

A COMPLETE HIP BASED FRAMEWORK FOR SECURE MICROMOBILITY

László Bokor ¹⁾, Szabolcs Nováczki ¹⁾, Sándor Imre ¹⁾

Abstract

This paper presents current results of designing and evaluating a new micromobility scheme based on the capabilities of Host Identity Protocol (HIP). HIP is a new approach to separate the identifier and locator roles of IP addresses, provides sophisticated security features and efficiently handles end-to-end mobility in global manner, but it shows inefficient behavior when used in scenarios requiring local mobility management. We introduce a complete framework that makes HIP able to serve as an efficient and secure micromobility protocol while preserving all the advantages of the base HIP functions as well. We also discuss a paging method fitting into the proposed framework in order to offer effective location management and improve the system performance. We evaluate our proposal by comparing it to other micromobility protocols using a simulation model implemented in OMNeT++.

1. Introduction

In recent years we have experienced extraordinary growth of data-centric wireless networks and the emergence of IP-enabled mobile devices. Telecommunication systems are altering towards an all-IP based architecture where convergence of wired and wireless technologies, protocols and terminals will provide integrated services on a common packet-based infrastructure. Naturally mobility is one of the most unique characteristics of the future's convergent architectures but mobility introduces a whole set of new challenges to the original Internet: extensions need to be developed to address mobile users' requirements in the widest range of different scenarios [1]. Wireless networks usually cover a large geographical area, which consists of several domains. A mobile user can change its point of attachment to the network basically in two different ways. On one hand the user can move inside a single domain, which is usually referred as micromobility. On the other hand the user can roam between different domains, which is called macromobility [2]. These two main scenarios of mobility can be managed at different layers of the traditional TCP/IP stack [3]. Unfortunately conventional TCP/IP protocols are already heavily overloaded with previously added different functionalities. Nevertheless network level solutions are most general since IP is ubiquitous in the Internet, but optimization and adding extensions to support mobility functions are very difficult, which motivated developers to support Internet mobility by introducing new layers. Host Identity Protocol (HIP) is one of the new approaches providing mobility management mechanisms by interposing the Host Identity Layer between the network and the transport layers [4]. HIP serves efficiently as a macromobility protocol, but shows unnecessary signaling overhead, packet loss and handoff latency in micromobility environment which requires fast, seamless and local handover control [5]. This motivated us to develop a complete HIP based micromobility framework in order to make the base protocol capable of efficiently managing micromobility situations as well.

The rest of the paper is organized as follows. In the next section we give firstly a short overview of HIP, highlighting the basic functionalities, entities, procedures and the macromobility extensions of

¹ Mobile Communication and Computing Laboratory (MC²L) – Mobile Innovation Center (MIK), Department of Telecommunications (BME-HT), Budapest University of Technology and Economics, Magyar Tudósok krt. 2, H-1117, Budapest, Hungary, {goodzi | nszabi | imre}@mcl.hu

the basic protocol. Section 3 introduces the main architecture, the basic operation and the security issues of our HIP micromobility framework called μ HIP, and presents the paging infrastructure for the proposed system. This is followed by the evaluation and simulation results of our framework in Section 4. Finally Section 5 concludes the paper.

2. Overview of Host Identity Protocol

There are lots of solutions providing uninterrupted IP connectivity for mobile entities in networks of the new century [6], [7], [8], [9]. Usually these solutions are based on the classic TCP/IP stack thus sharing the same basic problem: mobile entities are identified by IP addresses that depend on their actual topological location. This leads to semantically overloaded IP addresses as they are both identifiers and locators at the same time. This dualism makes mobility management very inconvenient because every movement (i.e. IP address change) indicates that all ongoing connections break up and must be established again at the new location.

The main concept of Host Identity Protocol (HIP) is to separate locators from identifiers [10], [11]. A new layer (Host Identity Layer) is introduced between the network and the transport layers. HIP defines a new, cryptographic namespace consisting of the Host Identifiers (HIs). HIs are devoted to hold the identity of nodes while IP addresses are continue act as pure locators. The basic function of HIP is to set up HI-based connections between nodes and to map HIs to IP addresses and vice versa. Using HIP, transport layer connections are no more bound to IP addresses, and connections do not have to be broken if location of hosts change. HIs are usually represented in protocol messages by their 128 bit long hash, the Host Identity Tag (HIT). In order to establish end-to-end connection HIP defines a four-packet handshake called the Base Exchange (BE). The BE results an IPSec Encapsulated Security Payload (ESP) and Security Association (SA) pair [12]. In case of moving endpoints the HIP connections may need to be updated. In such cases the mobility extension of HIP is used. This is a single three message sequence, which starts with an UPDATE packet holding the new locator information. The other packets are to securely verify the information. Since transport layer connections are bound to HIs, the address changes in the IP layer are totally transparent to applications running on a HIP node. This property makes HIP macromobility management and multihoming provisioning very convenient, simple and fast [13], [14]. Initial reachability of mobile nodes might need assistance of a special network entity called the Rendezvous Server (RVS). All mobile nodes should register its IP address at an RVS and keep this registration up to date. The RVS relies the first packet of the BE towards the mobile node [15], [16], [17].

There are already several enhancements and advanced applications that relies on the basic functions above of HIP [18], [19], [20], and show its wild range usability. In case of our extension HIP Service Discovery and HIP based Signaling Delegation is relevant. In [17] a registration extension for HIP is defined and shows how HIP enabled hosts can register themselves for a service to use which is provided by another HIP capable network entity. On the other hand [21] discusses two different ways to discover the available services. In the first scenario (called On-the-Path Service Discovery) the service provider resides on the packet forwarding path and listens to traffic. It offers its services for nodes communicating on the path by sending Service Announcement Packets (SAP) to them. In the second scenario (called Regional Service Discovery) the HIP host may initiate the service discovery by injecting Service Discovery Packets (SDP) into the network. The other powerful property of HIP is its capability to provide secure signaling delegation. According to the basic concept an initiator node requests another node (i.e. a mobility anchor point) to send signaling messages on behalf of it. In HIP-based networks there is a quite straightforward solution: based on the cryptographic identifiers special certificates can be generated by the nodes, which is the basis of secure signaling delegation [22].

3. μ HIP: Micromobility in the Host Identity Layer

As we introduced in the previous section, the mobility management capabilities of HIP fit the protocol well to the requirements set up by macromobility environments. Unfortunately HIP introduces unnecessary control messages, remarkable packet loss and handover latency in environments requiring localized mobility management, making the HIP approach much less efficient in such cases. In this chapter we propose a micromobility extension for HIP called μ HIP, which adds a gateway centric micromobility support with paging extension to the protocol. Our solution is based on a new network entity called Local Rendezvous Server (LRVS) that extends the functionalities of a normal HIP Rendezvous Server (RVS).

3.1. The proposed HIP micromobility architecture

Our proposed HIP micromobility architecture divides the network into administrative domains (i.e. micromobility areas). For every domain, there is an access network containing several wireless IP points of access (i.e. access routers with regular IP forwarding engine), and a Local Rendezvous Server responsible for managing Mobile Nodes (MNs) in the given domain and for connecting μ HIP access networks to the Internet. LRVS entities serve as gateways while using functions similar to RVSs: they provide registration service for MNs in a well defined micromobility area; in addition MNs are attached to a μ HIP access network using the IP address mapping function of the LRVSs. Every MN can register its locally valid IP address (referred as local IP address or IP_L in the rest of the paper) at the LRVS. The local IP address is valid only in the given domain (i.e. not a globally routable address). The LRVS maps the local IP address of the MNs to a globally routable address (IP_G). IP_G is chosen from a private address domain reserved for the given LRVS and is used to register the MNs at their RVSs and to deliver packets outside the domain.

3.2. Initiation mechanism

If a MN joins a new, locally managed network area, there is a need for an initialization mechanism in order to start the inner-domain life of the mobile node (see Figure 1). After entering, the MN physically connects to one of the access routers (AR) of the domain. Right after detecting the newly established physical connection and getting a serviceable IP address (IP_L), the MN either may actively initiate a HIP service discovery procedure or passively wait for a service announcement in order to detect the LRVS service provided in the visited network area [21]. Irrespectively of the used mechanism the MN will eventually be informed about the HIT and the IP address of the LRVS responsible for the actual domain. Step 1-3. in Figure 1 (yellow arrows) shows the case of Passive discovery where the MN (due to its movement) sends an UPDATE packet to its RVS and current Correspondent Nodes (CNs). The LRVS – according to the procedures of Passive discovery – intercepts the UPDATE packet, verifies the I1 source HIT and sends back a Service Announcement Packet (SAP) to the MN containing R1 data and information about the LRVS services (HIT and IP address of LRVS). After that the MN continues the service discovery by completing the registration to the LRVS with the final I2-R2 sequence. Till this point everything works almost the same way as it would be with a normal RVS. The main difference is that during this service discovery and registration procedure the LRVS not only opens a new entry in its database and registers the MN's HIT with its new, local IP address but maps it with a globally routable IP address (IP_G) as well.

After the MN is registered at the LRVS, it needs to perform the update or registration at the RVS and its current CNs as well; to be reachable for the current and future communication partners (step 4, yellow arrow). Therefore the MN – strongly relying on the self-certifying cryptographic identifiers provided by HIP – delegates its signaling rights [22] to the LRVS at which it is registered. The appropriate certificates can be sent during the service discovery of MNs, resulting that the LRVS will own the rights to signal on behalf of all mobile nodes in the current

micromobility domain. In possession of this delegation the LRVS is able to securely register or update to the RVSs and CNs on behalf of the MNs with globally routable IP addresses assigned to them.

After this initiation procedure the MN is registered at the LRVS (with the $HIT_{MN-IP_L-IP_G}$ triplet) and at the RVS (with the HIT_{MN-IP_G} pair) as well.

If a node (MN_2 in Figure 1) that had performed the same initialization mechanism in a different domain wants to establish a HIP association with an also initialized MN_3 , it sends the first packet (I1) of the Basic Exchange (step 1, blue arrow). In this packet the source IP address is the local IP address of the initiator (i.e. MN_2), the destination IP address is the IP address of the MN_3 's RVS (here we assume that the RVS of MN_2 and MN_3 are identical), the destination HIT is the HIT of MN_3 . The I1 packet is intercepted by the LRVS of the initiator's domain (i.e. $LRVS_2$). This LRVS changes the source IP address of the packet to the globally routable IP address of MN_2 (IP_{G2}) and sends the packet to the RVS (step 2, blue arrow). The RVS forwards the packet towards the registered (i.e. IP_{G3}) address of MN_3 (step 3). $LRVS_3$ knows the actual attach point of MN_3 , so it forwards the packet by changing the destination IP address of the packet (IP_{G3}) to the MN_3 's local address (IP_{L3}) (step 4, blue arrow). The BE continues in the regular way, without the inclusion of the RVS, but with the address changing function of the two LRVSs (step 5, blue arrow). (Note that the CHECKSUM field of IP packets should be recomputed after every address change, similarly as in case of standard RVSs.)

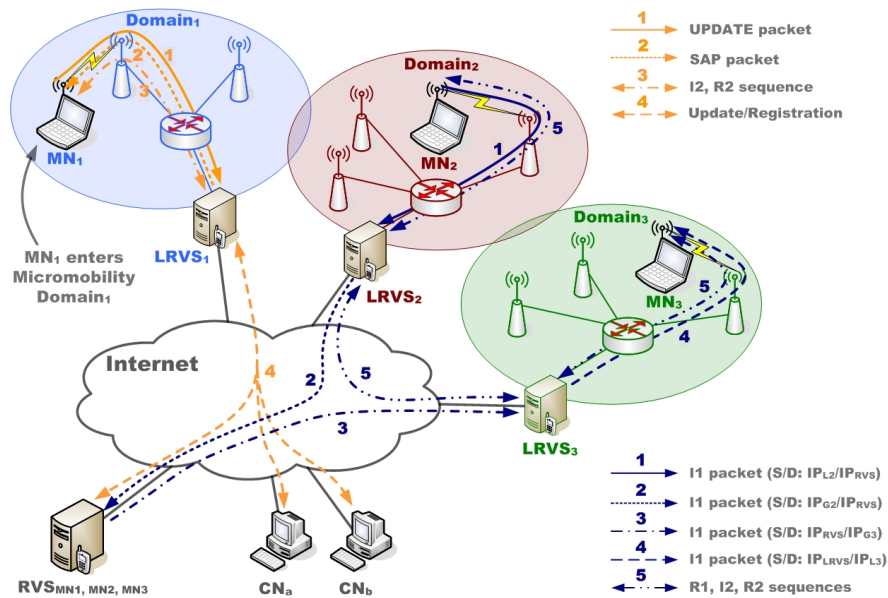


Fig. 1. Initiation mechanism and connection establishment in the μ HIP framework

After this message sequence there is an active HIP association available between the two nodes, and they can begin sending data packets to each other. Data packets are forwarded by the LRVSs to the actual local IP addresses of the MNs in the same way as they did during the BE. It is crucial to observe that due to the HIP based signaling delegation all the above functions of the LRVS system are to be considered secure.

3.3. Managing the handovers

3.3.1. Intra-domain handover procedures

If a moving node which had performed the initialization mechanism described in the previous section, moves to another possible point of attachment of the same domain, the MN will receive a new IP_L from a servicing AR belonging to the same LRVS (see MN_1 and yellow arrows in Figure

2). In this case the MN – realizing the change of its IP address – simply updates its registration (and if needed its delegation certificate as well) with its new local IP address at the LRVS.

The used update mechanism is detailed in [17]. It is important to note that neither the CNs of the MN nor the RVS has to be informed about the movement as it is locally handled. The address changes within a domain are managed by the LRVS system responsible for that particular domain: the movements of the MN are completely hidden from the outside world in order to reduce the signaling overhead, packet loss and handover latency in a significant degree.

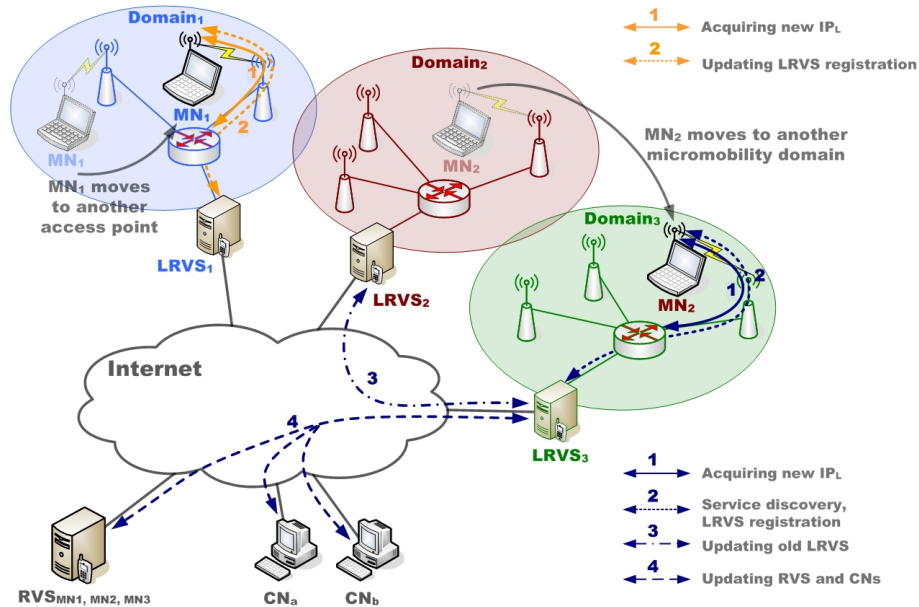


Fig. 2. Intra-, and inter-domain handover procedures

3.3.2. Inter-domain handover procedures

MN₂ and blue arrows in Figure 2 demonstrate a possible inter-domain handover scenario. In such cases, the MN moves between local administrative domains (i.e. Domain₂ and Domain₃) thus invoking global mobility management procedures of μ HIP. Arriving at the new domain, the MN will receive its new IP_L, and will discover the service parameters of the new LRVS (LRVS₃). After the MN realized that it leaved the previously used administrative domain by entering a new one and learned the HIT and IP address of the new LRVS, it performs a registration mechanism. This works the same way, as we described in Section 3.2. Since MN changes its old LRVS, it has to update its RVS and all the correspondent nodes with ongoing communication. But the first thing to do is to update the old LRVS (i.e. LRVS₂) to make it able to forward packets sent to the MN's old globally routable IP address as long as the MN has not finished updating the RVS and all of its CNs (step 3, blue arrow).

After the old LRVS is updated, MN begins to update its CNs and at last the RVS (step 4, blue arrows). It is done by performing a regular update mechanism, described in [15]. This update informs the RVS about the MN's new IP_G, which was given by the new LRVS (i.e. LRVS₃). When the MN finished all of the required updates with its CNs and the RVS, it removes the registration association at the old LRVS, or this association can be timeouted and automatically removed.

3.4. Paging

In mobility supporting IP based networks the exact topological location of every mobile node must be known for appropriate packet delivery. Therefore a serious trade-off has to be considered namely how tightly the network should track the actual location of a mobile node (i.e. how frequently should a MN send location updates) versus the required resources to locate a particular mobile node whose current position is not accurately known. In order to make possible to deal with

this trade-off in our proactive micromobility supporting framework, a HIT specific multicasting based paging extension is to be introduced in the system.

The basic idea of our paging scheme is shown in Figure 3 via an example μ HIP network configuration. The case of MN_1 shows the extended initialization mechanism with paging support, while the case of MN_2 introduces the procedures when a correspondent node from the outside network initiates a transmission towards an already initialized but actually inactive MN (MN_2) residing inside the domain. During the extended initialization the MN registers itself into the currently entered Paging Area (PA) as well. If there are no ongoing communication sessions on a registered MN, the mobile node only needs to update its LRVS when it migrates into another Paging Area. Therefore when an incoming session is detected in the LRVS (i.e. CN's packets are reaching the designated MN's LRVS), and if the LRVS system doesn't know the exact location of the destined MN (i.e. the MN_2 is in standby mode for a long time and its registration information is outdated, only its Paging Area is known), then it triggers the paging mechanism: appropriate paging requests will be sent by the LRVS system towards all access routers within the designated MNs suggested location area determined using a Paging Registration Database. Transporting the paging requests is done by a simplified HIT specific multicasting method based on [23], that carries the requests towards the MN through the corresponding subset of ARs. The MN will be eventually reached thus forcing it to perform a registration with the LRVS which results in successful connection build up with the initiator CN.

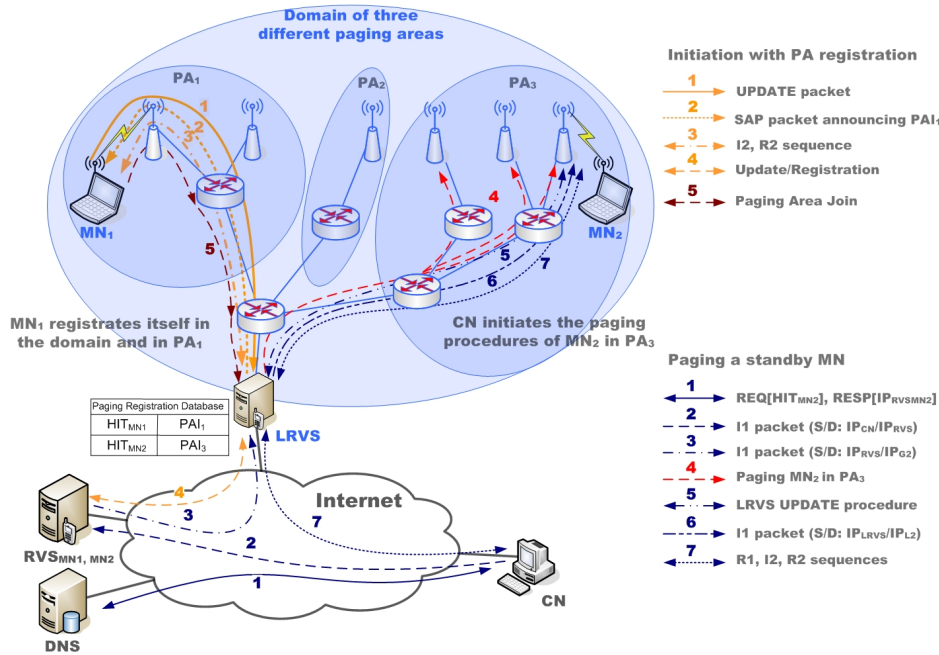


Fig. 3. Mechanisms of paging in the μ HIP framework

3.4.1 The Paging Registration Database

The Paging Registration Database (PRD) is a database located in the LRVS system. Every record in the PRD contains a Host Identity Tag (HIT) – Paging Area Identifier (PAI) pair. In our proposal PAIs are multicast addresses uniquely assigned to every paging area. Paging Area updates (i.e. PRD mappings) have longer timeout compared to a normal LRVS registration lifetime implicating a longer interval between consecutive PA updates. Note that both a normal LRVS registration/re-registration and a PRD mapping/remapping sequence can be initiated by sending a standard HIP UPDATE packet with an included LOCATOR parameter, but the different requests should be distinguished with different REG_INFO content (e.g. using the Reg_Type field for differentiating between the two functions) [17]. Thus the Paging Registration Database can be

maintained and kept updated similarly to the LRVS registration synchronization mechanisms introduced in the previous chapter.

3.4.2 Carrying the paging messages

In [23] authors present a Host Identity Specific Multicast (HISM) model and a unified Version Independent Group Management Protocol capable of handling HITs in order to provide solution for access control, accounting, mobility, and IPv4/v6 transition relating problems of the conventional multicasting methods. Based on their model we introduce a method which perfectly suits for the requirements of carrying the paging messages in our HIP based micromobility framework.

A Mobile Node after entering a μ HIP domain and finishing its initialization duties is considered to be registered in the LRVS system. However, in order to make prepared the MN for the paging functions we should integrate some other procedures into the initialization mechanisms. The scheme with the extended initialization is the following (Figure 3, case of MN_1).

During the LRVS Service Discovery sequence, the MN must be informed about its current paging area. The required information is the multicast group's IP address uniquely assigned to every single paging area, and can be included into the LRVS's SAP packet using the REG_INFO parameter (step 2, yellow arrow). After approving all the necessary information, the μ HIP implementation registers the multicast address of the current paging area in the operation system's registry and prepares the Paging Area Join message. This message is a multicast group management Join message containing the HIT_{LRVS} as we are to create a source specific multicast tree based on HIT information, and the HIT_{MN} for possible supplemental authentication purposes according to [23]. The Join message arrives to the first multicast router which starts the multicast tree building procedures (step 5, yellow arrows). After reaching the multicast router of the LRVS system (or any other intermediate router which is already on a branch of the issued multicast tree) the paging area join procedure finishes and the MN is ready to be paged.

Note that our μ HIP paging scheme doesn't require implementation of HIP layers in the routers even though the multicast tree is built based on HIT information. The only need is to implement the unified group management protocol, and using HITs in the routing table entries as tree states. All of these changes can be done by upgrading the router's multicast software.

4. Simulation Results

In order to evaluate the efficiency of the proposed μ HIP micromobility framework and compare our scheme to the standard HIP mobility and to a well known micromobility protocol called Cellular IP [24], we designed a discrete event simulation model and implemented it in OMNeT++, which is a component based, open source and open architecture simulation environment [25]. The implemented simulation model realizes the three different protocols, thus simulated mobile nodes can use the mobility supporting features of standard HIP, μ HIP and CIP, but can not rely on the paging functions of the latter two micromobility methods. The network model used for the evaluation consists of three main parts. We set up a domain for the correspondent nodes, a mobility domain, and a domain for the air interface containing the wireless access points and the mobile node. The MN is able to migrate between different APs with a constant speed such provoking intra- and/or inter-domain handovers. Inducing 150 independent handovers during simulation runs we measured the following parameters:

- *Handover Latency*: the time interval between the last packet arrived at the MN in the old network and the first packet fetched from the new AP.
- *Packet Loss*: the difference between the sequence numbers of the last packet arrived at the MN in the old network and the first packet fetched from the new AP.
- *Signaling Overhead*: the number of the mobility protocol messages during the pre-defined simulation time.

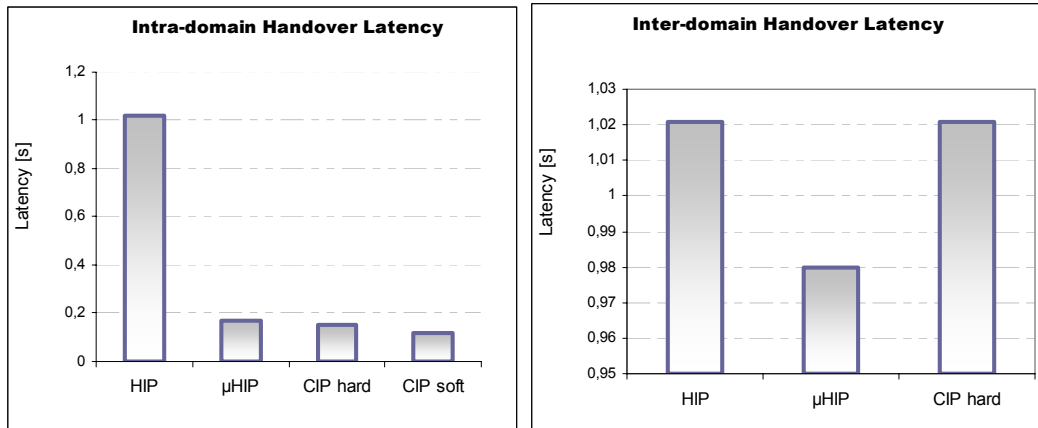


Fig. 4. Average latency of intra-domain and inter-domain handovers

Figure 4 shows the results gained from Handover Latency measurements. One can observe that the basic HIP specification performs very badly in intra-domain scenarios, which proves that our proposal extremely reduces the latency during intra-domain handoffs. This result comes from the fact that in basic HIP mobility the RVS and all the CNs must be updated after every AP change, while in case of μ HIP only the LRVS should be informed about the fact of intra-domain handovers. CIP outperforms μ HIP because in case of CIP, the mobility signaling messages must reach only the Cross-over Router, while in μ HIP these messages must arrive at the LRVS in every case. However the difference is not remarkable. In case of inter-domain handovers μ HIP presents the best performance. In inter-domain scenarios CIP uses MIPv6 which basic operation is similar to the standard HIP mobility functions. Therefore the results are explicable by the old LRVS updating mechanism of our protocol (see step 3, blue arrow in Figure 2), however this advantage is topology-dependent: in our simulated network the RTT between the old and the new LRVS is much less than between the new LRVS and the CNs.

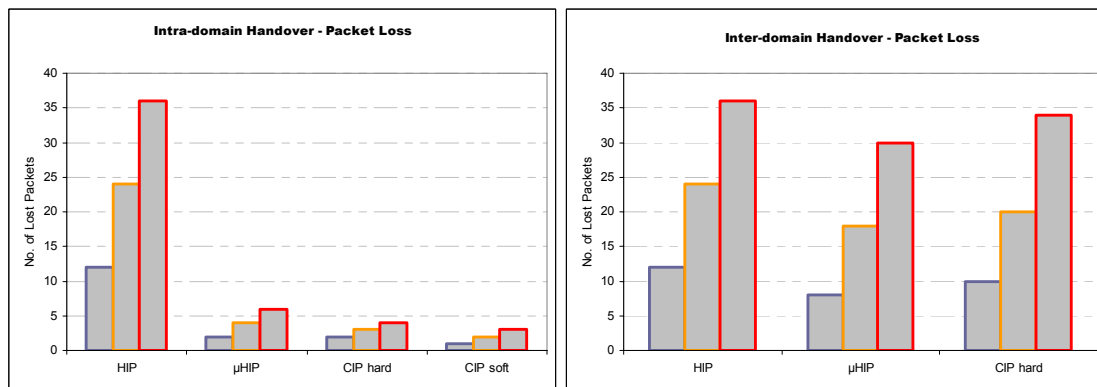


Fig. 5. Packet Loss per handover in intra-domain and inter-domain scenarios

The Packet Loss measurements are represented in Figure 5. In order to highlight the scalability issues of the examined protocols we defined three different configurations regarding the number of CNs involved (increasing from blue marking to red, respectively). One can recognize that in intra-domain scenarios μ HIP reduces the number of lost packets with a significant level, but CIP slightly outperforms our method. The explanation is the same as above: in case of CIP the update messages must reach only a Cross-over Router. Inter-domain scenarios reveal that there is no significant difference between the three evaluated protocols in this meaning, though μ HIP shows the best performance. The explanation is that if standard HIP mobility is used, the MN has to update all of the active HIP associations. Until an actively transmitting CN is not updated, all data packets destined to the old IP address of MN will be lost. The more CNs have to be updated, the higher

probability of packet loss is identified. But in our method if the MN changes the visited domain, it does not immediately closes its rendezvous association with the old LRVS; moreover, the MN updates its registration at the old LRVS by reporting the new IP_G address. This reduces the probability of potential packet losses during the handoff mechanism, since the MN is still reachable via the old LRVS.

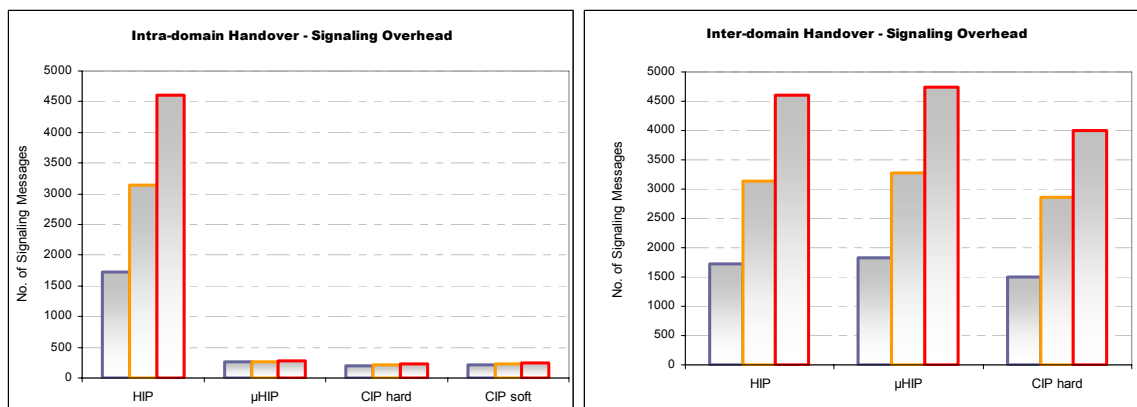


Fig. 6. Signaling overhead measured during intra-domain and inter-domain movements

Figure 6 illustrates the simulation results of measuring protocol overheads. μ HIP and CIP have approximately the same overhead during intra-domain handovers, while standard HIP shows inadequate performance in this matter as we expected. The reason of the little advantage of CIP compared to μ HIP is the fact that in Cellular IP all the communication packets (not only signaling messages) are used for location updates (i.e. route updates on the communication path in the micromobility domain). In case of inter-domain handovers μ HIP presents the highest overhead, however the difference is not remarkable. Since in our proposal at inter-domain handover an additional registration is needed with the new LRVS, and the old LRVS has to be updated as well so the results in signaling overhead measurements show some more compared to standard HIP and CIP related signaling messages.

5. Conclusions

In this paper we presented a brief survey of Host Identity Protocol and its living extensions. Motivated by the drawbacks of the existing HIP mobility, we introduced a micromobility extension for HIP. We proposed a new network entity, the Local Rendezvous Server, and a new HIP network architecture with the appropriate protocol mechanisms. We described how this new mechanism should be initiated, how it can manage intra-, and inter-domain handovers, and how paging can be performed. Our scheme was modeled and implemented in OMNeT++ simulation environment together with the basic HIP protocol and Cellular IP. Simulation results show that the handover latency, the number of lost packets during handoffs and HIP related signaling overhead can be radically reduced if our extension is used in micromobility environments, and μ HIP doesn't introduces significant overheads in macromobility scenarios as well, however, in some cases CIP slightly outperforms our proposal.

As a part of the future work we plan to make more representative simulations (extended with the implementation of paging mechanisms in CIP and μ HIP as well) to the base HIP mobility and to other existing micromobility protocols (e.g. HMIPv6). There is a far-gone research work regarding to enhance the reliability of our gateway centric micromobility extension by introducing an anycast based LRVS clustering scheme. Our future work includes extensive simulations of these efforts as well.

Acknowledgments

This work was supported by the ANEMONE project (which is partly funded by the Sixth Framework Programme of the European Commission's Information Society Technology) and the Mobile Innovation Center Hungary. The authors would like to thank all participants and contributors who take part in the work.

References

- [1] J.F. Huber: "Mobile next-generation networks", IEEE Multimedia, V. 11, I. 1, pp.72-83, Jan-March 2004.
- [2] Pierre Reinbold, (FUNDP) and Olivier Bonaventure, (UCL): "IP Micro-Mobility Protocols", IEEE Communications Surveys & Tutorials Third Quarter 2003, pp 40-57.
- [3] Deguang Le, Xiaoming Fu, Dieter Hogrefe: "A review of mobility support paradigms for the internet", IEEE Communications Surveys & Tutorials, V. 8, I. 1, pp. 38-51, 2006.
- [4] T. R. Henderson: "End-Host Mobility and Multihoming with the Host Identity Protocol", IETF Internet Draft <draft-ietf-hip-mm-05>, March 2007.
- [5] T. R. Henderson, J. M. Ahrenholz, and J. H. Kim: "Experience with the Host Identity Protocol for Secure Host Mobility and Multihoming", IEEE Wireless Communications and Networking, V. 3, pp. 2120-2125 March 2003.
- [6] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert: "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.
- [7] D. Johnson, C. Perkins, J. Arkko: "Mobility Support in IPv6", IETF RFC 3775, June 2004.
- [8] P. McCann: "Mobile IPv6 Fast Handovers for 802.11 Networks", IETF RFC 4260, November 2005.
- [9] H. Soliman, C. Castelluccia, K. El Malki, L. Bellier: "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", IETF RFC 4140, August 2005.
- [10] R. Moskowitz, P. Nikander: "Host Identity Protocol (HIP) Architecture", IETF RFC 4423, May 2006.
- [11] R. Moskowitz, P. Nikander, P. Jokela, T. Henderson: "Host Identity Protocol", IETF Internet Draft <draft-ietf-hip-base-08>, June 2007.
- [12] P. Jokela, R. Moskowitz, P. Nikander: "Using ESP transport format with HIP", IETF Internet Draft <draft-ietf-hip-esp-06>, June 2007.
- [13] T. Henderson: "End-Host Mobility and Multihoming with the Host Identity Protocol", IETF Internet Draft <draft-ietf-hip-mm-05>, March 2007.
- [14] T. R. Henderson, J. M. Ahrenholz, and J. H. Kim: "Experience with the Host Identity Protocol for Secure Host Mobility and Multihoming", IEEE Wireless Communications and Networking, V. 3, pp. 2120-2125 March 2003.
- [15] J. Laganier, L. Eggert: "Host Identity Protocol (HIP) Rendezvous Extension", IETF Internet Draft <draft-ietf-hip-rvs-05>, Jun 2006.
- [16] P. Nikander, J. Laganier: "Host Identity Protocol (HIP) Domain Name System (DNS) Extensions", IETF Internet Draft <draft-ietf-hip-dns-09>, April 2007.
- [17] J. Laganier, T. Koponen, L. Eggert: "Host Identity Protocol (HIP) Registration Extension", IETF Internet Draft <draft-ietf-hip-registration-02>, June 2006.
- [18] M.Särelä, P. Nikander: "Applying host identity protocol to tactical networks", In Proceedings of IEEE Milcom 2004, Monterey, California, USA, Nov 2004.
- [19] Joseph Y.H. So, Jidong Wang: "HIP Based Mobility Management for UMTS/WLAN Integrated Networks", Australian Telecommunication Networks and Applications Conference 2006.
- [20] P. Nikander, J. Arkko and B. Ohlman: "Host Identity Indirection Infrastructure", in Proc. of The Second Swedish National Computer Networking Workshop (SNCNW2004), November 2004.
- [21] P. Jokela, J. Melen, J. Ylitalo: "HIP Service Discovery", IETF Internet Draft <draft-jokela-hip-service-discovery-00>, June 2006.
- [22] P. Nikander and J. Arkko. "Delegation of Signaling Rights". Security Protocols 2002, LNCS 2845, pp 203-214, 2004.
- [23] Zsolt Kovacshazi, Rolland Vida: "Host Identity Specific Multicast", ICNS, p. 1, International Conference on Networking and Services (ICNS '07), Athen, 2007.
- [24] Andrew T. Campbell, Javier Gomez, Sanghyo Kim, Zoltán R. Turányi, András G. Valkó, Chieh-Yih Wan: „Internet micromobility”, Journal of High Speed Networks V. 11, pp. 177-198, IOS Press 2002.
- [25] OMNeT++: A public-source, component-based, modular and open-architecture discrete event simulation environment. Official homepage: <http://www.omnetpp.org/>