A SURVEY ON MICRO MOBILITY MANAGEMENT OF HOST IDENTITY PROTOCOL

Zeynep GURKAS AYDIN[1], Hakima CHAOUCHI[2], A. Halim ZAIM [3]

1*Istanbul University Engineering Faculty Computer Engineering, Istanbul, TURKEY
2 Telecom and Management SudParis, CNRS SAMAVOR, UMR 5157, Paris, FRANCE
3Istanbul Commerce University, Institute of Science and Engineering, Istanbul, TURKEY
E-mail: zeynepg@istanbul.edu.tr, hakima.chaouchi@it-sudparis.eu, azaim@iticu.edu.tr

Abstract: *Host Identity Protocol (HIP) is a new protocol that employs the idea of separation of the role of IP addresses as host identification and location identifier. It also introduces protocol level security in its nature. It is manly designed for macro mobility as Mobile IP, but it has some shortcomings in terms of micro mobility regarding to signaling load and handover latency. Several researches and proposals have been introduced to enhance the micro mobility features of HIP. This paper is a survey on micro mobility techniques of HIP.*

Keywords: *Keyword1, keyword2, keyword3.*

1. Introduction

Mobility is a very important feature for internet and networking architecture. With the fast spreading of IP based wireless and mobile networking, the mobility of users became indispensable. With mobility, some key features revealed such as continuing the quality of service during movements and several proposals and techniques have been introduced based on different protocols in order to provide the mobile users' needs.

Generally, the techniques and rules which are applied as a mobile node moves frequently within a network and changes it point of attachment, are called mobility management. Traditionally, in TCP/IP protocol stack, there are different mobility management techniques operating in different layers. Host Identity Protocol is a new layer for TCP/IP stack locating between network and transport layers and offering several functionalizes from security to multi homing.

In this study, we firstly present an overview for key features of Host Identity Protocol and later a survey on micro mobility management proposals of HIP.

2. Host Identity Protocol

In today's internet architecture, IP addresses are used both as locators and as identifiers of a node in the network. This dual role of IP addresses has several problems. Firstly, IPv4 is still widely used than IPv6, so address space of IPv4 becomes insufficient due to increasing Internet usage and number of hosts. Furthermore, as the mobility of devices increase, dual role of IP addresses makes mobility management complicated.

In order to solve these problems Host Identity Protocol (HIP) is proposed by IETF (Internet Engineering Task Force) and IRTF (Internet Research Task Force) [1]. HIP approach requires adding a new layer in the TCP/IP stack between the transport layer and the IP layer. The role of this layer is to make mapping between host identities, which are used in upper layers of TCP/IP stack.

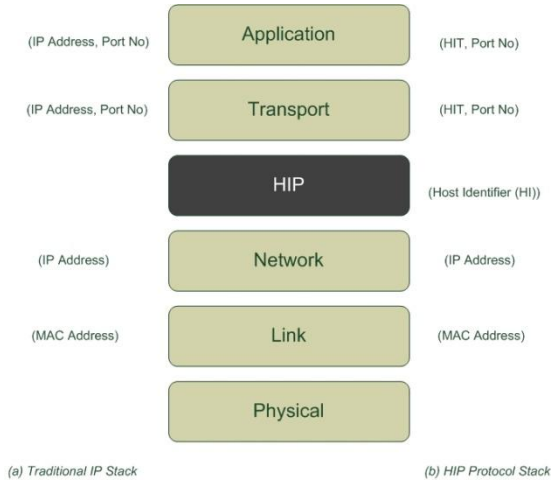


Figure 1. Host Identity Protocol in TCP/IP protocol stack

One of the design choices defined in HIP is, that the Host Identity (HI) is the public key from a public/private key pair. This key can be represented by the Host Identity Tag (HIT), a 128-bit hash of the HI, and has to be globally unique in the whole Internet universe. Another

Received on:16.01.2011
Accepted on:08.04.2011

representation of the HI is the Local Scope Identity (LSI) which is 32-bits size and can only be used for local purpose. One of the issues completely presented in HIP is that the Host Identity (HI) is the public key from a public/private key pair. This key can be represented by the Host Identity Tag (HIT), a 128-bit hash of the HI, and has to be globally unique in the whole Internet universe. Another representation of the HI is the Local Scope Identity (LSI) which is 32-bits size and can only be used for local purposes.

2.1. HIP Namespace

HIP introduces a new namespace composed of Host Identities (HIs). A Host Identity is a cryptographic entity which corresponds to an asymmetric key-pair. The public identifier associated to a HI is consequently the public key of the key-pair. A host may have more than one HI's but this HIs are uniquely related to a single host. HIs will assume the identifier role in upper layers. HIs become public if they are stored in DNS. The length of the HI depends on the cryptographic algorithm used. In order to cope with the problems that may occur in upper layers, two fixed length identifiers are defined in HIP.

A Host Identity Tag (HIT) is a 128-bit representation for a HI. It is a cryptographic hash over HI. There are two advantages of using a hash: a) It is fixed length, so it is easier to use in upper layer protocols and b) It represents the HI in a consistent format to the protocol.

HITs identify the sender and recipient of HIP packet. It is unique. It is rarely possible that a single HIT may represent more than one HI.

A Local Scope Identifier (LSI) is a 32-bit or 128-bit local representation of HI. It may be needed to use in existing APIs or protocols. It is shorter than HIT as advantage but just available for a local scope. The 32 bit long version is IPv4 compatible and a 128 bit long version is IPv6 compatible [1].

2.2. Base Exchange

The HIP Base Exchange is a cryptographic key-exchange procedure performed at the beginning of the HIP communication establishment. The HIP Base Exchange is built around a classic authenticated Diffie-Hellman key exchange. The BE is four-way packet exchange between the Initiator (I) and the Responder(R). The four way handshake of HIP BE is shown in Figure 2. Base Exchange is defined in RFC 5201[1] and RFC 5203 [2].

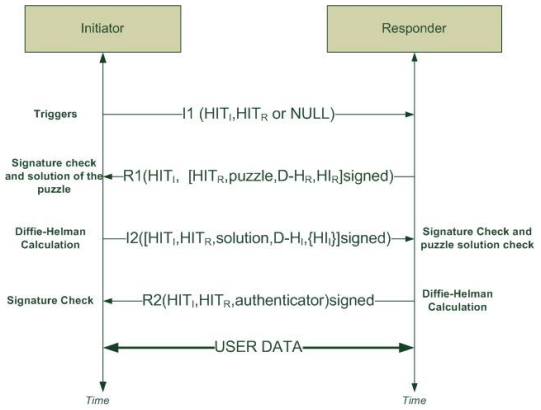


Figure 2. HIP Base Exchange

2.3. Rendezvous Servers

The initial IP address of a HIP host should be stored in order to make the host reachable. Traditionally, the DNS is used for storing this information. The problem with the DNS system is the latency; updating the location information each time the MN moves, the update is not fast enough. The Rendezvous Mechanism is designed to solve this problem. The Rendezvous Server (RVS) keeps the all information of HIP communication. The location information of RVS is just stored in DNS. If a MN wants to communicate with other MNs, all nodes have to register with their RVS. Figure 3 shows the HIP Base Exchange with RVS.

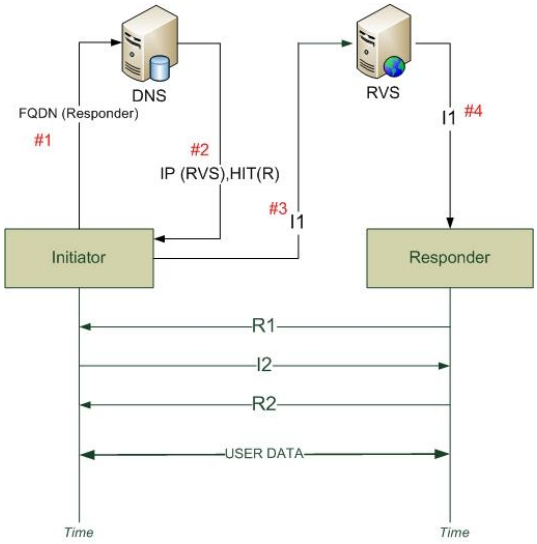


Figure 3. HIP Base Exchange with RVS

The HIP enable Responder(R) should register to the RVS with its HIT and current IP address. Firstly, the initiator queries about the responder with FQDN (Fully Qualified Domain Name) message from DNS and DNS response to it with the IP address of RVS that the responders belongs to and the HIT of responder. When Initiator (I) wants to establish a connection with R, it first send the I1 packet to one of the R's rendezvous servers or to one of IP addresses (if it can be learnt via DNS). Initiator gets the IP address of R's RVS from DNS and sends the I1 packet to the RVS for Base Exchange. RVS checks weather

it has the HIT of I1 packet. If HIT belongs to itself, it sends the I1 packet to related IP address. R sends the R1 packet directly to Initiator without RVS. Rendezvous mechanism is defined id RFC 5204 [3].

3. Micro Mobility Management On Host Identity Protocol

In HIP, mobility management is defined in a general scope in RFC 5206 [4]. According to basic proposal for mobility management of HIP, when a mobile node changes its location in the network, UPDATE message exchange occurs. A LOCATOR parameter in this packet carries the new IP address to the corresponding nodes or rendezvous servers. With this packet, two nodes may either decide to continue their communication with their current connection or decide to re-key their association and generate a new Diffie-Hellman key. Figure 4 shows the basic updating scenario without any rekeying between two nodes. UPDATE messages may include more parameters but the basic parameters are shown in the figure.

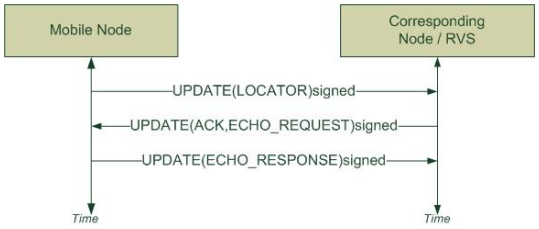


Figure 4. Update Exchange of HIP

HIP also has multi-homing support in its nature. In HIP terminology, while the mobility means changing locators, the multi homing means adding new locators for a mobile node. A node with multi homing support may have multiple interfaces with multiple IP addresses.

The most research contributions of HIP are based on mobility management due to the shortcomings of HIP's location and handover management procedures. In HIP, both micro-and macro mobility procedures is implemented within the same rules. As we stated before, HIP is mainly designed to cope with macro mobility such as Mobile IP, so managing the micro mobility with macro mobility rules reveals out some problems in terms of performance and usability.

For frequent moves of a mobile node, signaling overhead and latency of update exchange may be significantly high due to network topology and number of movements. As known, most of the movements of a mobile node in a network are behaving as micro mobility. Also, if the location of CNS and RVS is geographically far from MN, the latency of updates brings an overhead for network performance. There are also problems for mobile node that, since it has to complete some security based operations during the update process if necessary, an overhead reveals for these nodes.

Due to the basic problems of HIP's mobility management above, there are several researches considering a contribution to HIP for micro mobility management, especially for handover management. This section presents a overview of proposed studies for HIP related to handover and location management.

3.1. μHIP

μHIP [5] extends the HIP with a gateway centric network component and paging extension. This new network component is called Local Rendezvous Server (LRVS), thus extends the properties of RVS. μHIP proposes to divide the network domain into various administrative domains; each one is managed by LRVS. In every domain, there is an access network and a LRVS. LRVS is responsible for managing the mobile nodes and connections of μHIP enabled access networks to the Internet. Mobile nodes register their local IP addresses to the LRVS. LRVS maps local and global IP addresses as in HMIP. LRVS inherits the role of RVS and also acts as a gateway to the Internet.

a) Initiation

When a MN enters into a new domain, it needs to start an initiation mechanism to communicate within this domain. After entering to the domain, MN connects to an Access Router (AR) in a regular way. After connection and getting a new local IP address, MN, either starts a HIP discovery procedure or wait for the service announcement of LRVS. After that, MN gets information about the HIT and IP address of the LRVS. Then, service discovery happens in which MN waits for the service announcement of LRVS. MN sends UPDATE packets to its CNs and LRVS. LRVS receive the update packet and verifies I1 source HIT, replies to MN with SAP (Service Announcement Packet) including R1 and information about LRVS. Then, MN continues its registration to LRVS with service discovery procedure with I2-R2 message pair. Until this point, everything seems like RVS registration procedure. The basic difference is that : during this service discovery and registration procedures, LRVS not only open a new database record about MN's new HIT and maps with local IP address, but also maps the HIT with globally routable IP address. After the registration of MN to LRVS, sending an update or a new registration is needed to RVS in order to be reached by its CNs. After all that steps, MN is registered to LRVS with HIT_{MN}-IP_{local}-IP_{global} triplet, to RVS with HIT_{MN}-IP_{global}

b) Intra-Domain Handovers

If a MN moves a different point of attachment within the same domain, it starts to receive service from a different AR in the same LRVS service domain. MN that realizes the change of its IP address updates its record at LRVS with its new IP address. CNs or RVS of the MN are not informed about this movement and updates. LRVS is responsible for the movements within the domain. Since network components out of the MN's domain are not informed about the movements, signaling overhead, packet loss and handover latency is reduced.

c) Inter-Domain Handovers

If the MN_2 moves between different local domains, inter-domain procedures of μHIP are invoked. Arriving at the new domain, MN receives a new local IP address and discovers information about the new LRVS ($LRVS_3$).After MN learns its new HIT and IP address from LRVS; it starts a new registration procedure. Since MN changed its LRVS, it needs to update its RVS and all CNs to keep on communication. But, first thing that it has to do is to update its old LRVS ($LRVS_2$) in order to forward its incoming packets to MN's old globally routable IP address until the end of update procedures in the first step. After the update of old LRVS, MN updates its RVS and finally its CNs. Then, RVS updates its record about the MN with its new global IP address. After finishing all updates, MN disconnect from it old LRVS or this connection is closed automatically after a timeout value.

3.2. Micro-HIP (mHIP)

mHIP [6] is designed as an extension of HIP in order to reduce the unnecessary signaling and control messages . It introduces new network components such as mHIP Agents. There are two types of mHIP agents. All mHIP enabled network components in mHIP network architecture are called mHIP agents. Their main role is during the intra-domain handovers. In mHIP, mHIP Gateway component acts similarly to LRVS in μHIP especially during initiation mechanisms. mHIP routers are able to handle the intra-domain handoff and so load of mHIP gateways and signaling load of handoff is reduced. Multi homing scenario is also included in mHIP whereas there are no explanations about multi homing in μHIP.

a) mHIP Agents

mHIP gateway serves as a root router and acts similar to LRVS in μHIP. mHIP gateway keep the records of MNs within a domain. MN registers to a mHIP gateway. When mHIP gateway receives data or signaling packets, it redirects these packets to the correspondent MN. *mHIP Router* mHIP routers redirect the HIP bases communication to the current location of MN. It also manages the intra-domain handover. With this role, they reduce the load of mHIP gateways and so handover latency is reduced.

b) Initiation

When a MN enters into a new domain, it needs to start an initiation mechanism to register to the mHIP gateway. MN gets the HIP and IP information from the ICMP announcement messages and starts registration procedure with mHIP gateway. mHIP gateway and MN exchange their information about the signatures used in the system. All mHIP agents in the same domain get the information about the MN's HIT and new IP address. Finally, MN registers to its RVS with its new HIT.

c) Intra-Domain Handovers

If there is no ongoing communication during MN's intra-domain handover, MN send an UPDATE packet to mHIP gateway to inform about its new IP address. The nearest mHIP which is located between the the old location of the MN (NmHIPA in the related study) and mHIP gateway captures the UPDATE packet and signs the packet with selected signature scheme. When MN receives and verifies the signed packet, intra-domain handover process is complete. The all mHIP agents learn the HIT and IP address of MN. The old location mHIP also notifies all neighbors to update the MN's record.

If there is an ongoing communication during MN'S handover, the MN sends an UPDATE packet to CN. NmHIPA captures this UPDATE message before CN and replies to it by signing the packet with the signature scheme of the domain. After MN replies to the address checking required by NmHIPA intra-domain handover procedure is complete. NmHIPA updates the mappings and notify the neighbors about the change of IP address of the MN.

3.3 Dynamic Hierarchical Host Identity Protocol (DH-HIP)

DH-HIP [7] is a location management scheme and introduces three levels architecture of rendezvous servers as Rendezvous Server (RVS), Gateway RVS (GRVS) and Local RVS (LRVS) respectively. The size of administrative domain managed by a LRVS is determined by the mobile node according to the packet arrival rate and mobility status after selection of LRVS. DH-HIP architecture network is divided into two types of domains: autonomous and administrative domains. While LRVS are responsible for managing administrative domains, GRVS are responsible for autonomous domains. Autonomous domains may consist of several administrative domains. GRVS is responsible for communication between LRVS and MNs during registration and connection initiation procedures of DH-HIP. In DH-HIP, size of administrative domains, which means the number of access routers managed by same LRVS, is set according to the packet arrival and mobility rate of MNs in order to minimize signaling cost. In DH-HIP scheme, all ARs inherit the roles of LRVS. When MN enters the network, it registers its HIT and IP address at LRVS, GRVS and RVS respectively. While MN registers at LRVS directly, during registration of GRVS and RVS, previous level rendezvous server intercepts the packets and replace the MN's IP address and HIT with themselves and forward them. If a CN wants to communicate with MN, after querying DNS; it obtains the IP address of RVS. The interception and forwarding of messages continue in some steps of Base Exchange too.

3.4. Early Update For Host Identity Protocol (eHIP)

eHIP [8] is a handover management protocol which also inherits the usage of LRVS as in μHIP. The main idea of

eHIP architecture is using the hierarchy of rendezvous servers in order to minimize HIP registration and update latency. eHIP architecture supports n level hierarch but in existing proposals three levels of rendezvous servers are investigated (The main RVS, H1 level and H2 level from now on). eHIP network architecture contains a main and global RVS in the networks and all sub level RVS are connected to it. The lower level RVS manages the sub domains which are called "hierarchy levels". The inner-most sub domain consists of the access points and the RVS managing them.

a) Initiation

When a mobile node enters a new domain, it basically registers with the H2 level RVS in a regular way. The registration of MN to upper levels is done via the trusted update establishment between RVS. A pre-registration procedure also exist in eHIP architecture that means, when a MN enters a new H1 domain, after upper level updates by H2 level RVS, H2 level RVS registers this MN in a passive mode to other H2 level rendezvous servers under the management of same H1 level rendezvous server.

b) Intra-Domain Handovers

The handovers inside a H2 domain of a mobile node do not affect the procedures of ongoing communication regarding the upper level rendezvous servers. Since MN is managed by same rendezvous servers in H1 and H2 level, the main handover management contribution of this proposal is about inter-domain handovers of a MN.

c) Inter-Domain Handovers

We can divide the types of inter-domain handovers of eHIP in two ways: H1 level and H2 level. When a mobile nodes changes it location between different H1 domains, which means it switches to a different H1 level RVS also. Early update procedure is triggered by router advertisement messages and first update message is sent through the MN's current RVS in order to start the process. When H2 level RVS realizes that new H2 level RVS invoked in early update message is in a different H1 level domain, an error type information message in sent to MN. After this message, MN starts a regular registration procedure with this new RVS since it is in a different H1 domain.

When a mobile node changes its location between different H2 level sub domains which are managed by same H1 level RVS, early update is triggered in the same way with router advertisement messages. If every condition is suitable, current H2 level RVS of MN starts the update process with new H2 level RVS on behalf of MN. When all these updates procedures finish between rendezvous servers and MN completely lose its connection from its old point of attachment, directly sends a finish update message to its new RVS. New RVs is responsible to update the upper levels and corresponding node about the MN. Finishing the update means for mobile node to continue its session and be able to send and receive new data in it s new location. Early update procedures bring the advantage of starting the handover update management for a mobile node before it loses the connection from current point of attachment and reduce the handover latency.

3.5. HIP Based Micro Mobility Optimization

Muslam et.al's study [9], a new network component called Co-Agent (Co-A) for each domain is proposed to extend the micro mobility behavior of HIP. LRVS is also inherited from μHIP. The main role of Co-A is managing mobile nodes during intra and inter domain handovers by acting as both a mobile and a corresponding node. LRVS of each domain is normally responsible for mapping local-global addresses of mobile nodes. The HI and IP of Co-A are also mapped with MN and the Co-A can receive local IP addresses from another domains for MNs which it manages. Owing to Co-A can monitor the movement of MNs; it can prevent the packet loss by informing the related entities in the network and optimize handover.

a) Initiation

When a MN enters a new domain, it registers itself to LRVS as usual. It does not need to register to RVS, but LRVS must be registered to DNS. In this approach, MNs ask for advertisement messages from access routers by sending Router Solicitation messages. Therefore, MN determines its Co-A and register itself and its Co-A to LRVS. After the LRVS's mapping procedures, a secure connection is established between Co-A of MN and Co-A and CN.

b) Intra-Domain Handovers

Access points periodically broadcast advertisement messages that contains HIT and IP of Co-A. If intra domain movement occurs, no operations are needed to do for MN, Co-A acts instead of MN. Since LRVS and MN exchange information about their registration in their domain.

c) Inter-Domain Handovers

When a MN changes its domain and inter domain handover occurs, it realizes this again by Router Advertisement Messages , then it registers itself to new LRVS through one of Co-A. MN's old Co-A inform the CN's LRVS via MN's old LRVS about its new location. After some other message exchange between Co-As, CN's LRVS forwards data to MN through its new LRVS.

3.6. An Extension of HIP for Next Generation Wireless Networks

This study proposes to optimize the handover process by informing the related entities about the access technology in next generation wireless networks [10]. The solution they propose is based on a scenario where both

communicating hosts are mobile. Their main aim is handling mobility of two mobile communicating nodes when they change their access technologies, namely when vertical handover occurs. The main concept of their proposal is introducing a new message for update procedure named as VHO_NOTIFY. This message informs the nodes about the technology that they will communicate next, in order to let the corresponding peer to know which interface to activate. This VHO_NOTIFY message also has a role for handover process that some parameters related to handover (IP addresses etc.) may be sent earlier to inform peers about handover. They also introduce a new type of UPDATE message named as NEW_UPDATE. The main difference between NEW_UPDATE and regular HIP UPDATE message is about the content of LOCATOR parameter. Unlike regular HIP, in NEW_UPDATE, LOCATOR parameter may not be the IP address of the owner of this message. Briefly, by allowing sending VHO_NOTIFY and NEW_UPDATE messages with old access technology, informing the corresponding peer about the next technology will be used. So, the necessary information about handover may be sent before handover starts.

3.6. Simultaneous End-Host Mobility Extension for HIP

This scheme's main idea is to enhance the role of RVS to support simultaneous mobility in HIP in which two communicating host change their locations at the same time [11]. As these simultaneous movements occur, both nodes inform their RVS about their new addresses.

The basic idea of this solution is relaying UE-PEER messages. This enhances the role of RVS. To avoid the loss of UE-PEER messages, they offer the interception of UE-PEER messages from MNs by RVS. But, second UE-PEER message exchange occurs since first attempts of RVS to relay the UE-PEER messages are done toward their old addresses. After timeout, UE-PEER message exchange is done. This second attempt is not done through RVS, besides third UE-PEER exchange is again intercepted by RVS. After this third data exchange, data flow starts.

3.7. HIP-PMIPv6 Based Localized Mobility Management for Multihomed Nodes

In this study, the authors propose a global and localized mobility management scheme based on the integration of HIP and Proxy Mobile IPv6 [12]. This scheme brings a solution for inter technology handovers and multi homing in PMIPv6.

The initiation procedure of HIP-PMIPv6 combination is mostly relies on the procedures of PMIPv6. The regular RVS update process of HIP follows the message exchanges and settings based on PMIPv6 in order to set up the trusted connection. In case of ongoing communications, regular HIP update procedures occur in order to update the corresponding nodes. Due to the type of IP addresses used by PMIPv6, LRVS idea cannot be inherited as in mHIP and μHIP. The macro mobility procedure is inherited from regular HIP whereas the micro mobility procedure is defined as a combination of HIP and PMIPv6.

a) Intra-Technology Handover

Since there is no change on locator of mobile node during movement, HIP does not sense the intra-technology handover. This procedure is completely based on PMIPv6. No updates to RVS and corresponding nodes (CNs) occur since the mobile node does not detect any change of its interface.

b) Inter-Technology Handover

Inter-technology handover means that a mobile node switches on to its second interface during an ongoing communication. If a MN switches on to its second interface, it again obtains the same Home Network Prefix if it is in the same domain. In this case, MN does not send an UPDATE to its RVS but sends to corresponding nodes to notify them about its new IP address of second interface. Mobile Access Gateway intercepts this UPDATE packet and does not forward it to CNs. It performs the necessary update operations on behalf of mobile node through other network elements.

3.8. Localized Mobility Management for HIP (L-HIP)

In L-HIP [13], a localized mobility management technique is presented by inheriting the idea of somehow proxy mobile IPv6. In their scheme, some entities in the network are responsible to track the mobile nodes' movements such as PMIPv6. They introduce a new entity called Local Mobility Management Server (LMMS) to cope with the intra-domain mobility especially. They also employ the usage of Mobile Access Gateways (MAGs) of PMIPv6 and present handover management scheme based on combination of PMIPv6 and HIP.

4. Conclusion

As new type of networks revealed and demand from networking and internet increased, the hosts did not remain in their fixed locations and became mobile. Due to these changes, handing the mobility became an important key issue for wireless and mobile networking. The most popular Mobile IP protocol and its extensions are the first and well-known studies related to the mobility concepts. IP addresses play a central role on mobility management methods such as identifying the nodes location and also acting as an identity number. As new needs and demands revealed, this role of IP addresses started to be insufficient and new locator-identifier splitting ideas have been introduced. Host Identity Protocol which we examined in this paper, is one of the use cases of this idea. Since it is and ongoing developing protocol, the studies on it about both mobility management and other concepts will continue in future. The idea of separation of the dual role of IP addresses is very important and a vital problem in today's internet

architecture. This study is related to the handover management feature of HIP, which still has shortcomings in original design.

5. Acknowledgment

This study is a part of PhD thesis entitled “Design of a New Mobility Management System for Next Generation Wireless Networks” at Istanbul University, Institute of Sciences. Telecom SudParis also support this study.

6. References

[1] R. Moskowitz, P. Nikander, P. Jokela, “Host Identity Protocol (HIP)”, RFC 5201.
[2] J. Laganier, T. Koponen, L. Eggert, “Host Identity Protocol (HIP) Registration Extension” RFC 5203
[3] J. Laganier, L. Eggert, “Host Identity Protocol (HIP) Rendezvous Extension”, RFC 5204
[4] P. Nikander, T. Henderson, Ed., C. Vogt, J. Arkko, “End-Host Mobility and Multihoming with the Host Identity Protocol”, RFC 5206
[5] L.Bokor, S.Novaczki, S. Imre, “A Complete HIP Based Framework for Secure Micromobility”, MoMM2007.
[6] J. Y. Hon So, J.Wang, “Micro-HIP : A HIP-based Micro-Mobility Solution”, Proceedings of ICC 2008 Workshop, Page(s): 430 - 435
[7] S. Yang , Y. Qin , D. Yang, “Dynamic Hierarchical Location Management Scheme for Host Identity Protocol”,Lecture Notes in Computer Science, Mobile Ad-Hoc and Sensor Networks, Springer Berlin / Heidelberg, Volume 4864/2007, Pages 185-196 as proceedings of MSN 2007, Beijing, China.
[8] Z. Gurkas Aydin, H. Chaouchi, A. H. Zaim, “eHIP : Early Update for Host Identity Protocol”,ACM Mobility Conference 2009, Article No.: 55, September, Nice,France.
[9] M.M.Muslam, H.Anthony Chan, N.Ventura, “HIP Based Micro-Mobility Management Optimization”, IWCMC 2009, Cannes-La Bocca, pages 291-295
[10] N.Toledo, M.V. Higuero, E.Jacob, J.Matias, “Extending the Host Identity Protocol for Next Generation Wireless Networks”, IFIP WOCN 2009, Cairo-Egypt
[11] F.Hobaya, V.Gay, E.Robert, “Host Identity Protocol Extension Supporting Simultaneous End-host Mobility”, IWCMC 2009, Cannes-La Bocca, pages 261-266
[12] Iapichino, G. Bonnet, C., “Host Identity Protocol and Proxy Mobile IPv6: A Secure Global and Localized Mobility Management Scheme for Multihomed Mobile Nodes”, GLOBECOM 2009, Honolulu
[13] B.Hu, T.Yuan, Z.Hu, S.Chen, “L-HIP : A Localized Mobility Management Extension for Host Identity Protocol”, WiCOM 2010, Chengdu