaling information (i.e., HIP header with source and destination HITs, and HIP parameters) must be applied only to HIP control packets but not in case of data transfer messages.

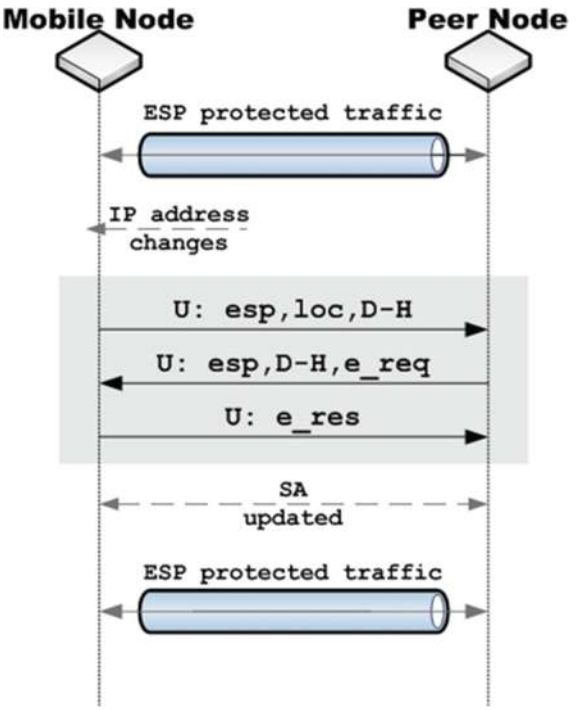
During HIP operation IP addresses (i.e., locators) are intended to be used mostly for "on-the-wire communication" between peer hosts, while upper layer protocols and applications use HIs (or HITs) instead. This implies the need of some method to translate domain names to HIs. Using the existing infrastructure of DNS for this translation is quite straightforward. Therefore (Nikander & Laganier, Host Identity Protocol Domain Name System Extension, 2008) designed a new resource record for the DNS, and laid down how to use it with the Host Identity Protocol. This novel resource record allows a HIP node to store its Host Identity and other relevant information (e.g., HIT) in the DNS.

BASIC HIP MOBILITY AND MULTIHOMING SUPPORT

The base specification of HIP describes a secure locator update procedure, which we describe here in detail. The procedure is used to maintain the HIT-IP mappings between the communicating peers (Nikander, Henderson, Vogt, & Arkko, 2008). The mobile endpoint informs partners that its location has changed. Inherited from the key idea of HIP the update procedure does not affect higher layer connection. The procedure is transparent for all established connections of the transport or application layers. This property makes HIP an exciting ground to develop sophisticated mobility schemes or use it to handle more complicated and advanced mobility scenarios like micromobility (Bokor, Nováczki, & Imre, A Complete HIP based Framework for Secure Micromobility, 2007), network mobility (Nováczki, Bokor, Jeney, & Imre, 2008), per-application mobility (Bokor, Zeke, Nováczki, & Jeney, 2009), or distributed mobility (Bokor, Faigl, & Imre, A Delegation-based HIP Signaling Scheme for the Ultra Flat Architecture, 2010; Faigl, Bokor, Neves, Daoud, & Herbelin, Evaluation of two integrated signalling schemes for the ultra flat architecture using SIP, IEEE 802.21, and HIP/PMIP protocols, 2011). The update sequence is illustrated on Figure 3.

This is the most simple mobility scenario specified for HIP. There are two HIP capable nodes, which have established communication sessions. Note that their higher layer connections are bound to HITs instead of IP addresses. In case the IP address of the mobile node is changed, it will trigger a HIP update procedure by sending an UPDATE (U) message to its peer(s). This delivers the new location information (loc) and informs the peer if the mobile wants to update the security parameters (esp). If there is a need for refresh, the mobile also sends the updated parameters (D-H). The update procedure is proved to be protected against security attacks. On one hand

Figure 3. The HIP UPDATE procedure



all the messages are digitally signed by the peers,authenticating the origin of the message and the message for any party using the HI of the sender. On the other hand there is a built in protection against distributed Denial-of-Service attacks. The second and the third message of the update procedure implements this. The peer node receiving the first UPDATE packet verifies the signature and answers with another UPDATE packet. This includes information to update the security parameters (esp and D-H) and a data block that contains a nonce (e_req). This must be echoed back by the mobile node in the third UPDATE packet (e_res). This simple echo request-response sequence verifies the new address of the mobile node.

A related functionality of HIP is host multihoming. In case of multihoming the HIP node owns more than one physical interfaces and/or global addresses. However the update procedure described above is used to update the primary locator of HIP nodes, a multihomed node can inform its peers about secondary locators it is reachable at. It is recommended to use different SAs for different interfaces and/or addresses. To do this, a multihomed HIP host creates a new inbound SA and a corresponding SPI. This is also managed by the update procedure. The first UPDATE packet should hold an ESP_INFO parameter having the NEW SPI field set to the newly created SPI value and setting the OLD SPI field set to zero. The packet also contains a LOCATOR parameter that indicates the new address-SPI mapping and the old one as well. Peers will use the primary locator as long as it is available and can switch to one of the secondary locators upon loss of connection.

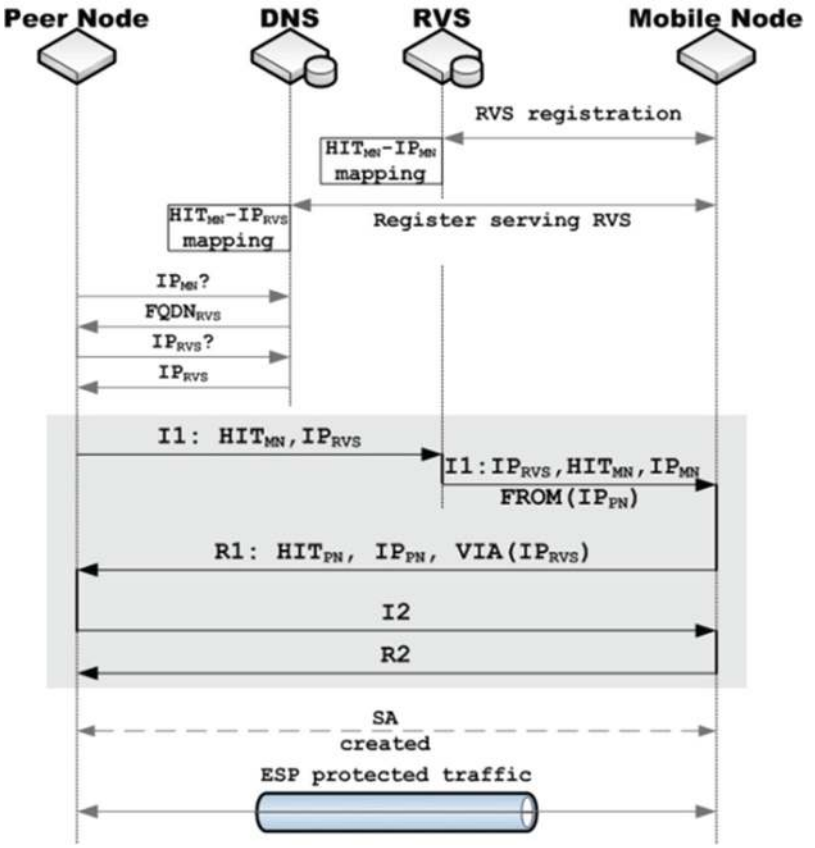
The above introduced update procedure for mobility and multihoming can handle locator changes in case there are ongoing HIP sessions between the endpoints. However this is not a solution for initial reachability of mobile nodes and cannot cope with simultaneous mobility of endpoints. Initial reachability is the problem

about how to provide a permanent anchor point for mobile nodes that makes it able to reach them no matter what their actual location is. Simultaneous end-host mobility covers scenarios where both endpoints are moving away from their location more or less parallel. Thanks to this the UPDATE messages cannot reach their destination. The messages are delivered to the old locations of the peers and the partners will lose each other and they have to restart their common session(s).

There is an extension in HIP standards that introduces an anchor point called the Rendezvous Server (RVS) to solve the above cases (Laganier & Eggert, Host Identity Protocol (HIP) Rendezvous Extension, 2008). Figure 4 shows the service the RVS provides for mobile HIP nodes to handle scenarios described above.

The RVS is known to every potential peer nodes by e.g., DNS queries. The RVS stores the actual HIT-IP mapping for registered mobile nodes. The Base Exchange is assisted by the RVS to enable connection establishment for the peers. Here we describe the sequence in detail. First the mobile node has to register itself at the RVS to use the offered service (Laganier, Koponen, & Eggert, Host Identity Protocol (HIP) Registration Extension, 2008). This creates an entry in the RVS database that holds the HIT-IP mapping for the mobile. The entry is updated time-to-time by the mobile if its IP address changes. After registration the mobile informs the DNS indicating its serving RVS. At this point any potential peer can initiate a HIP connection with the mobile. The peer performs DNS queries to get to know the

Figure 4. Operation of HIP RVS mechanisms



serving RVS of the mobile it wants to reach. This is a two-stage query. First the peer asks the IP of the mobile node indicating its domain name. The DNS returns the domain name of the RVS. In the second stage the peer asks the IP address of the RVS and the DNS returns its IP address. Now the peer can trigger the Base Exchange by sending the I1 message. This is delivered to the RVS. The anchor point knows the actual IP address of the mobile node and modifies the I1 message accordingly. The RVS also attaches an additional data field to the message that identifies the original sender of the message (FROM(IP_{PN})). The message is delivered than to the mobile, which continues the Base Exchange by sending the R1 message. This also contains an additional parameter, which verifies that the I1 message was forwarded by the RVS (VIA(IP_{RVS})). Finally the connection setup finishes in the regular way without the inclusion of the RVS. Note that the RVS is used only in the connection setup. Any other communication (signaling or data) between the peers is transferred in the direct path. The similar process must be followed when the endpoints are changing IP addresses parallel. In this case the HIP connection is broken and must be reestablished.

However, there is another extension for HIP that solves simultaneous end host mobility in a more sophisticated way than the standard RVS scheme. In (Hobaya, Gay, & Robert, 2009) the authors define an extension to HIP which improves mobility management of the core protocol. The proposal defines that mobile nodes are configured to send all UPDATE messages to the serving RVS of the correspondent nodes. As mobiles nodes always update their RVS upon mobility the latter will always have an up-to-date mapping between the HIT and IP address of mobile nodes. UPDATE messages sent to the RVSs are never lost and are delivered to the correct location. Note that opposed to the standard HIP mobility framework, this extension suggest that RVSs should be always included in the update process. Nodes do not have to wait the regular update process to fail first but they can immediately involve RSV entities. This of course ensures the delivery of UPDATE packets but introduces unnecessary delay in non-simultaneous mobility scenarios.

ADVANCED MOBILITY MANAGEMENT IN THE HOST IDENTITY LAYER

The Host Identity Protocol was created with basic host mobility a simple multihoming support in mind as important part of the main design principles. However, the flexibility of the protocol enables the design of advanced mobility management schemes built on the top of the base specification.

Micromobility

Access systems of modern mobile architectures commonly consist of one or more domains providing users with topologically valid IP addresses and connecting users to the IP core through the wireless interface. These domains of wireless access networks can be aggregated and special protocols can be assigned for local mobility management of the group of domains in order to offer fast and seamless handover control over a limited geographical area. In such cases we speak about micromobility, and the aggregated group of domains is called micromobility domain. Mobility management solutions of such structures (i.e., micromobility protocols) are specially designed for environments where mobile terminals change their network points of attachment so often that the general mobility management protocols (i.e., macromobility solutions) originate excrescent overhead and ineffective operation.

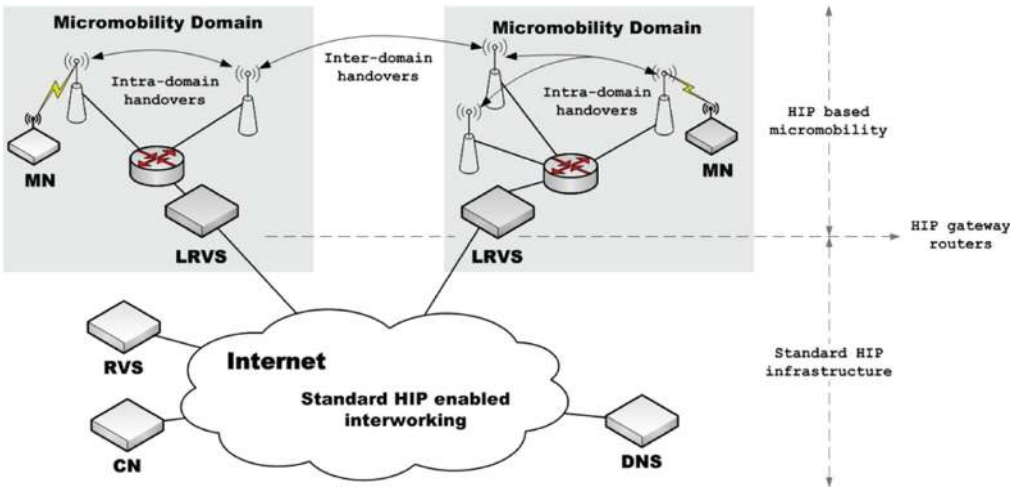
Basic HIP mobility mechanisms are only for macromobility support and further extension of the base protocol is needed for micromobility. The original idea of integrating micromobility with HIP was presented by Ylitalo, Melén, Nikander, et al. (2004) and Ylitalo, Melén, Nikander, and Torvinen (2004) where a secure micromobility management scheme based on Lamport one-way hash chains and secret splitting techniques was introduced for IP networks.

However, this scheme is not built on an effective and intact micromobility model as it only focuses on the security issues and it also does not consider protocol details regarding the operation and the mobility support. Moreover, in this method MNs still need to update their location information at the RVS during the handover, therefore the scheme cannot fulfill the requirements of micromobility architecture: it is only a partial answer for the complex problem.

The first complete solution for HIP-based micromobility management was presented in Nováczki, Bokor, and Imre (2006), and Bokor, Nováczki, and Imre (2007) where we introduced a novel HIP gateway entity called the Local Rendezvous Server (LRVS) which is responsible for managing HIP Mobile Nodes (MNs) in a given domain (see Figure 5 for details). LRVS gateways provide HIP registration service for users in the domain, and also introduce an IP address mapping function which is used to attach the MNs to the μHIP access network by registering the local locators (IP_L) of MNs. IP_L is valid only in the given domain and the LRVS is responsible for mapping every IP_L to a globally routable address (i.e., global locator, IP_G) chosen from a private address pool. IP_G is used to register the MNs at their RVSs and to deliver packets outside the micromobility domain during further communication sessions.

The basic operation of this architecture starts with an initialization mechanism right after the MN joined the domain. First the MN physically connects to one of the access routers (AR) of the domain, then gets the local locator based e.g. on IPv6 stateless autoconfiguration. After this, the MN either may actively initiate a HIP service discovery procedure (Jokela, Melen, & Ylitalo, HIP Service Discovery, 2006) or passively wait for a service announcement in order to detect the LRVS service provided in the visited micromobility area. In some way the MN will be informed about the HIT and the IP address of the LRVS responsible for its actual domain, and will register itself to the LRVS with the Base Exchange sequence. During this service discovery and registration procedure the LRVS not only registers the MN's HIT with the new IP_L, but maps IP_L with a globally routable address (IP_G) as well. After the MN successfully registered at the LRVS (with the HIT_{MN}-IP_L-IP_G triplet), it needs to perform the update and/or registration procedures at its RVS and current CNs (with the HIT_{MN}-IP_G pair) in order to be reachable for the current and possible future communication partners. Therefore

Figure 5. μHIP architecture



the MN – strongly relying on the self-certifying cryptographic identifiers provided by HIP and on the mechanisms introduced by (Nikander & Arkko, Delegation of Signaling Rights, 2004) – delegates its signaling rights to the LRVS at which it is registered. The appropriate certificates are sent after the BEX, resulting that the LRVS will own the rights to signal on behalf of all MNs in the micromobility domain under its authority. In possession of these delegated rights the LRVS is able to securely register or update to the RVSs and CNs on behalf of the MNs with the IP_G global locators assigned to them.

During μHIP connection establishment between already initialized MNs initiator starts the Base Exchange and sends the first packet (I1) which will be intercepted by the LRVS in the initiator's domain. This LRVS changes the source IP address of the I1 packet to the initiator's global locator and sends the packet to the RVS of the responder. The RVS forwards the packet towards the responder's registered global locator thus reaching its serving LRVS which knows the actual location of the responder, so the packet can be forwarded by changing the destination IP address of the I1 packet to the responder's actual local locator. The Base Exchange continues in the regular way, without the inclusion of the RVS, but with the address mapping function of the two LRVSs. This message flow builds up an active HIP association between the initiator and responder, so they can begin sending data packets to each other.

In case of intra-domain handovers the MN will receive a new IP_L from the new Access Router belonging to the serving LRVS. In this case the MN – realizing the change of its IP address – uses (Laganier, Koponen, & Eggert, Host Identity Protocol (HIP) Registration Extension, 2008) to update its registration (and if needed its delegation certificate as well) with its new IP_L at serving LRVS. It is important to note that neither the CNs of the mobile node nor the RVS has to be informed about the movement as the address changes are locally handled by the proposed micromobility extension. The movements of nodes are completely hidden from the outside world resulting in less signaling overhead, packet loss and handover latency.

In case of inter-domain handovers the mobile node moves between local administrative domains thus invoking the macromobility management procedures. Arriving at the new domain, the node will receive a new local locator, and will discover the service parameters of the new LRVS. After the MN realized that it leaved the previously used micromobility domain by entering a new one and learned the HIT and IP address of the new LRVS, it performs the initialization mechanism. Since MN changes its old LRVS, it also has to update its RVS and all the correspondent nodes with ongoing communication.

(Bokor, Nováczki, & Imre, A Complete HIP based Framework for Secure Micromobility, 2007) proposes a paging extension to μHIP in order to effectively locate a particular mobile node whose current position is not accurately known in the network, to reduce signaling costs and to save power consumption of MNs. The solution is based on the HIT specific multicasting (HISM) proposal (Kovácsházi & Vida, 2007) and implements an efficient location tracking that distinguishes between active and idle MNs, applies multicast group IP addresses for identification of paging areas (PA) in the system, and uses HISM mechanisms for passing paging messages to MNs through the multicast tree (built and maintained based on HIT information) of the MNs actual paging area.

The work of Yang S. et al. (2008) also describes a HIP paging extension called P-HIP where LRVSs are controlling paging areas identified with the LRVSs' HIT, and – as the network always knows the current paging area of the mobile node – paging request messages are broadcasted towards all access routers in the paging area in order to find an idle MN. The main feature of P-HIP is similar to the HISM based paging scheme: only active MNs must update their locators when they move within the same paging area.

Several extensions of μHIP were published using the original proposal as a basis for further

optimization of HIP mobility mechanisms. So and Wang (2008) introduced mHIP which introduces hierarchy in the micromobility domains by defining two different types of nework agents: mHIP gateways and mHIP routers. The main roles of these agents are to handle HIP-based signaling messages of the intra-domain handovers, and to re-direct the connections to the correct location. All mHIP agents in this scheme can sign the message on behalf of the whole group. The mHIP gateway is basically an LRVS: it is the root of all mHIP routers in a domain keeping the location information of the MN inside the domain. The mHIP router is a HIP layer router that redirects HIP sessions to the MN's current location. mHIP routers are also able to handle the intra-domain handover signaling inside the domain so that the handover latency and load of the mHIP gateway can be further reduced. Description of operation within multihoming scenarios is also included in mHIP.

Muslam, Chan, and Ventura (2009) designed an extension aiming to improve intra-domain communication of μHIP. The scheme also presents a new entity called Co-Agent (Co-A) for each domain. Co-A is responsible for managing MNs in the given domain and for acting as virtual Mobile Nodes and Corresponding Nodes during both intra- and inter-domain handovers in order to reduce the number control messages required in mobility management. In this framework the LRVS still manages the connectivity between domains' access networks and the Internet.

DH-HIP (Dynamic Hierarchical HIP) is also a HIP-based micromobility management scheme introducing a three level architecture of rendezvous servers as Rendezvous Server (RVS), Gateway RVS (GRVS) and Local RVS (LRVS), respectively. In this scheme (Yang, Qin, & Yang, 2007) the size of a domain managed by a LRVS is determined dynamically by the MN itself, according to the packet arrival rate and mobility status after LRVS selection. The network in the presented DH-HIP architecture is divided into autonomous and administrative domains, where autonomous domains may consist of several administrative domains. LRVSs are managing the administrative domains, while GRVSs are responsible for the autonomous ones. GRVS nodes are dealing with the control of the communication between the LRVS and MNs.

eHIP (Early Update for HIP) improves handover latency by applying two basic concepts: the hierarchy and the anticipation of the location update process of HIP (Aydin, Chaouchi, & Zaim, 2009). In addition to the introduction of a hierarchical domain approach, this scheme also extends μHIP with an early update mechanism in which MNs obtain their new IP addresses from the network they are about to enter and make their registration before the actual handover process. Such an early update handover can be triggered based on different parameters applied to the handover decision engine of the MN.

Iapichino, Bonnet, Herrero, Baudoin, and Buret (2009) and Iapichino and Bonnet (2009) propose to merge the advantages of network-based micromobility management of Proxy Mobile IPv6 (PMIPv6) with HIP's macromobility management, security, vertical handover and multihoming capabilities. This integrated HIP-PMIPv6 approach results in a system architecture with double benefits. On one hand it incorporates an efficient micromobility extension of HIP. On the other hand it supports PMIP with macromobility management skills in a framework where users can securely use the different access technologies for connecting their multihomed devices and also can move sessions from one interface to another one without breaking the already established secure associations, such being connected to the always best network available.

Network Mobility

Network mobility (NEMO) is one of the latest scenarios discovered in the mobility management research area. Protocols addressing networks in motion has to deal with mobility of whole networks, not only single endpoints. Moving networks are usually consisting of one or more mobile routers (MR) and several different mobile network nodes (MNN) connected to the MR. The MR is the gateway to

reach the rest of the network for MNNs. All data and control signaling sent by the MNNs are traveling through the MR. The task of the MR is to provide uninterrupted connection for MNNs and handle mobility situations so that it is transparent to the MNNs. MNNs are not limited to single end terminals, they can also be whole mobile networks such creating nested NEMO structures. Such a nested network may contain multiple levels of moving networks attaching and detaching dynamically each other. To handle such complicated mobility scenarios there is a need for a very effective, scalable, flexible and secure solution. Host Identity Protocol provides a strong basis for such an extension.

The first proposal addressing HIP-based NEMO was described in (Ylitalo J., Rethinking Security in Network Mobility, 2005). The authors discuss the basics of a possible NEMO solution that handles HIP aware mobile networks. While this paper is the first work touching mobility of HIP networks as a whole, it does not get into describing the details of the solution. Later the authors have further developed their ideas, which also will be discussed in this chapter.

A hybrid HIP-MIPv6 based network mobility management scheme has been proposed by Herborn, Haslett, Boreli, and Seneviratne (2006). It enables HIP based MNNs to communicate with MIPv6 based MRs. NEMO signaling is performed by the MR and is based on MIPv6 bindings. Inside the moving network HIP bindings are used between the MR and the MNNs.

The solution called HIP-NEMO (Nováczki, Bokor, & Imre, A HIP based Network Mobility Protocol, 2007; Nováczki, Bokor, Jeney, & Imre, 2008) extends μHIP to be able to handle moving networks. This scheme can be considered as the first complete and pure HIP-based NEMO solution. In HIP-NEMO we introduced a new HIP capable network entity is introduced called the mobile Rendezvous Server (mRVS). The mRVS provides continuous connectivity for the served MNNs and also for other moving networks connected to it. Moreover the mRVS is in charge to be the signaling proxy for MNNs. The MNNs delegate their signaling rights to the mRVS thus it can control any mobility scenarios almost seamlessly to MNNs. Figure 6 shows the initial steps of a HIP-NEMO based moving network. First of all the mRVS discovers all LFNs, which are registering themselves at the mRVS and delegating their signaling rights to it. The mRVS maintains a mapping between the HIT of the LFNs and their IP address valid inside the moving network. This mapping entry is than associated with an IP address assigned by the mRVS. The purpose of this address is exactly the same as in case of μHIP. It is valid outside the moving network and is exchanged with the LFNs actual IP address by the mRVS. After the initial registration the mRVS does the necessary signaling for the LFNs. It informs the RVS and the DNS as shown in Figure 6 as step 2 and 3. The RVS creates a special mapping that contains the HIT and global IP address of the LFN and is associated with the HIT of the mRVS. This latter association is useful when the moving network changes its network point of attachment. The mRVS has to perform only one update sequence indicating its new IP address and HIT. The RVS automatically refreshes all other entries that are associated with the HIT of the mRVS. Finally the DNS is informed about the serving RVS.

As these initial steps are completed it is possible to trigger a communication session with one of the LFNs in the mobile network. Figure 7 can be used to track the process. The peer node queries the DNS for the IP address of the LFN by giving its HIT in the query, and gets the IP address of the RVS serving the LFN. The first packet of the Base Exchange is sent to the RVS, which forwards the packet towards the mRVS according to its mapping. The destination IP address is the one assigned by the mRVS to the LFN at the registration phase. The I1 packet is intercepted by the mRVS and the destination address is changed to the one of the LFN valid inside the moving network. Finally the LFN receives the message and answers with the second Base Exchange message (R1). The source address is changed at the mRVS to the globally reachable one and sent directly to the peer. The connection setup finishes in the regular

Figure 6. HIP-NEMO network initialization

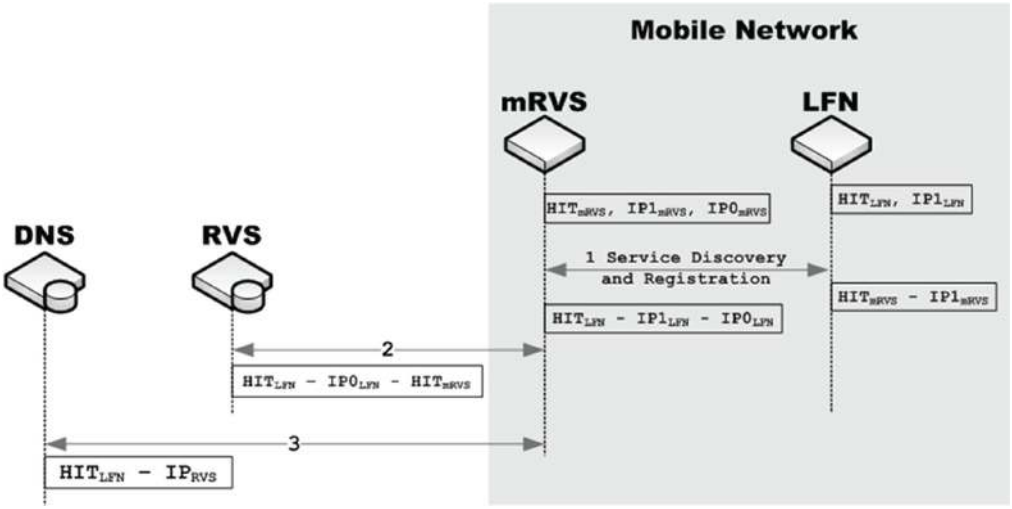
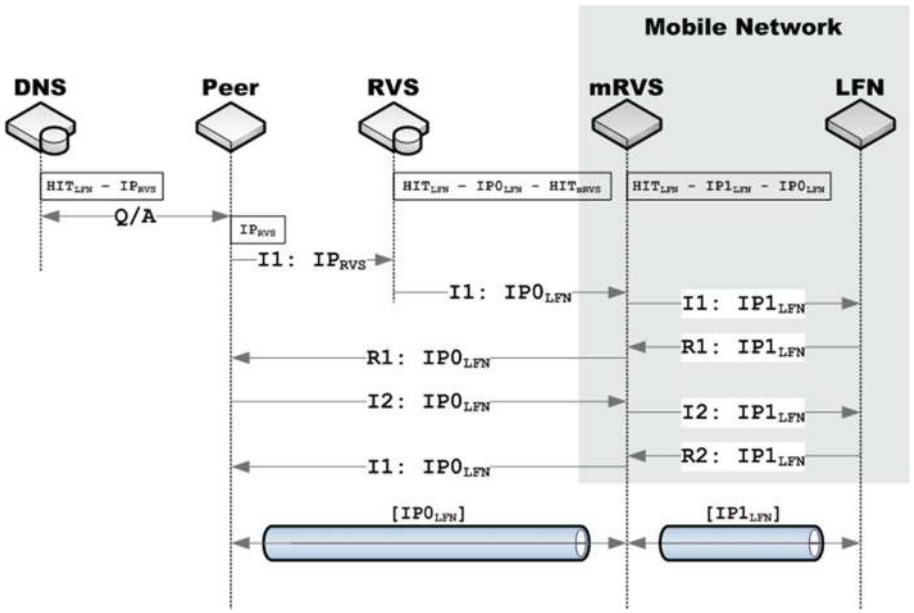


Figure 7. HIP-NEMO connection establishment



way. Note that all the packets (signaling or data) send by or addressed to the LFN are intercepted by the mRVS. This entity changes the source or the destination addresses depending on the direction of the communication.

The key issue in field of mobile networks is how nested mobile subnetworks are handled. Nested NEMOs are challenging problems as they usually raise serious scalability problems. In HIP-NEMO nested subnetworks are

managed by special inter mRVS signaling. A bi-directional IP tunnel is built up between mRVSs. All signaling and data addressed to nested networks is injected through this tunnel. Moreover, signaling between mRVSs manages the introduction of new nested subnets as well as nested subnet handover situations. The detailed description is out of scope of this summary.

An alternative solution that uses HIP to handle moving networks is described in Ylitalo, Melé, Patrik, and Petander (2008) and Melen, Ylitalo, Salmela, and Henderson (2009). The proposal is based on signaling delegation between MNNs and the HIP enabled mobile router. After the initial registration all the signaling needs of MNNs are performed by the mobile router. The main difference compared to the above solution is that there is no need to change the source and destination addresses of packets passing the boundary of the moving network. Instead a special NAT functionality is implemented in the MR. The MR intercepts packets passing through it and checks the ESP header. This contains a special parameter; the Security Parameter Index (SPI) that can be used to identify nodes behind the MR. This maintains an association between the SPI values and the IP address of the MNNs. Based on this information the packets can be routed to the proper endpoint. The proposal can also handle nested mobile networks in a scalable manner.

Flow Management, Dual-Stack Mobility and Location Privacy

With the advance of heterogeneous access structures – and considering that users are running multiple applications simultaneously – the traditional per-host or network mobility management technique cannot be the optimal solution for handling connection changes. Instead, the concept of per-flow or per-application mobility management is to be introduced, where a dedicated interface (i.e., access network) is selected for each application according to its QoS requirements and the actual networking conditions.

Aiming to benefit from this novel concept in practice, authors of Pierrel, Jokela, and Melen (2006) and Pierrel, Jokela, Melen, and Slavov (2007) proposed firstly a method where two HIP nodes, of which at least one is multihomed, can separate different upper layer data flows (e.g., TCP and UDP) between peers and allow flows to use different interfaces at the multihomed node. This HIP extension basically describes mechanisms for flow identification and carrying filter rules (i.e., policy transfer) in HIP signaling.

In Bokor, Zeke, Nováczki, and Jeney (2009) authors go even further by defining and evaluating a complete HIP-based per-application mobility management platform. This platform consists of a Monitoring/Mediator Agent (collecting protocol specific information from different layers for cross-layer per-application mobility decisions), an Application Profile DataBase (storing and maintaining profile attributes of ongoing application sessions for decision support), a Decision Engine (processing inputs from the above entities and making mobility decisions), and a HIP Agent. The HIP Agent is responsible to initialize mobility procedures in the HIP layer based on the control information sent by the Decision Engine, and also to maintain per-application bindings between the host machine and its partners. From the HIP point of view, multihomed Security Associations are the protocol elements which can make a HIP system to be able to handle mobility in an application-wise manner. In consequence, the HIP Agent implements a certain SA grouping scheme and a modified UPDATE mechanism which are the keys to the HIP-based per-application mobility management. The approach is end-to-end based and uses spanned SAs between communicating peers as basis for operation, therefore standards of HIP DNS and RVS extensions are left intact, and only SA handling, packet processing and UPDATE procedure are slightly modified in the scheme.

In Fekete (2009) the author introduces a policy based flow management system for multihomed HIP hosts focusing on the defini-

tion of a simple language to specify policies that influence the source and destination IP addresses of outgoing packets. The solution makes possible to express policies for selecting IP addresses based on different QoS parameters (e.g., bandwidth, RTT) or other kind of access characteristics like the cost of usage, and requires only minimal changes to the Host Identity Protocol.

Standard operations of Host Identity Protocol consider IPv4 and IPv6 interworking but lack support of cross-family handovers. The problem within the base specification is that when locators are included in the R1 and I2 packets of the Base Exchange with the preferred bit (i.e., this indicates address the corresponding peer prefers to use) set. This forces the peer to immediately switch to the preferred locator and makes it impossible to handle alternative locators. One modification (Varjonen, Komu, & Gurtov, Secure and Efficient IPv4/IPv6 Handovers Using Host-Based Identifier-Locator Split, 2009; Varjonen, Komu, & Gurtov, Secure and Efficient IPv4/v6 Handovers Using Host-Based Identifier-Location Split, 2010) proposed for HIP suggests that the locators should be sent in the Base Exchange with preferred bits unset. Locators communicated this way should be considered as alternative locators, which do not have to be used immediately. This makes cross-family handovers possible because peers can inform each other about all available addresses they are reachable at. Cross-family handovers are having high importance as they can aid transition from IPv4 towards IPv6. This makes coexistence and transition less painful.

With traditional mobility management protocols mobile nodes are informing their peers if they are available at a new location. However this communication is rarely protected in a sufficient way and does not provide location privacy for the users. If a third entity captures location update messages, it can locate the sender and trace its movements which most users want to avoid. A recent extension (Maekawa & Okabe, 2009) to HIP enables to empower the base protocol with location privacy features. The proposal combines two solutions to enable complete location privacy for mobile HIP users. An earlier solution (Matos, Santos, Girao, Liebsch, & Aguiar, 2006; Matos, et al., 2006) defined a limited location privacy framework for HIP while BLIND (Ylitalo & Nikander, BLIND: A Complete Identity Protection Framework for End-Points, 2006) provided a much enhanced solution but without mobility support. This novel scheme integrates the strong points of the above two methods and introduces complete location privacy with mobility. The key idea is to use Temporary Host Identifiers (THI) for location update purposes. THIs are constructed so that capturing them provides no information about the location of the user.

HIP in 3G and Beyond Mobile Architectures

The use of Host Identity Protocol in telecommunication architectures such as 3G UMTS, LTE/EPS, etc., can provide number of benefits and possible achievements but also can cause a number of issues for the network operator. Here we summarize aspects of HIP in 3G and beyond systems by means of mobility management and scalability, focusing on HIP-SIP integration, network interface selection and support of distributed and flat mobile architectures. A wider survey on issues arising when a network operator wants to deploy HIP for its own customers is presented by authors of Dietz, Brunner, Papadoglou, Raptis, and Kypris (2005).

Today and future telecommunication networks likely rely on the wide-scale capabilities of IP Multimedia Subsystem (IMS) and Sessions Initiation Protocol (SIP) protocol. Rothenberg, Wong, Verdi, and Magalhae (2008) state that IMS and SIP can be seamlessly supported and can clearly benefit from any identifier/locator split architecture in terms of security, mobility and multihoming based on transparently using permanent cryptographic node identifiers decoupled from the actual network locators. Recent standardization activities of the ITU Telecommunication Standardization Sector (ITU-T) also encourage operators for integration of the ID/Loc separation concept

into future network architectures (Y.ipsplit, 2009; Y.ipv6split, 2009). Based on the above and according to (Henderson, 2004) it can be concluded that the main benefit a HIP-enabled IMS/SIP networking infrastructure would offer is advanced and more efficient mobility management (such as micromobility or network mobility management), possible integration of rendezvous servers with SIP proxy and redirection servers, and NAT traversal.

Author of (Heikkinen, 2008) tries to provide a HIP-SIP integrated IMS architecture in order to allow enhanced interaction that takes into account the liability and reliable identification needs of the different entities partaking in communication, i.e. the user, the access operator, and also the home network. This scheme allows non-repudiative accounting records to be made meaning that if the user has used the service, this cannot be denied afterwards. Similarly, if the user does not seem to be honest in its service usage in terms of compensation, the service will no longer be provided.

Camarillo, Mas, and Nikander (2008) present a complete HIP-SIP interworking framework where SIP-based services between HIP-enabled hosts take advantage of the mobility, security, and multihoming capabilities of HIP. Additionally, some SIP-based services can also benefit from the IPSec-based data encryption provided by HIP.

A HIP based mobility management extension of 3G UMTS architecture is presented in So and Wang (2006), where the focus is on heterogeneous UMTS/WLAN access environments. Implementation work is also in progress regarding HIP-SIP integration: (Wagner, 2006) presents the first measurement results of a real-life HIP-SIP interworking system.

The I-HSIP scheme (Li, Chen, Su, Jin, & Zeng, 2009) also presents an integrated HIP-SIP based mobility management architecture for next generation mobile wireless networks in order to support secure and efficient mobility services for both real-time (running over RTP/UDP and SIP) and non-realtime (applying TCP and HIP) applications. This architecture merges the similar operations and entities of HIP and SIP (such as SIP server and HIP RVS), aiming to minimize the system signaling cost and to improve handover performance.

SHIP (Yang, Zhou, Qin, & Zhang, 2009) is a cross-layer mobility management scheme based on SIP and HIP. SHIP focuses on handover optimization: by the way of integration a one-suite protocol stack comes into existence that provides seamless mobility and fast handoff. The basic idea behind SHIP is that the MN and the CN use their HITs to establish the SIP sessions, and the MN uses the HIP update procedures instead of the SIP location update scheme in case of handovers.

HIP-SIP interworking in future communication architectures also tries to apply HIP for the design of a peer-to-peer version of SIP (P2PSIP) (Bryan, Matthews, Shim, Willis, & Dawkins, 2008). Several proposals suggest either to use HIP directly e.g., (Hautakorpi, Camarillo, & Koskela, 2007), or just borrow ideas from HIP like (Cooper, Johnston, & Matthews, 2007).

A very active and rapidly developing research area of HIP focuses on the scalability problems of mobile Internet architectures. Existing wireless telecommunication infrastructures are not prepared to handle the forecasted traffic increase (Cisco, 2013), current systems and also mobile architectures under standardization (e.g., 3GPP, 3GPP2, WiMAX Forum) follow centralized approaches that cannot scale well to the growing traffic demands (Bokor, Faigl, & Imre, Flat Architectures: Towards Scalable Future Internet Mobility, 2011). Distributed and flat networks are on their way to be implemented not only requiring novel architectural design paradigms, special network nodes and proprietary elements with peculiar functions, but also demanding certain, distinctive mobility management schemes sufficiently adapted to the distributed architecture. In fact, distributed and dynamic mobility management mechanisms (DMM) and the relating decision methods, tunneling schemes, information, command and event services form the key routines of the future mobile Internet designs.

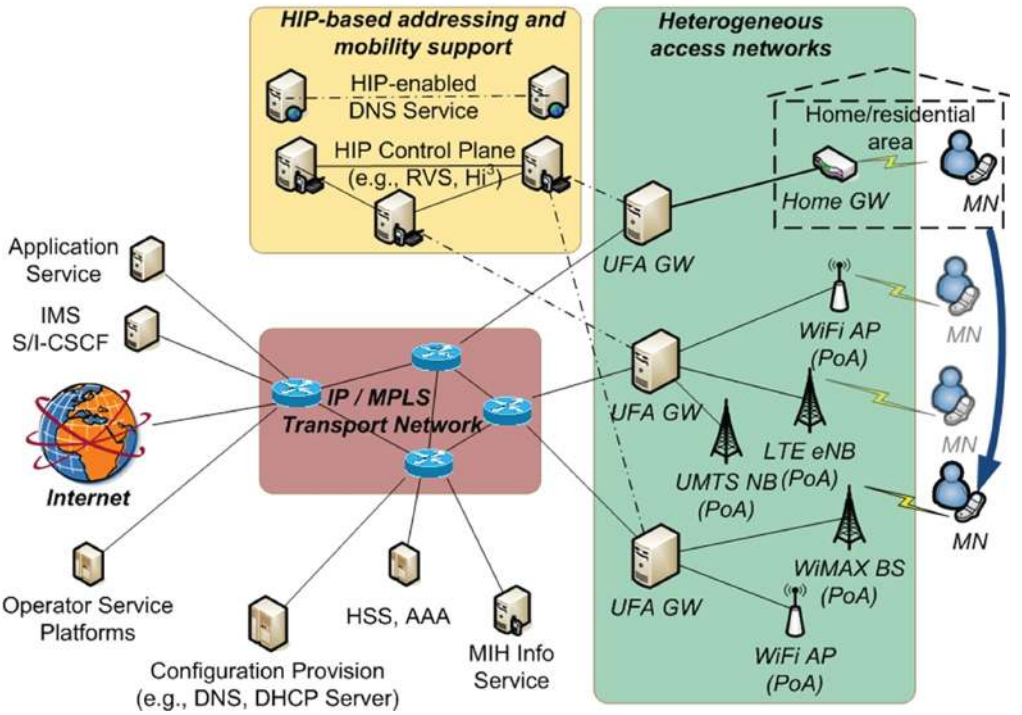
Regarding the concept of distributed/flat mobile internet architectures, one important challenge is the provision of service continuity during inter-GW handovers (e.g., the GW means the first IP-hop in case of 3GPP, non-3GPP accesses to the EPC). Seamless inter-GW handover should be provided for real-time applications, but according to the current standards, attachment to new GWs, e.g. in case of changing ePDG, the complete attachment procedure is performed. Due to the distribution of GWs, inter-GW handovers will happen more and more frequently, thus reduction of security overhead due inter-GW handovers is an important challenge within the focus of this technology.

The first HIP-based mobility scheme for distributed and flat architectures was presented in (Faigl, et al., Evaluation and Comparison of signalling protocol Alternatives for the Ultra Flat Architecture, 2010; Bokor, Faigl, & Imre, A Delegation-based HIP Signaling Scheme for the Ultra Flat Architecture, 2010; Faigl, Bokor, Neves, Daoud, & Herbelin, Evaluation of two integrated signalling schemes for the ultra flat architecture using SIP, IEEE 802.21, and HIP/PMIP protocols, 2011). The solution is called HIP-based Ultra Flat Architecture (UFA-HIP) and depicted in Figure 8. The proposed system comprises four main parts:

1. Several access networks;
2. An ip/mpls transit network;
3. A handover preparation and initiation subsystem (e.g., based on ieee 802.21 media independent handover standard); and
4. A HIP-based control network.

In this scheme centralized IP anchors between Point of Access (PoA) nodes and correspondent nodes are totally removed, and network functions are placed at the edge of the transit and access networks (close to the Point of Access (PoA) nodes) in the Ultra Flat

Figure 8. UFA-HIP: A HIP-based ultra flat architecture



Architecture Gateways (UFA GWs). The main tasks of the HIP-capable UFA GWs:

1. Performing fast cross layer (L2 and HIP-level) access authorization;
2. Actively interacting with hosts through delegation-based HIP and IPsec association management and context transfer for optimized message exchange in HIP-based UFA mobility and multihoming operations. (Note that this framework transports end-to-end flows between MNs and CNs in a hop-by-hop manner. The middle-hops are the UFA GWs, i.e., the delegates of the end peers);
3. Performing the actual mapping/routing between outer header IPsec tunnels based on inner header identifiers.

The control network in the upper part of Figure 8 (HIP-based addressing and mobility support) contains a HIP-compatible Domain Name System ýfor resolving domain names to host identities and/or locators depending on the actual situation. In addition there is the HIP Control Plane which stores and distributes dynamic and presumably frequently changing binding information between host identities and locators of all actively communicating (mobile) hosts in UFA-HIP. This control plane might be a conventional RVS park or a complete distributed HIP signaling architecture like Hi3 (Gurtov, Korzun, Lukyanenko, & Nikander, 2008)ý. The records managed here are provided by the UFA GWs using their own global locators as location information to be bounded with identities of their actively interacting partners.

The control of the functions shown in Figure 8 brings cross-layer HIP modules in the UFA GWs, MNs and Correspondent Nodes (CNs). HIP Base Exchange (BEX) and Update procedures deal with dynamic negotiation of IPsec security associations between the MN and the UFA GW to protect user data and mutually authenticate the MN and the network. The handover execution procedure is started by the source UFA GW. HIP and IPsec contexts are established between the target UFA GW and the MN's CNs, furthermore, between the target UFA GW and the MN, using the mediation of the source UFA GW. This is possible due to the delegation of HIP signaling rights from the MN and from the target UFA GW to the source UFA GW. Context Transfer Protocol (RFC4067) is used to transfer the HIP and IPsec contexts from the source UFA GW to the target UFA GW and the MN. As the contexts are in their place the MN is notified by the handover preparation and initiation subsystem to attach to the new PoA. The handover preparation and initiation subsystem handles handover preparation issues and relating signaling tasks in order to initiate proactive HIP handover procedures in the UFA and to support both network and mobile controlled handover decisions.

EVALUATION

The aim of the performance evaluation in this work is to compare the handover performance of our μHIP, HIP-NEMO and UFA-HIP proposals with the standard Host Identity Protocol capabilities. Comparisons were performed by modelling the above four protocols by focusing on the handover support of both schemes. In order to provide a highly configurable, extensible, and adequate model for UFA-HIP, we extended our previous IPv6-based Host Identity Protocol simulation framework called HIPSim++ (Bokor, Nováczki, Zeke, & Jeney, 2009). The model is built on the top of the 1.99.3 version of INET which is an extension and TCP/IP model collection of the component based, modular OMNeT++ 4.2 discrete event simulation environment (Varga & Hornig, 2008). The different scenarios and sub-scenarios were defined by using the OMNeT++ NED language (for topology description) and the *omnetpp.ini* configuration file (for parameter setup and definition of different simulation runs).

Simulation Environment

Our comparisons were performed by setting up the four main scenarios (*I*, *II*, *III*, *IV* – HIP, μHIP, HIP-NEMO and UFA-HIP, left to right

on Figure 9 and 10, respectively) in similar a topology.

In the standard HIP scenario (*I*) the mobile HIP host (User Equipment) changes its network point of attachment by connecting to another Wi-Fi access point due to its movement signed by the arrow. As AP 1 and AP 2 are in different IP networks advertising different IPv6 prefixes, the IPv6 address of the UE will be changed after reattachment. Standard HIP mechanisms handle the situation by running the UPDATE process. During the simulation built-in TCP and UDP application models were used to generate traffic between the UE and its correspondent node. Access Points were connected to the Router 3 simulating an Internet-wide communication

Figure 9. Simulation scenarios for standard HIP (left) and µHIP (right) schemes

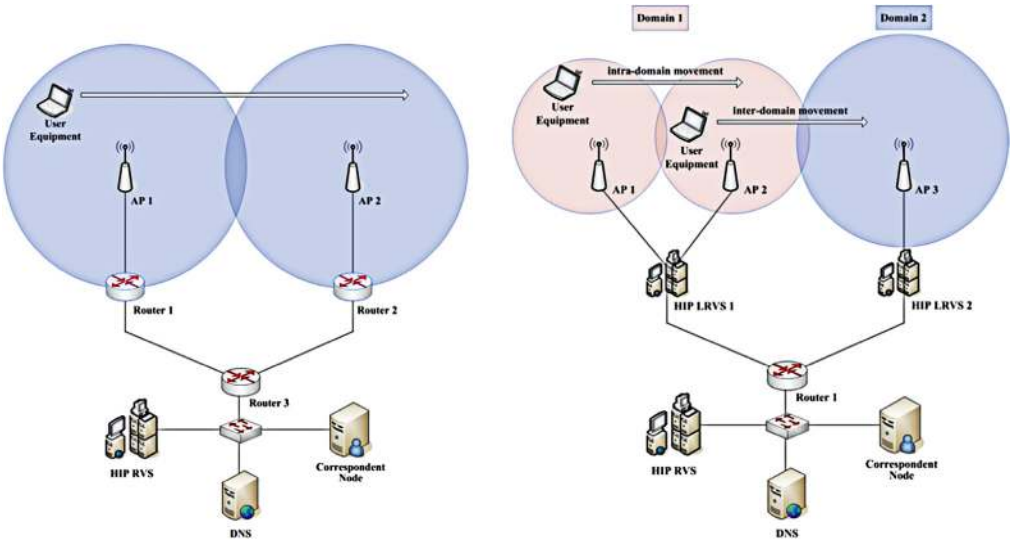
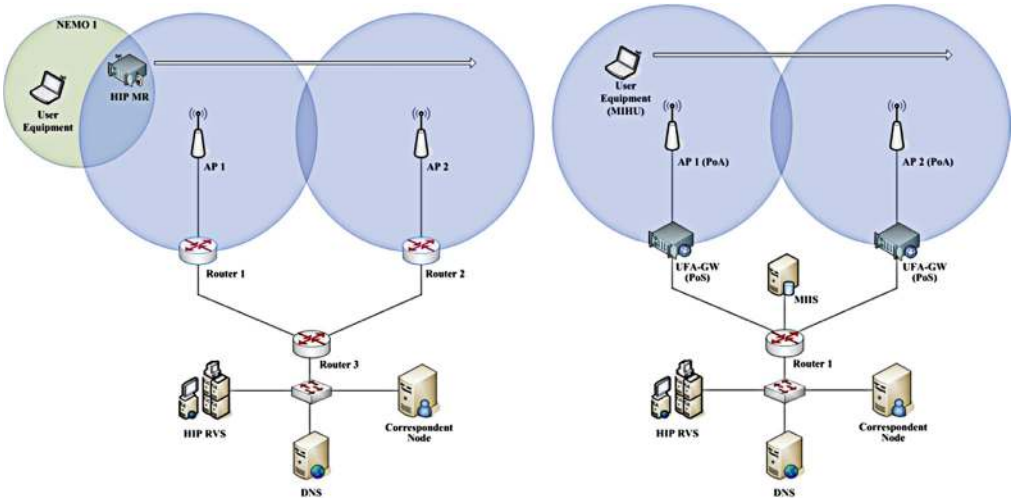


Figure 10. Simulation scenarios for HIP-NEMO (left) and UFA-HIP (right) schemes



with an average RTT of 300ms between the UE and the Correspondent Node / HIP Rendezvous Server. A simple Domain Name Service model is used to simulate DNS procedures, but they are initiated only before connection establishment (i.e., HIP Base Exchange).

For the μHIP scenario (*II*) the difference lies in the introduction of micro-mobility domains: HIP LRVS 1 and 2 replace the access routers and control their Domain 1 and 2, where the first one owns two access points (AP1, AP2) providing possibilities to simulate intra-domain handovers inside LRVS1. Inter-domain handovers are also implemented by changing the UE's network point of attachment from AP2 to AP3.

In case of HIP-NEMO (*III*) we introduced a HIP Mobile Router (HIP MR), which handles the mobility of NEMO 1 consisting the User Equipment as a mobile network node inside the moving network besides the MR.

In the UFA-HIP case (*IV*) the topology is basically the same as Figure 9, but the protocols (and therefore some networking elements) are different. In this scenario Router 1 and Router 2 are not simple access routers anymore but UFA GWs with all the UFA-HIP gateway mechanisms and protocol extensions described above. The UFA-HIP scenario also contains an INET Notification Board (INET/OMNeT++, 2013) based model of 802.21 Media Independent Handover Framework providing a simple but adequate implementation of access network independent functions aiming to monitor currently available L2/L1 resources, prepare L2 resources, and commit L2 handovers. The UFA-HIP's proactive context transfer (designed t be working in a GW-GW and GW-CN manner) is also implemented in this advanced scenario.

Results

In all the scenarios shown in Figure 10, the UE is able to migrate between the different APs with a constant speed such provoking handovers situations. By inducing 100 independent handovers during simulation runs we measured three main parameters such creating three sub-scenarios.

Sub-scenario *A* measures Handover Latency defined here as the time elapsed between loosing the connection at the old AP and the UE/MR/UFA GW sending out the last mobility management related signalling packet (e.g., HIP UPDATE packet) while connected to the new AP. The measurements are analyzed in function of different average Router Advertisement (RA) intervals such creating the simulation runs (each executed 100 times) defined by the different RA values.

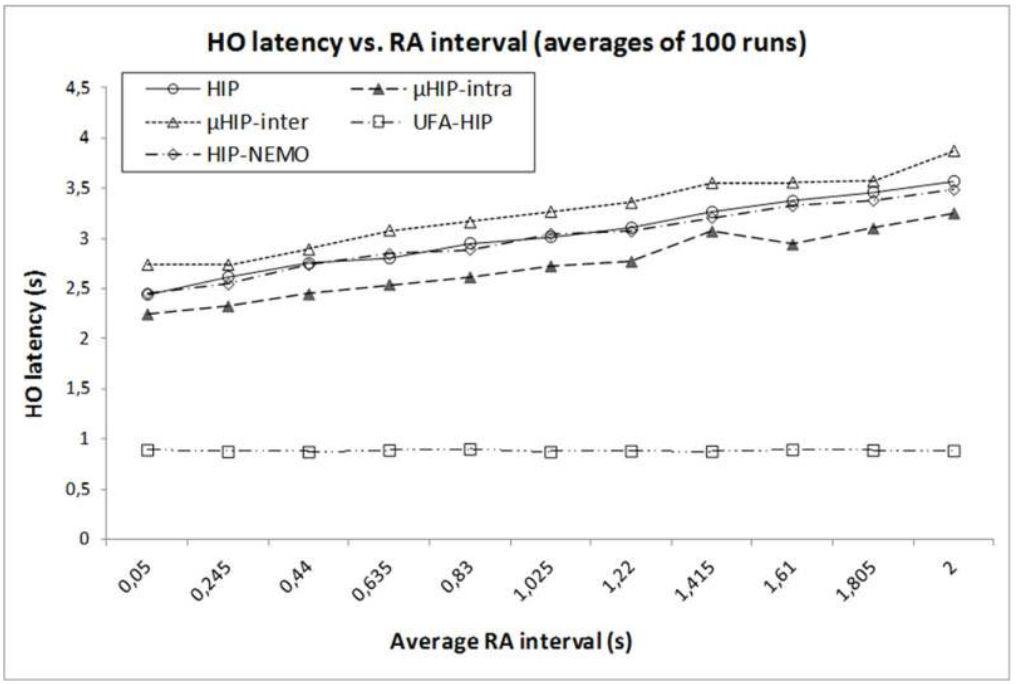
Sub-scenario *B* measures UDP packet loss during handover situations in function of different data rates of the UDP application originated by the UE towards the CN. The simulation runs defined for all sub-scenarios (i.e., *I/B*, *II/B*, *III/B*, and *IV/B*) were created by setting the inter-packet departure time of the UDP application.

In sub-scenario *C* we measured TCP throughput of one minute experienced at different handover frequencies. Here the simulation runs were defining the number of handovers suffered by the UE/NEMO per minute form 0 to 9. In order to achieve this, we created ten different movement paths for the UE/NEMO in ten different motion configuration files.

The simulation results gathered in the introduced sets of scenarios are presented in three different graphs.

Figure 11 presents the handover latency as the average of the 100 handover series for every RA interval. Measurements show that UFA-HIP handover performance is independent of the subsidiary IP layer mechanisms (i.e., delays of acquiring IP address, duplicate address detection, etc.) and keeps service interruption delay below 1 sec. It means that the handover latency is caused only by the physical reattachment procedures in UFA-HIP (Wi-Fi AP re-association in our simulations). Measurements show that the service interruption delay of UFA-HIP is independent from the configuration delay in the target network (i.e., RA interval), and about 70% smaller than the standard HIP case in average, thanks to the advanced proactive operation

Figure 11. Handover latency in function of different RA intervals



which basically reduces the handover disruption to the Layer 2 (re-)attachment delay. It is also showed that the latency of µHIP intra-domain handovers is around 10% better compared to the basic HIP performance, but the inter-domain cases produce approx. 6% higher values due to the additional management tasks when entering a new micro-mobility domain. Performance of HIP-NEMO matches standard HIP handover performance: MNN's delegation of signalling rights to its HIP MR makes service interruption delay of network mobility handover management similar to the basic HIP protocol.

Figure 12 introduces results of sub-scenario *B* for every evaluated protocol, and shows how much UDP packet was lost during a handover in a HIP, µHIP, HIP-NEMO and UFA-HIP based system. Points on the graph represent the average UDP packet loss of 100 handovers for every offered datarate value. The differences and similarities of the examined protocols' handover performance are clearly observable in the UDP transport layer. Our simulations show how µHIP enhances the handovers in intra-domain scenarios by the cost of slightly worse results for inter-domain HO events. HIP-NEMO again demonstrates similar behaviour to the base HIP protocol, but again: it HIP-NEMO is able to handle mobility not only for a single UE but for all the nodes of a complete moving network within the cost of a HIP update procedure. The power of the proactive, context-transfer based distributed solution designed for ultra flat architectures is highlighted by the fact that the number of lost UDP packets is 54% less in average for the UFA-HIP case compared to the legacy Host Identity Protocol performance.

Figure 13 depicts the TCP throughput proportion of the four protocols under analysis in a one minute communication session between the UE and the CN experienced at different handover frequencies from 0 to 9. The gain of µHIP in intra-domain use-cases is clear but for UFA-HIP it is even more eye-catching especially when the circumstances are deteriorating (i.e., the number of handovers is increasing): in case

Figure 12. UDP packet loss in function of offered data-rate

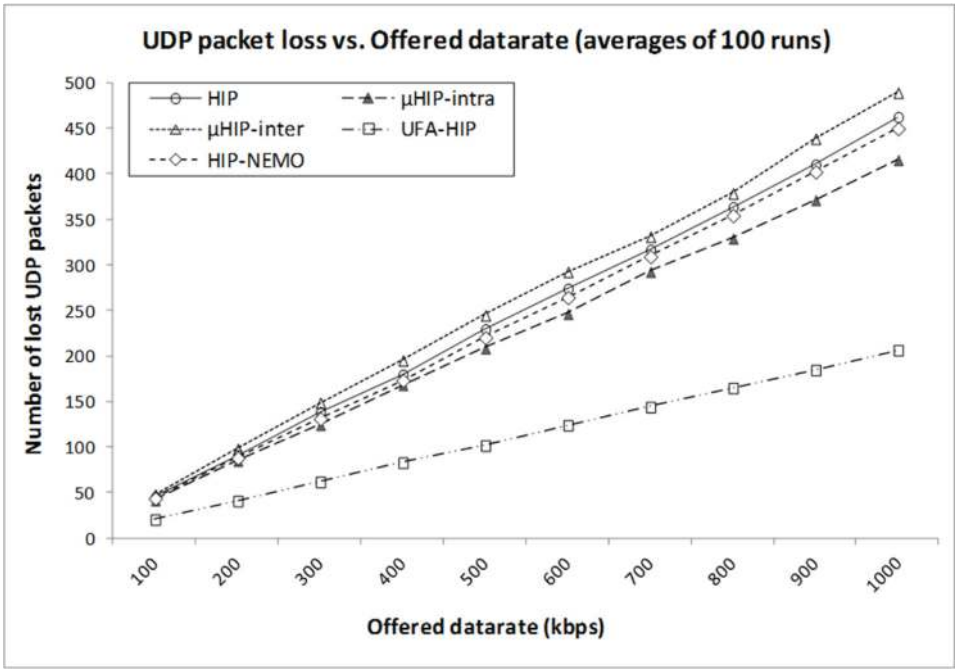
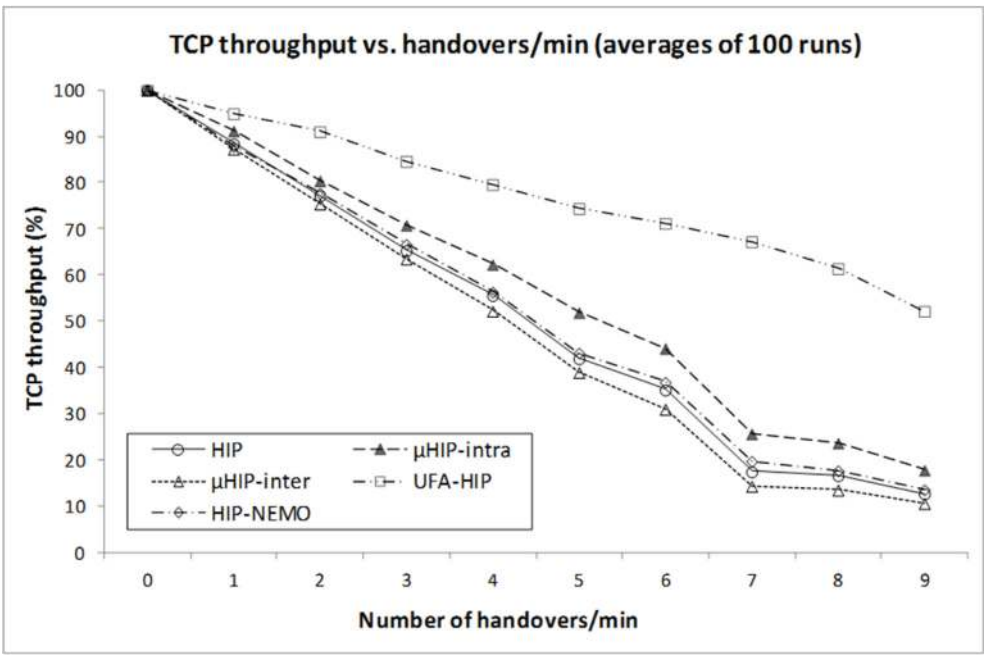


Figure 13. TCP throughput in function of number of handovers per minute



of the highest handover frequency UFA-HIP shows more than 300% gain in TCP throughput, but also the average gain of the advanced distributed scheme is above 52% compared to HIP.

Simulation results show that the handover latency and the number of lost packets during handoffs can be significantly reduced while the TCP throughput can be considerably increased in case of the UFA-HIP proposal, meaning that relevant improvements in handover performance can be achieved besides the enhanced scalability when applying intelligent distributed HIP gateways in the mobile network. Also μHIP provides observable gains, but without proactivity and cross-layer information provision it cannot approach UFA-HIP in handover performance. HIP-NEMO provides a valuable functional extension without additional costs in handover latency and higher layer performances. However, introduction of HIP technologies in current or evolving mobile architectures is not an easy job: the structural modifications inside the common TCP/IP protocol stack raises serious deployment concerns which should be tackled for widespread application of HIP based networking solutions.

CONCLUSION

In this paper we presented the basics of HIP focusing on how it can be utilized to support advanced mobility scenarios and manage complex mobility management problems. The main part of the article was devoted to introduce HIP's built-in mobility management capabilities followed by its numerous extensions designed to implement mechanisms like micromobility, network mobility, per-application mobility, simultaneous end-host mobility, dual-stack handover support, location privacy, and application of HIP in 3G and beyond architectures. We have modeled and evaluated four of the schemes – all developed by us in our previous works but never analyzed in such complex models and well-elaborated scenarios. Our goal was to show that HIP is one of the most promising instances of the ID/Loc separation concept, on which several advanced mobility services and applications can be built, while also keeping the generic security and unique architectural properties of the base protocol. We also tried to prove that HIP and the related research work are quite far from being ready or closed. A lot of effort was put into this research area, but a lot more design and implementation experience will be needed to ensure the widespread usage of HIP and the integration of the mobility management schemes based on it. As a part of our future work we will compare the signaling overhead of our schemes introducing another viewpoint into the analysis: at what cost in means of additional signaling in the wired and wireless networking segments can we implement advanced mobility management protocols in the Host Identity Layer.

ACKNOWLEDGMENT

The publication was supported by the TÁMOP-4.2.2.C-11/1/KONV-2012-0001 project. The project has been supported by the European Union, co-financed by the European Social Fund. The publication also received funding from the "Virtualization-based Mobile Network Optimization" project of the Hungarian National Development Agency (EUREKA HU 12-1-2012-0054), carried out in the framework of CELTIC-Plus project CP2012/2-5 SIGMONA. The authors also would like to express their appreciation to László Csordás and János Gulyás for their valuable contribution to this research.

REFERENCES

Aydin, Z. G., Chaouchi, H., & Zaim, A. H. (2009). eHIP: Early update for host identity protocol. In *Proceedings of the 6th International Conference on Mobile Technology, Application & Systems,* Nice, France.

Bokor, L., Faigl, Z., & Imre, S. (2010). A delegation-based HIP signaling scheme for the ultra flat architecture. In *Proceedings of the 2nd IWSCN*, Karlstad, Sweden (pp. 9–16).

Bokor, L., Faigl, Z., & Imre, S. (2011). Flat architectures: Towards scalable future internet mobility. *Lecture Notes in Computer Science*, *6656*, 35–50. doi:10.1007/978-3-642-20898-0_3

Bokor, L., Nováczki, S., & Imre, S. (2007). A complete HIP based framework for secure micromobility. In *Proceedings of the 5th @WAS International Conference on Advances in Mobile Computing and Multimedia (MoMM2007)*, Jakarta, Indonesia (pp. 111-122).

Bokor, L., Nováczki, S., Zeke, L. T., & Jeney, G. (2009). Design and evaluation of host identity protocol (HIP) simulation framework for INET/OMNeT++. In *Proceedings of the 12-th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM 2009)*, Tenerife, Canary Islands, Spain (pp. 124-133).

Bokor, L., Zeke, L. T., Nováczki, S., & Jeney, G. (2009). Protocol design and analysis of a HIP-based per-application mobility management platform. In *Proceedings of the 7-th ACM International Symposium on Mobility Management and Wireless Access (MobiWAC 2009)*, Tenerife, Canary Islands, Spain (pp. 7-16).

Bryan, D., Matthews, P., Shim, E., Willis, D., & Dawkins, S. (2008, July 7). Concepts and terminology for peer to peer SIP. *IETF Internet Draft*. draft-ietf-p2psip-concepts-02.

Camarillo, G., Mas, I., & Nikander, P. (2008). A framework to combine the session initiation protocol and the host identity protocol. In *Proceedings of the Wireless Communications and Networking Conference (WCNC 2008. IEEE),* Las Vegas, NV.

Cisco. (2013, February). *Cisco visual networking index: Global mobile data traffic forecast update 2012-2017*. Retrieved September 20, 2013, from http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.pdf

Cooper, E., Johnston, A., & Matthews, P. (2007, December). A distributed transport function in P2P-SIP using HIP for multi-hop overlay routing. *IETF Internet Draft*. draft-matthews-p2psip-hip-hop-00.

Dietz, T., Brunner, M., Papadoglou, N., Raptis, V., & Kypris, K. (2005). *Issues of HIP in an operators networks*. draft-dietz-hip-operator-issues-00.

Faigl, Z., Bokor, L., Neves, P., Daoud, K., & Herbelin, P. (2011). Evaluation of two integrated signalling schemes for the ultra flat architecture using SIP, IEEE 802.21, and HIP/PMIP protocols. *Computer Networks*, 1560–1575. doi:10.1016/j.comnet.2011.02.005

Faigl, Z., Bokor, L., Neves, P., Pereira, P., Daoud, K., & Herbelin, P. (2010). Evaluation and comparison of signalling protocol alternatives for the ultra flat architecture. In *Proceedings of the 5th International Conference on Systems and Networks Communications (ICSNC)*, Nice, France (pp. 1-9).

Fekete, G. (2009). Policy based flow management with the host identity protocol for multihomed hosts. In *Proceedings of the First International Conference on Emerging Network Intelligence,* Sliema, Malta.

Gurtov, A., Korzun, D., Lukyanenko, A., & Nikander, P. (2008). Hi3: An efficient and secure networking architecture for mobile hosts. *Computer Communications*, *38*, 2457–2467. doi:10.1016/j.comcom.2008.03.014

Hautakorpi, J., Camarillo, G., & Koskela, J. (2007, November). Utilizing HIP (Host Identity Protocol) for P2PSIP (Peerto- peer Session Initiation Protocol). *IETF Internet Draft*. draft-hautakorpi-p2psip-with-hip-01.

Heikkinen, S. (2008). Security and accounting enhancements for roaming in IMS. In *Proceedings of the 6th International Conference on Wired/Wireless Internet Communications (WWIC 2008). Lecture Notes in Computer Science 5031* (pp. 127-138). Tampere, Finland: Springer.

Henderson, T. (2004). *Can SIP use HIP.* Retrieved April 15, 2010, from HIP Workshop, 61st IETF meeting: http://hiprg.piuha.net/workshop/

Herborn, S., Haslett, L., Boreli, R., & Seneviratne, A. (2006). HarMoNy - HIP mobile networks. In *Proceedings of the 63rd IEEE Vehicular Technology Conference, VTC.*

Herborn, S., Huber, A., Boreli, R., & Seneviratne, A. (2007). A scheme for host identity delegation. In *proceedings of the IEEE/Create-Net/ICST International Conference on COMmunication System softWAre and MiddlewaRE (COMSWARE),* Bangalore, India.

Hobaya, F., Gay, V., & Robert, E. (2009). Host identity protocol extension supporting simultaneous end-host mobility. In *Proceedings of the Fifth International Conference on Wireless and Mobile Communications (ICWMC '09)*, Cannes/La Bocca, France (pp. 261-266).

Iapichino, G., & Bonnet, C. (2009). Host identity protocol and proxy mobile IPv6: A secure global and localized mobility management scheme for multihomed mobile nodes. In *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM'09),* Honolulu, Hawaii (pp. 1-6).

Iapichino, G., Bonnet, C., Herrero, O. d., Baudoin, C., & Buret, I. (2009). Combining mobility and heterogeneous networking for emergency management: A PMIPv6 and HIP-based approach. In *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, Leipzig, Germany (pp. 603-607).

INET/OMNeT++. (2013). *The INET Framework for OMNeT++*. Retrieved September 20, 2013, from http://inet.omnetpp.org/

Jokela, P., Melen, J., & Ylitalo, J. (2006, June). HIP service discovery. *IETF Internet Draft*. draft-jokela-hip-service-discovery-00

Jokela, P., Moskowitz, R., & Nikander, P. (2008, April). Using the encapsulating security payload (ESP) transport format with the host identity protocol (HIP). *RFC 5202*.

Kovácsházi, Z., & Vida, R. (2007). Host identity specific multicast. *International Conference on Networking and Services (ICNS '07),* Athen, Greece.

Laganier, J., & Eggert, L. (2008). Host identity protocol (HIP) rendezvous extension. *RFC 5204*.

Laganier, J., Koponen, T., & Eggert, L. (2008). Host identity protocol (HIP) registration extension. *RFC 5203*.

Li, Y., Chen, W., Su, L., Jin, D., & Zeng, L. (2009). Mobility management architecture based on integrated HIP and SIP protocols. In *Proceedings of the International Conference on Telecommunications (ICT '09),* Marrakech, Morocco (pp. 243-247).

Maekawa, K., & Okabe, Y. (2009). An enhanced location privacy framework with mobility using host identity protocol. In *Proceedings of the Ninth Annual International Symposium on Applications and the Internet (SAINT '09)*, Bellevue, WA (pp. 23-29).

Matos, A., Santos, J., Girao, J., Liebsch, M., & Aguiar, R. (2006, March). Host identity protocol location privacy extensions. *IETF Internet Draft*. draft-matoship-privacy-extensions-01.

Matos, A., Santos, J., Sargento, S., Aguiar, R., Girao, J., & Liebsch, M. (2006). HIP location privacy framework. In *Proceedings of the Fiirst ACM/IEEE International Workshop on Mobility in the Evolving Internet Architecture* (pp. 57–62). New York, NY: ACM Press.

Melen, J., Ylitalo, J., Salmela, P., & Henderson, T. (2009, May 26). Host identity protocol-based mobile router (HIPMR). *IETF Internet Draft*. draft-melen-hip-mr-02.

Moskowitz, R., & Nikander, P. (2006, May). Host identity protocol (HIP) architecture. *IETF RFC 4423*.

Moskowitz, R., Nikander, P., Jokela, P., & Henderson, T. (2008, April). Host identity protocol. *RFC 5201*.

Muslam, M., Chan, H., & Ventura, N. (2009). HIP based micro-mobility management optimization. In *Proceedings of the Fifth International Conference on Wireless and Mobile Communications (ICWMC '09),* Cannes, La Bocca (pp. 291–295).

Nikander, P., & Arkko, J. (2004). Delegation of signaling rights. LNCS 2845, (pp. 203-214). Security Protocols 2002.

Nikander, P., Henderson, T., Vogt, C., & Arkko, J. (2008). End-host mobility and multihoming with the host identity protocol. *RFC 5206*.

Nikander, P., & Laganier, J. (2008, April). Host identity protocol domain name system extension. *RFC 5205*.

Nováczki, S., Bokor, L., & Imre, S. (2006). Micromobility support in HIP: Survey and extension of host identity protocol. In *Proceedings of the MELECON 2006* (Vol. *1*, pp. 651-654). Málaga, Spain.

Nováczki, S., Bokor, L., & Imre, S. (2007). A HIP based network mobility protocol. In *Proceedings of the SAINTWONEMO 2007,* Hiroshima, Japan (pp. 48-52).

Nováczki, S., Bokor, L., Jeney, G., & Imre, S. (2008, January). Design and Evaluation of a Novel HIP-Based Network Mobility Protocol. *Journal of Networks*, *3*(1), 10–24.

Pierrel, S., Jokela, P., & Melen, J. (2006, June 19). Simultaneous Multi-Access extension to the Host Identity Protocol. *IETF Internet-Draft*. draft-pierrel-hip-sima-00.

Pierrel, S., Jokela, P., Melen, J., & Slavov, K. (2007). A Policy System for Simultaneous Multiaccess with Host Identity Protocol. IEEE ACNM2007. Munich, Germany.

Rothenberg, C. E., Wong, W., Verdi, F. L., & Magalhae, M. F. (2008). SIP over an Identifier/Locator Splitted Next Generation Internet Architecture. *10th IEEE International Conference on Advanced Communication Technology (ICACT08)*. Republic of Korea.

So, J., & Wang, J. (2008). Micro-HIP a HIP-based micro-mobility solution. In *Proceedings of the IEEE International Conference on Communications Workshops (ICC Workshops '08.)*, Beijing, China (pp. 430-435).

So, J. Y., & Wang, J. (2006). HIP based mobility management for UMTS/WLAN integrated networks. In *Proceedings of the Australian Telecommunication Networks and Applications Conference.*

Varga, A., & Hornig, R. (2008). An overview of the OMNeT++ simulation environment. In *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops (SIMUTools2008)*. Marseille, France.

Varjonen, S., Komu, M., & Gurtov, A. (2009). Secure and efficient IPv4/IPv6 handovers using host-based identifier-locator split. In *Proceedings of the 17th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2009)* (pp. 111-115). Split-Hvar-Korcula.

Varjonen, S., Komu, M., & Gurtov, A. (2010). Secure and efficient IPv4/v6 handovers using host-based identifier-location split. *Journal of Communications Software and Systems*, *6*(1).

Wagner, S. (2006, December 1). Implementation and evaluation of the interaction between host identity protocol and session initiation protocol. *Masterarbeit im Studiengang "Angewandte Informatik*.

Yang, S., Qin, Y., Luo, H., & Zhang, H. (2008). P-HIP: Paging extensions for host identity protocol. In *Proceedings of the IEEE Communications Workshops (ICC Workshops '08),* Beijing, Chaina.

Yang, S., Qin, Y., & Yang, D. (2007). Dynamic hierarchical location management scheme for host identity protocol. Lecture Notes in Computer Science, Mobile Ad-Hoc and Sensor Networks, 4864/2007 as proceedings of MSN 2007.

Yang, S., Zhou, H., Qin, Y., & Zhang, H. (2009, June). SHIP: Cross-layer mobility management scheme based on session initiation protocol and host identity protocol. *Journal of Telecommunication Systems*, *42*(1-2). doi:10.1007/s11235-009-9164-y

Y.ipv6split, I.-T. (2009, March 5). Framework of ID/LOC separation in IPv6-based NGN. *ITU-T Draft Recommendation*.

Y.ipsplit, I.-T. (2009, Feb. 6). General requirements for ID/locator separation in NGN. *ITU-T Draft Recommendation*.

Ylitalo, J. (2005). Re-thinking security in network mobility. In *Proceedings of the NDSS Wireless and Security Workshop,* San Diego, CA.

Ylitalo, J., Melé, J., P. S., & Petander, H. (2008, May 20). An experimental evaluation of a HIP based network mobility scheme. *WWIC 2008, LNCS, 5031/2008*, 139–151.

Ylitalo, J., Melén, J., Nikander, P., & al., e. (2004). Re-thinking security in IP-based micro-mobility. In *Proceedings of the 7th Information Security Conference (ICS'04)*, Palo Alto, CA (pp. 318-329).

Ylitalo, J., Melén, J., Nikander, P., & Torvinen, V. (2004, September 21). Re-thinking security in IP based micro-mobility. *Lecture Notes in Computer Science, 3225/2004*, 318-329.

Ylitalo, J., & Nikander, P. (2006). BLIND: A complete identity protection framework for end-points. *Lecture Notes in Computer Science*, 3957.