Muslam et al. EURASIP Journal on Wireless Communications and Networking (2017) 2017:71
DOI 10.1186/s13638-017-0853-z

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Distributed mobility management with mobile Host Identity Protocol proxy

Muhana M. Muslam[1*], H. Anthony Chan[2] and Neco Ventura[3]

Abstract

The architectural evolution from hierarchical to flatter networks creates new challenges such as single points of failure and bottlenecks, non-optimal routing paths, scalability problems, and long handover delays. The cellular networks have been hierarchical so that they are largely built on centralized functions based on which their handover mechanisms have been built. They need to be redesigned and/or carefully optimized. The mobility extension to Host Identity Protocol (HIP) proxy, mobile HIP Proxy (MHP), provides a seamless and secure handover for the Mobile Host in the hierarchical network. However, the MHP cannot ensure the same handover performance in flatter network because the MHP has also utilized the features offered by the hierarchical architecture. This paper extends the MHP to distributed mobile HIP proxy (DMHP). The performance evaluation of the DMHP in comparison to MHP and other similar mobility solutions demonstrates that DMHP does indeed perform well in the flatter networks. Moreover, the DMHP supports both efficient multi-homing and handover management for many mobile hosts at the same time to the same new point of attachment.

Keywords: Handover, Distributed mobility, Mobility management, Mobility proxy

1 Introduction

Cellular network is evolving from a hierarchical to a flatter architecture [1]. The nature of a hierarchical architecture can be harnessed to efficiently and seamlessly support host mobility. This is because it is possible to select/identify between a mobile host (MH) and correspondent host (CH) a functional entity, which can be updated on the MH's current location. Consequently, handover performance will be optimized since the selected entity is topologically closer than the CH to the MH. Unfortunately, that specific aspect of a hierarchical architecture's nature that allows the selection of a central entity for handover optimization is no longer available in a flat architecture where entities are distributed across different networks.

The architectural evolution from hierarchical to flatter networks to handle increased data traffic volumes creates new challenges as identified in [1]. These challenges include single points of failure and bottlenecks, non-optimal routing paths, scalability problems, and long handover delays. Consequently, the handover mechanisms such as [2–4] that have been built based on the centralized mobility function need to be redesigned and/or carefully optimized again.

To support mobility with both Host Identity Protocol (HIP) hosts and non-HIP hosts in hierarchical networks, HIP proxy and mobile HIP can be integrated into mobile HIP proxy (MHP). In [3], we had presented a preliminary design of the MHP which was able to support centralized mobility management only. It therefore still has all the drawbacks of centralized mobility management described in [1]. For the host mobility support in flat network architectures, an improved design of the MHP to take the role of mobility anchor will achieve distributed mobility. This paper introduces such a network-based and distributed mobility management. It distributes to the access networks such as mobility anchors based on an improved design of the MHPs to support the IP hosts in all these networks. The proposed distributed mobile HIP proxy (DMHP) enables host mobility in a flat network architecture and addresses problems of handover delay, scalability, single point of failure, packet loss, and signaling overhead. Further enhancement can be added to our proposal, DMHP, by

* Correspondence: muhana@ccis.imamu.edu.sa
[1]Department of Information Technology, Al-Imam Muhammad Ibn Saud Islamic University, Riyadh, Saudi Arabia
Full list of author information is available at the end of the article

(1) using an optimization model to provide useful theoretical insights and a protocol of distributed data query such as one presented in [5] and (2) using a distributed online algorithm that employs an optimal stopping theory to let nodes make adaptive, online decisions on whether this communication opportunity should be exploited to deliver data packets in each meeting event as explained in [6]. Although the method in [5] is developed to efficiently allow data query in a Mobile Ad hoc Social Network (MASON), many of its ideas can be employed by DMHP, i.e., designed for infrastructure networks without centralized host mobility support, that may lead to further improvement.

The main contributions in this paper are (1) introducing a network-based distributed mobility management solution for MHs in flat networks, (2) developing an architecture using the advantages of host identity protocol (HIP) for both HIP-enabled MH and non-HIP-enabled MH to support secured mobility and multi-homing, (3) developing mechanisms to enable our proposed solution, DMHP, to manage the handover of several MHs to the same new point of attachment (N-PoA), and (4) qualitatively and quantitatively investigating our proposed solution, DMHP, as well as some widely referenced distributed mobility solutions.

The rest of the paper is organized as follows: Section 2 reviews the related work. Section 3 presents the proposed solution while Section 4 presents the simulation results and performance analysis. Section 5 concludes the paper.

2 Related work

Many mobility solutions have employed the network-based approach to provide mobility support to hosts that lack mobility support capability. For example, Proxy MIPv6 (PMIPv6) [4] extends mobile IPv6 (MIPv6) [7] to provide network-based mobility support which is not implemented in the MH protocol stack. However, PMIPv6 relies on the dual role of IP addresses for host identity and locator, and it lacks scalable mobility support and required extensions to work in a flat network architecture.

Furthermore, in [8–10], authors extend PMIPv6 to provide network-based distributed IP mobility management solutions. However, these solutions need to communicate with some central or distributed entity to verify and validate the handed over mobile hosts, thereby incurring additional delay and signaling. In [10], authors have proposed a mobility solution, called multiple local mobility anchor (MLMA), in which authors used the PMIPv6 while employing a replicating strategy. Since MLMA supports the host mobility management in flatter networks, i.e., the same context our proposal is prepared for, further details about MLMA are presented and its handover procedures are shown in Fig. 1. As shown in this figure which explains the MH's handover procedure, the network consists of many access networks represented by access routers (AR), AR1 to ARn. MLMA has replicated the PMIP's local mobility anchor (LMA) into each of the ARs, AR1 to ARn, as well as the gateway router (GW).

In the MLMA, when the MH performs the handover from an access network through which the MH has established the active session, at AR1 collocated with LMA, to another access network, at AR2 which detects the attachment of the MH and sends an proxy binding update (PBU) packet to all ARs and GW in the network. When the ARs and the GW in the network receive the PBU, they all reply with proxy binding acknowledgment (PBA) packets, one packet from each. Therefore, MH data traffic routing is improved. However, the MLMA has the following shortcomings: (1) large buffer is needed in each AR collocated with LMA to maintain a record for each MH in the network in which host mobility is managed by MLMA; (2) additional time is needed to search the database of MH records involving maybe simple but rather large buffer, when MH performs a handover, on when to receive packets for each of the MHs in the network; (3) high signaling overhead for the new AR of MH to update all the other ARs and GW inside the network in which host mobility is managed by MLMA; and (4) MLMA does not have any mechanism that support management of handover of many MHs to the new AR.

We have presented in [3] a preliminary mobility management design of MHP. It provides seamless, secure handovers for both HIP-enabled and non-HIP-enabled mobile hosts without unnecessary signaling overheads to the hosts. However, it is only a centralized approach.

The papers [11, 12], and [13] have developed network-based distributed mobility solutions using ID/locator separation architecture. However, [11] and [12] is only concerned with network mobility, whereas [13] leverages neither network-based mobility support for host nor HIP proxy.

Although the PMIPv6 and MHP achieve a good handover performance in the hierarchical network architecture, there is a need for mobility solutions to respond to the challenges of evolving the network architecture from being hierarchical to being flat.

The preliminary design of MHP we reported in [3] combines mobility function with the HIP proxy function. Yet its mobility function is not serving as a mobility anchor but rather is equivalent to that of a mobile access gateway in PMIPv6. It relies on another centralized entity to serve as a mobility anchor to support mobility. MHP is therefore a centralized mobility management protocol with the drawbacks described in [1].

Distributed mobility management function is more general and more capable of serving the future mobile internet which continues to flatten. Compared to our

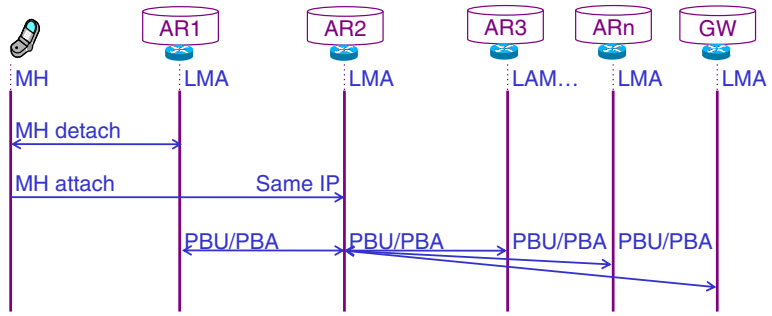

Fig. 1 MH handover procedures using MLMA

preliminary design, we have enriched the MHP function to act as a mobility anchor, which collocates at the access router. Distributed mobility management is then supported by these mobility anchors. There is no longer need to rely on a separate centralized entity, as in [3], which is now removed. The elimination of a centralized anchor also simplifies signaling.

3 Network-based distributed mobility management

This section introduces a network-based distributed mobility management solution that distributes the MHPs to the access networks to provide HIP and mobility support to all IP hosts. These mobility management functions of the MHP do not rely on any centralized mobility function such as the local mobility anchor in [2, 4] and the local rendezvous server in [3]. The MHPs are also included at the access routers taking advantage of the HIP proxy capability. They enable handover of mobile hosts in the flat network architecture with good performance. They enable an MH, whether or not HIP enabled, to use the same IP address as it changes its points of attachments within the flat network architecture. To support the distributed solution, MHPs provide the following functions: (1) each proxy serves as local mobility anchor for all connections established through it (proxy); (2) each proxy updates its neighbor proxies about the MHs that established their connections through it so the new proxy can determine the previous proxy from a distributed database; (3) a new proxy serves a mobile gateway and establishes channel between the previous and new proxies; and (4) a new proxy sends directly to CH the traffic for connections established through it and sends via previous proxies the traffic for connections established through other proxies.

3.1 Mobility management architecture

The architecture for network-based distributed mobility management with a mobile HIP proxy is shown in Fig. 2.

The rendezvous server (RVS) [14] with the DNS enables reachability of an HIP host by maintaining a mapping between the host identity, called HIT, and the IP address of the MH. This design, called distributed mobile HIP proxy, adds a set of co-located mobility and HIP proxy functions at the access router. Like the MHP

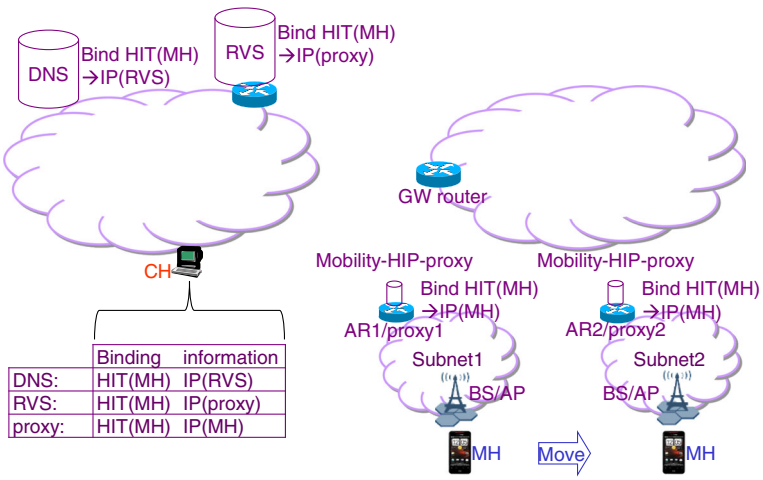

Fig. 2 Design of network-based distributed mobility management and HIP proxy

[3] for the hierarchical network architecture, the mobile HIP proxy performs HIP signaling on behalf of non-HIP MH so that HIP services can be offered to non-HIP enabled hosts. It also tracks the movement of the MH and updates the MH binding record if the MH is moving away from the network during an established session even when the session is active. The binding information, which is shown in a table in Fig. 2, is managed in the hierarchy DNS-RVS-proxy to enable reachability of an MH which is registered with the mobility-enabled HIP proxy.

3.2 Registration and reachability

Before using an HIP service, an HIP host needs to register with the service using the registration mechanism defined in [15]. The registration of an MH, which may either be HIP enabled or not, is illustrated in Fig. 3. This figure illustrates an example flow diagram of DMHP operations for the attachment of an HIP enabled MH and a non-HIP enabled MH.

Upon detection of a MH attachment, the MHP checks whether the MH is HIP enabled or not. If not, the MHP assigns a HIT and returns it to the MH. The MHP uses the HIT, from the HIP MH or the assigned one for non-HIP MH, to check whether the MH is registered or not. If it is not registered, the MHP sends an update message to the RVS, which is the intermediate server of location information between the MHP entities and the DNS servers.

After registration, the mobile HIP proxy contains the binding of the HIT of the MH, HIT (MH), to the IP address of the MH, IP (MH). The RVS contains the binding of the HIT of the MH, HIT (MH), to the IP address of the proxy, IP (proxy). The DNS contains the binding of the HIT of the MH, HIT (MH), to the IP address of the RVS, IP (RVS).

If the MH has more than one interface, it has to register the physical address for each of its interfaces with its host identity, HIT (MH). For example, if the MH has two interfaces and their physical addresses are PHYaddr1 and PHYaddr2, then MH registers its HIT (MH) with both its physical addresses, PHYaddr1(MH) and PHYaddr2(MH). This information will be registered at the MHP through which the MH is attached during the registration process. This information is also accessible from other MHPs to which the MH is possible to move/connect. Therefore, the MH uses its identity, HIT (MH), to find its record and thus be able to preserve its ongoing communication sessions even those established via other interface so as to support multi-homing.

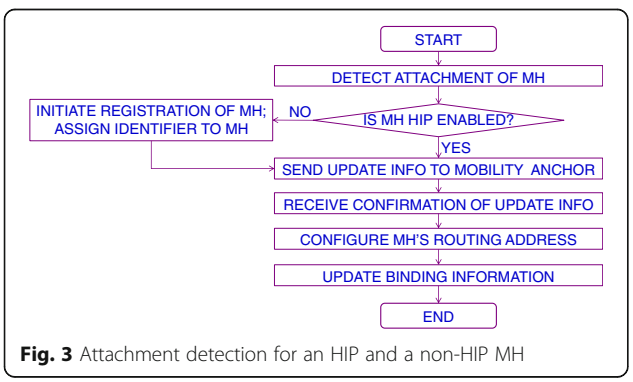

Fig. 3 Attachment detection for an HIP and a non-HIP MH

3.3 Establishing communication sessions

This distributed mobility management design enables data traffic between either an HIP-enabled MH or non-HIP-enabled MH and a CH. A Security Association (SA) is set up prior to the transport of data plane traffic. If the MH is an HIP host, the SA ends or terminates at the MH. If the MH is not an HIP host, the SA ends at the mobile HIP proxy to which the MH is registered.

Like the MHP, two pairs of initiation-response packets (I1, R1 and I2, R2) are exchanged to prepare for an SA establishment. Figure 4 illustrates an example flow diagram of MHP operations in establishing an HIP base exchange (HIPBE) between an HIP-enabled MH and an HIP-enabled CH. In addition, the figure illustrates an example flow diagram of MHP operations in establishing an HIPBE between a non-HIP enabled MH and an HIP enabled CH.

Upon receiving an I1 packet from the CH, the RVS checks if the destination HIT corresponds to that of a registered MH. If so, the I1 packet is forwarded to the registered IP address of the proxy. Upon receiving an I1 packet from the RVS, the mobile HIP proxy checks the destination HIT in the HIP header. If the destination HIT corresponds to that of a registered HIP-enabled MH, the mobile HIP proxy (proxy1) forwards the I1 packet to the MH. The mobile HIP proxy does not store any binding in the case of the HIP MH. The MH will store the binding HIT (CH):IP (CH), and the MH will send the reply R1.

If the destination HIT corresponds to that of a registered MH which is not HIP enabled, the mobile HIP proxy (proxy2) stores the binding HIT (CH):IP (CH). The mobile HIP proxy (proxy2) will send the reply R1 on behalf of the MH.

After the successful exchange of the two initiation-response packet pairs, an HIP SA will be established between the initiator and responder. In data traffic, the HIP proxy (proxy2) uses the HIP SA and ESP to encapsulate/decapsulate non-HIP MH data packets, whereas the HIP MH uses its HIP SA and ESP to process its data. Figure 5 shows how the HIP SA is used based on the traffic type, HIP or IP traffic. In addition, it illustrates an example flow diagram of MHP operations as a MHP receives a packet for and from a MH.

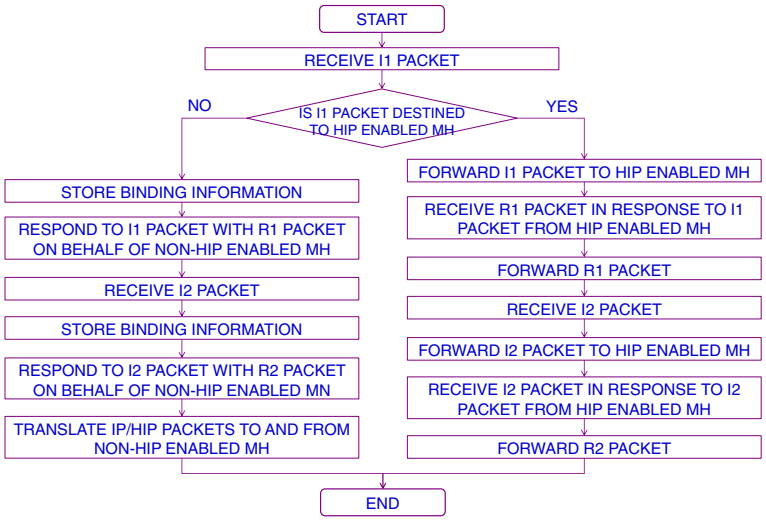

Fig. 4 HIP SA establishment detection for an HIP and a non-HIP MH

When the MHP receives HIP packets destined for one of its MHs, it checks first whether the packets are sent for an HIP or non-HIP MH. When the MHP receives packets from a non-HIP, the MHP determines first whether packets need HIP services or not. To achieve this, there are two solutions: (1) enable the network-layer of the MHP to pass the received packets to the HIP layer. The HIP identifies the IP flow to which the received packets belong and accordingly offer HIP services if needed; and (2) add a flag, for example, an HIP flag to the packets of a flow that requires HIP services. The MHP then offers the HIP services if the HIP flag is set to 1.

The re-use of the established HIPSA allows the MH to avoid some delay and signals and thus enable the seamless IP handover in a secure way. In addition, the proposed DMHP ensures another way to at least obtain some of the necessary security information from the local server, while the full authentication is being performed at the original servers as explained in the HIP RFCs. In this case, at the server, for example, as responder in a remote network location, the average of the end-to-end delay for the inter-domain will be about 110 ms [16] that can lead to a long handover delay.

3.4 Handover

Figure 6 shows the handover procedure of a MH, which is either HIP MH or non-HIP-enabled MH, between two wireless access networks belonging to the domain managed by the same GW. The MH is communicating with an HIP-enabled CH (not included in the figure) which lies in a different domain.

The MH may change its point of attachment (PoA) and attach to another mobile HIP proxy (proxy2) under the same GW. During this attachment, the MH presents its HIT and previous IP address to proxy2. Proxy2 then determines the previous proxy, proxy1, from the network prefix of the MH's previous IP and then acts as the HIP proxy and updates the binding record of the MH at

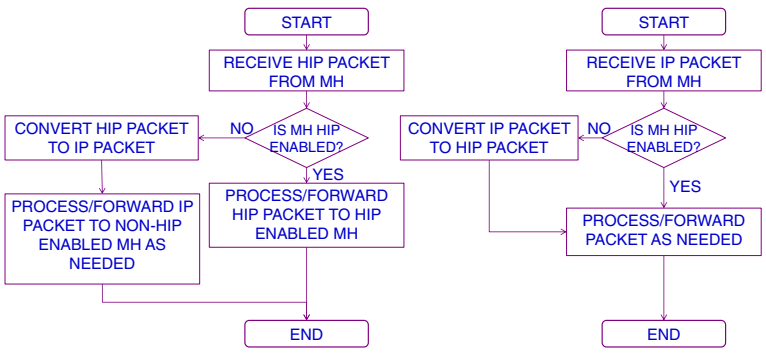

Fig. 5 HIP SA for data processing, encapsulation, and decapsulation

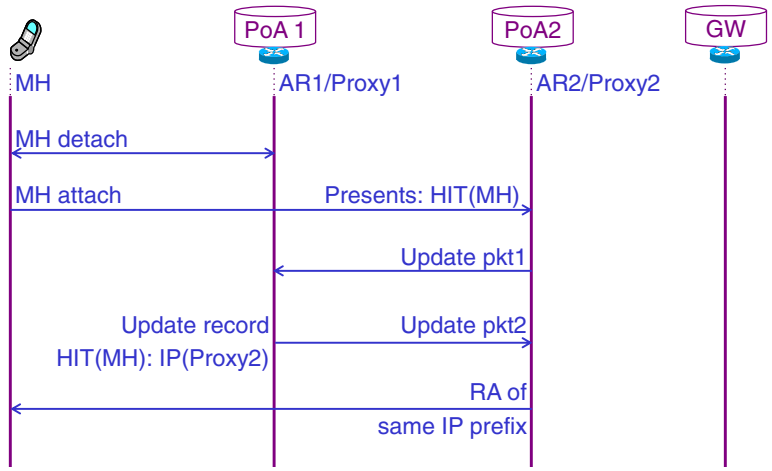

Fig. 6 Packet flow after MH handover within the IPn domain

proxy1. Communicating with proxy1 allows proxy2 to securely know the context of the established HIP SA.

Note that in a secure private network, for non-HIP MH, HIP communications can be terminated at proxy1 and then exchanged with a MH as IP communications via proxy2. That is, proxy1 performs HIP proxy functions while proxy2 performs mobility support. The advantages of this approach are the following: (1) non-HIP MH can move to any mobility-enabled access router and still preserve its active sessions with HIP CHs and (2) it allows load balancing, for example, if the proxy is heavily loaded, it can assign some of the load to other HIP proxies. However, this approach can result in inefficient routing if the distance between proxy1 and proxy2 is large while the distance between the GW and proxy2 is small. In the DMHP, all HIP communications are handled in the new proxy, proxy2. Furthermore, the DMHP can ensure efficient routing and reduces vulnerability between the MH and the proxy.

When the MH performs the handover from a network through which the MH has established the active session, proxy2 detects the attachment of the MH and sends an UPDATE packet (packet1) to proxy1. When proxy2 receives the reply UPDATE packet (packet2) from proxy1, it will send a RA to the MH. The RA will have the same network prefix that the MH used to configure its IP address in the proxy1 subnet. The MH, therefore, retains the same IP address configuration so that duplicate address detection (DAD) is not needed. This procedure significantly reduces handover latency, signaling overheads and packet loss.

Figure 7 shows exchanged messages between entities in a wireless communications system as a non-HIP-enabled MH performs a handover from one access network to another, through which the active session is established.

When the MH returns to the proxy, through which the active session is established, the proxy checks its cache binding to identify the MH and where its active sessions are established. If the sessions were established via the new proxy, the latter updates the record of the MH and starts serving it instead of forwarding to

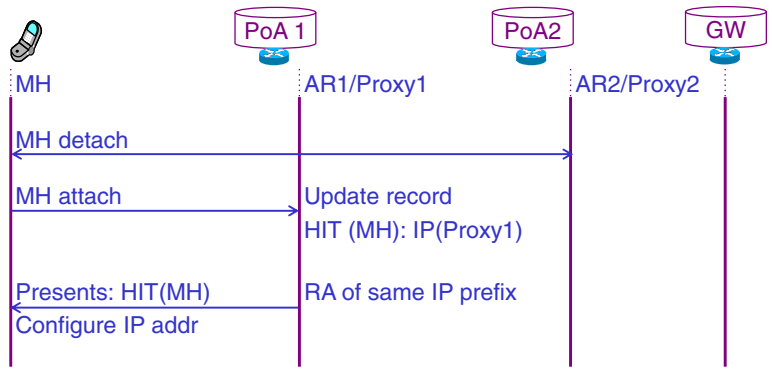

Fig. 7 Handover procedure of a MH using DMHP

another proxy. It is important to note that the proxy does not send any handover-related signaling, and thus, the location update delay is eliminated. Furthermore, there is no need to update the MH record at the RVS since the MH is still reachable via the registered proxy at the RVSs. Unlike [8–10], the DMHP does not incur additional handover delay due to verification and validation of handed over MHs. And also unlike [12], the DMHP does not incur additional handover delay due to configuration of new IP address in the same domain and thus DAD delay.

So far, we have discussed the handover of a single MH. Suppose, however, that two or more MHs need to handover to the same new point of attachment, N-PoA. An example scenario is when a train carrying many passengers moves from one network to another. Therefore, if two or more mobile hosts have moved at the same time to the N-PoA, how does the N-PoA handle these MHs? And in which order?

The movement of many mobile hosts at the same time to the same new point of attachment, N-PoA, is one that can affect the handover latency, packet loss, and handover-related messages. Either the newly attached MHs can detach from different PoAs (that is where some MHs are coming from different PoAs) or all MHs detached from the same PoA. The former case is referred to as case 1 and the other as case 2. Such concurrent movement (handover) of MHs may result in long handover latency and packet loss as well as more handover messages, however. In this paper, we discuss various methods to ensure the efficient management of many MHs that move at the same time to the same new PoA, so that handover performance is maintained. To the best of our knowledge, none of the existing host mobility solutions have addressed the abovementioned issue.

In Fig. 8, we show case 1 with two MHs, MH1 and MH2, coming from different points of attachment, PoA1 and PoA2, and attaching to the same new point of attachment, N-PoA.

Furthermore, in Fig. 9, we show case 2 with three MHs, MH1, MH2, and MH3, coming from the same points of attachment, PoA1, and attaching to the same new point of attachment, N-PoA.

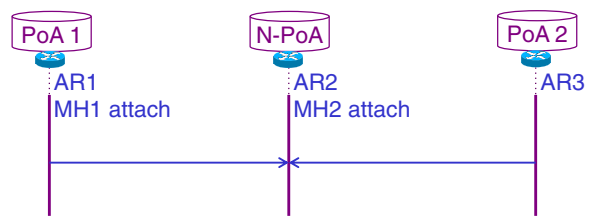

Fig. 8 Many MHs attach at the same time to the same N-PoA but coming from different PoAs using DMHP

Fig. 9 Many MHs attach at the same time to the same new PoA using DMHP

In case 1, if many MHs coming from different PoAs have moved to the same N-PoA, the N-PoA must first classify the MHs into different groups based on their old PoAs. The N-PoA sends only one update packet, which we called a group UPDATE packet and denoted by GUPDATE packet, for each group and not for each MH. An example that explains this scenario is shown in Fig. 10. As depicted in the figure, the N-PoA has classified the MHs, the nine MHs, into three groups because the attached MHs are coming from three different PoAs, PoA1, PoA2, and PoA3. Let us name these groups as group1, group2, and group3. Group1 includes two MHs (MH1 and MH2), group2 includes three MHs (MH3, MH4, and MH5), and group3 includes four MHs (MH6, MH7, MH8, and MH9). It is important to note that the number of MHs will equal the number of groups if each MH is coming from a different PoA, which is the worst case.

In case 2, if at the same approximate time many MHs have moved (handover) to the same N-PoA, the N-PoA builds an aggregated mobility packet that we denoted by AgUPDATE pkt1 and then sends it to the old PoA from which the MHs detached. The aggregated UPDATE packet includes the identifiers for all MHs attached to the N-PoA. Sending of only one packet (an aggregated UPDATE packet) will reduce the signaling overhead and

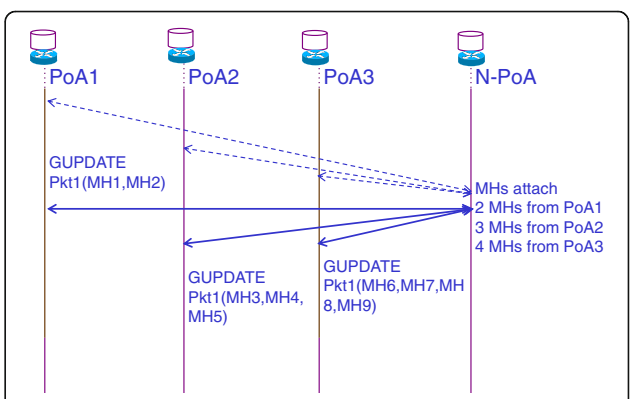

Fig. 10 Handover procedure of many MHs at the same time from different PoAs to the same new PoA using DMHP

Table 1 Simulation parameters under which MHP and DMHP are examined

Parameter	Value	Parameter	Value	Parameter	Value
Speed	1 m/s	Mobility model	Rectangle	Route advertise interval	≥0.3 s
No. of POA	2	Packet flow	Bi-dir CBR		≤0.7 s
No. of MH	1	UDP packet transmit rate	0.13 s	AP power	2.0 mW
Grid size (m^2)	850 × 850	Packet size	256 B	Beacon freq.	0.1 s

location update latency as well as the packet loss. That is because only one update packet will be sent to update locations of many MHs instead of sending a separate update packet for each MH.

Consider a movement of n MHs $\{MH_0, MH_1,..., MH_{n-1}\}$ in case 1. After that, the N-PoA will send three UPDATE packets, GUPDATE packets, instead of nine UPDATE packets. One of the three UPDATE packets (that include the identifiers of MH1 and MH2) will be sent to the PoA1. One of the remaining two UPDATE packets (one that includes the identifiers of MH3, MH4, and MH5) will be sent to the PoA2. The last one of the remaining two UPDATE packets (one that includes the identifiers of MH6, MH7, MH8, and MH9) will be sent to the PoA3. On the reception of each of these UPDATE packets, an acknowledge packet that we called GUPDATE packet2 will be sent to the N-PoA. Specifically, one acknowledgement packet will be sent from each of the PoAs, PoA1, PoA2, and PoA3.

When handover of many mobile hosts to the same N-PoA occurs (case 2), the N-PoA must respond to and service it as quickly as possible. It is inefficient for the N-PoA to send a separate update packet for each MH. The principal reasons for this are as follows: (1) numerous MHs can come from the same old PoA as in the scenario of a train. Thus, it makes sense to only send one update packet for MHs' location update. (2) A mechanism is needed to manage the sharing of the bandwidth and other resources by multiple MHs handover at the same time and coming (detached) from different old PoA.

The N-PoA includes multiple MH identifiers on a single update packet. Such a method we termed multi-update. It can be more efficient than multiple update packets for each single MH because multi-update communication is faster than multiple update packets communication. In addition, one multi-update uses significantly less signals than multiple update packets.

4 Simulation and results

4.1 Simulation setup

The OMNeT++ v.4 [17], which is an open source network simulator, is used to model the functionality of DMHP.

The simulation environment under which the authors examined the DMHP constitutes two IEEE 802.11b subnetworks with MHPs co-located within the access routers. The two subnetworks partially overlap. A fixed HIP CH (i.e., hipsrv) is placed outside the access network of the MH and runs a UDP application to transmit a data stream at 15 Kbps with a packet size of 256 bytes to the MH. It is important to note that these application settings are chosen to represent configuration of the voice IP application. Although TCP applications are popular, we only check the performance of DMHP for UPD applications because these applications are delay-sensitive. The simulation runs for 25,000 s while the MH speed is fixed at 1 m/s as it moves from subnet 1 that is managed by MHP1 to subnet 2 that is managed by MHP2 and vice versa. The simulation parameters of this scenario are described in Table 1.

This section presents and analyzes the handover performance results obtained from the MHP and DMHP. The handover delays, packet loss, and signaling overheads are investigated. Also investigated are other factors that affect MH handover performance such as the number of MHs simultaneously performing handover while communicating with different CHs. In addition, end-to-end delays before and after the MH handover are investigated.

Using the abovementioned simulation, the authors examined the model (DMHP). In addition, they recoded and analyzed a hundred handovers for the DMHP. The fluctuation in the handover latency (HOL) of the DMHP and MHP over the first 23 handover (HO) instances is depicted in Fig. 11.

It is important to note that experiment of MHP is conducted in the hierarchical networks whereas experiment of DMHP is conducted in the flat networks. It is observed that the DMHP exhibits varying handover

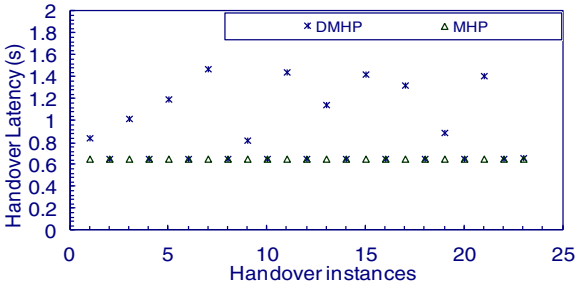

Fig. 11 The first 23 handovers for DMHP and MHP

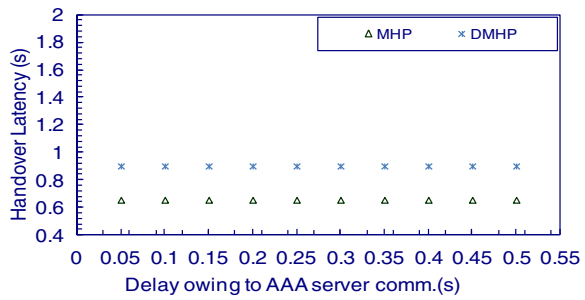

Fig. 12 Impact of AAA server delay on Handover delay of the DMHP and MHP

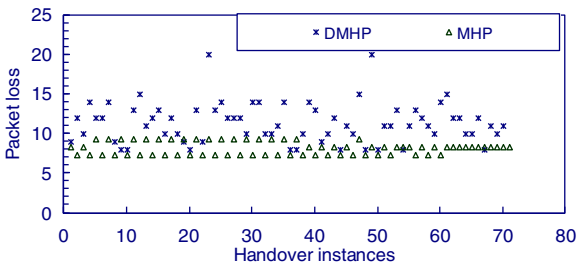

Fig. 14 The first 70 packet loss for DMHP and MHP

latencies, which vary between 0.6 and 1.8 s in the handover from a visited network to the home network and from the home to a visited network, respectively. This is because the DMHP communicates with the PoA of the session, that is, the PoA in the home position when the MH moves from the home to a visited network, to redirect the data traffic via the new PoA, that is, the PoA in the visited network. It is also evident from the measurements presented in the figure, in the IP handover towards the PoA of the session, that the handover delay due to location updates has been completely eliminated. This is because in the DMHP, when returning to the PoA of the session, the MHP stops forwarding the data traffic and thus serves as an authoritative MHP. These services are provided for both HIP and non-HIP MHs.

With respect to the handover of many MHs at the same time, the handover latency depends on the number of MHs and number of old PoAs for those MHs. These different situations are explained above and referred to as case 1 (MHs come from different old PoAs) and case 2 (all MHs come from the same old PoA). In case 1, time needed to complete the handover of many MHs can be described by the following equations.

$$L_{\text{ly3HO}} = L_{\text{Loc}_{\text{update}}}(Gn) + L_{\text{IP addr. config.}} \quad (1)$$

$$L_{\text{loc}_{\text{update}}}(Gn) = L_{\text{gupdate pkt1}} + L_{\text{gupdate pkt2}} \quad (2)$$

Where L_{ly3HO}, Gn, ly3HO, $L_{\text{Loc\_update}}$, $L_{\text{IP addr. config}}$, $L_{\text{gupdate pkt1}}$, and $L_{\text{gupdate pkt2}}$ denote the total latency of MH's handover at layer 3 and the group number and thus determine the old PoA for each of MHs, latency of location update, latency of IP address configuration, latency of the first update packet sent from the new PoA to any of old PoA from which one or many MHs detached, and latency of the reply update packet from each of the old PoA to the new PoA, respectively. For simplicity, let us assume that times (latencies) needed to update each of old PoAs are equal. With this assumption, all the old PoAs of MHs will be updated approximately during the same time. Therefore, the location update latency, $\text{latency}_{\text{Loc update}}(Gn)$, of DMHP is similar to the location update latency required to mange handover of only one MH.

In case 2, the time needed to complete the location update of many MHs, coming from the same old PoA and moving to the same N-PoA, using DMHP is similar to the location update latency required to manage handover of only one MH.

Figure 12 illustrates the relationship between the delays owing to the security process with a third party, for example, an Authentication, Authorization, and Accounting (AAA) server, and the handover delay of the DMHP and MHP. Every point on the graph represents an average of the MH handovers, layer-2 and layer-3 handovers, measured while the MH was moving with a speed of 1 mps. Like the MHP, the DMHP is not affected by a third party security delay since the security checks are not performed at the third party and thus avoids additional delay. The main advantage is that DMHP achieved this in the flat networks while MHP achieved that in the hierarchical networks.

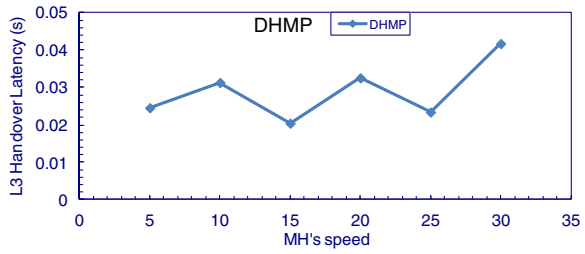

Fig. 13 Impact of MH speeds on the handover delay for the DMHP

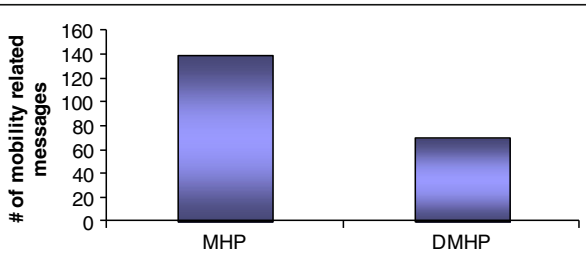

Fig. 15 Handover-related messages of the MHP and DMHP

Table 2 Signaling overheads of PMIPv6-based distributed mobility, MHP, MLMA, and DMHP

Parameters\scheme	PMIPv6-based DM	MHPP	MLMA	DMHP
No. of UPDATE packets per IP handover when MH has ongoing communications with 1 CH	6	2	2(*r*)	2 (for home_to_visted handover only)
Are there any signalling overheads on MH's interface?	No	No	No	No
Are there any signalling overheads due to configuration of new IP address?	No	No	No	No
Are there any signalling overheads due to contact with centralised mobility entity?	Yes	Yes	No	No
Are there any signalling overheads due to contact with centralised security entity?	Yes	Yes	Yes	No

Figure 13 shows how different MH speeds affect the handover delay of the DMHP. Each point in the graph represents an average of all the MH handovers, from the home network to the one, the MH moves away from the PoA of the active sessions, and vice versa, made within 2,000 s for each different MH speed. For example, the number of HOs the MH has performed with a speed of 5 mps is five times the number of handovers the MH has performed with a speed of 1 mps. Here, we considered the average of all the MH handovers for each different speed. In handover delay, the measurements with different MH speeds are interesting in that the HO delay for MH speeds of 15mps is lower than the handover delay for MH speeds of 10mps. The figure depicts the impact of the different MH speeds on the location update delay (layer 3 handover) for the DMHP when the MH moves from home to a visited network, in which MH moves away from the PoA of the active sessions. As shown in the figure, the impact of the MH speeds on the handover delay for the DMHP when MH moves from a visited to the home network, in which the MH moves to the PoA of the active sessions, is negligible. This is because when the MH is detected at the PoA of the active sessions, it just stops forwarding the traffic of the MH via another PoA. In other words, when the MH moves to the PoA of the active sessions, the DMHP is less affected.

Figure 14 depicts the packet loss of the DMHP and MHP. The authors measured the loss of data packets of a UDP application in the unidirectional traffic going from the CH to the MH during IP handover. It is important to note that in these measurements, there is no buffering or forwarding technique used to mitigate the packet loss, i.e., number of packet losses. Like the handover delay, packet loss in DMHP is small when MHs move towards the PoA of the session while packet loss is high when the MH moves away from it. To mitigate the packet loss of DMHP to the same level of MHP or even further, a buffer at the previous point of attachment can be used while the DMHP offers host mobility support in an architecture (flat) in which the MHP cannot be used.

Handover-related messages in the DMHP and MHP are portrayed in Fig. 15. In the DMHP during 25,000 s simulation time, the MH performed 70 handovers. Thus, Fig. 10 depicts the handover-related messages for the MHP and DMHP over the first 70 handovers. It is evident from the figure that the DMHP has outperformed the MHP in the handover-related signaling since the DMHP does not use any handover-related messages when the MH moves to the PoA of the session. It is important to note that a case where the MH performs a handover during active sessions established through different PoAs is not present in the said figure.

Furthermore, signaling overheads of PMIPv6-based distributed mobility management solutions [8, 9], HIPP-MIP [2], MHP [3], MLMA [10], and DMHP are described in Table 2. The first row in Table 2 indicates the number of binding update messages when the MH has ongoing communication sessions with one CH. In fact for DMHP, the number of binding update messages when the MH has ongoing sessions with n CHs is the same as a case where the MH has a session with one CH. Thus, the mobility related signaling overheads of the DMHP is not affected by the increasing number of CHs with which the MH has ongoing communication sessions. This is because the DMHP updates only the PoA through which the active sessions are established and not the CHs. Furthermore, unlike distributed mobility solutions in [8–10], the DMHP does not require a consultation with any third party on security aspects as it has capabilities of self-certifying at the HIP layer. Moreover, DMHP avoids all signals related to DAD and signal overheads on the HIP MH interface. In MLMA [10], the number of required mobility signals per one MH handover is described by an equation, $2*(r)$, where "r" indicates

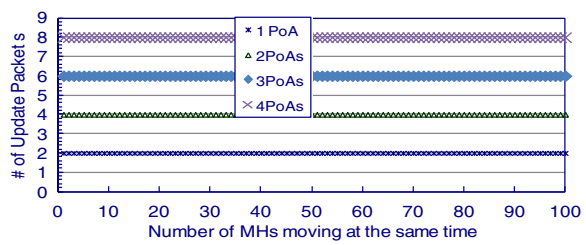

Fig. 16 Signaling overhead for many MHs attach at the same time to the same N-PoA but coming from different PoAs using DMHP

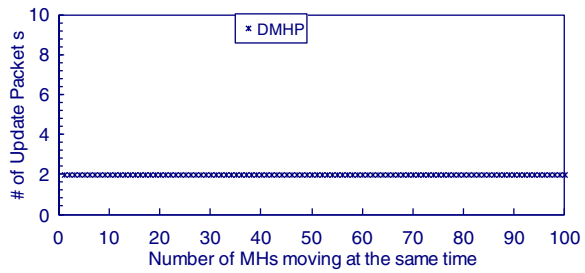

Fig. 17 Signaling overhead of DMHP for managing handover of many MHs at the same time to the same N-PoA but all coming from the same PoA using DMHP

the number of the ARs plus one GW in the network in which the MLMA is used as host mobility solution.

With respect to the handover of many MHs at the same time, the signaling overhead will also be affected by the number MHs, number of old PoAs for MHs, mechanism employed to manage handover of many MHs. Signaling overhead of DMHP used for case 1 (MHs come from different old PoAs) is shown in Fig. 16 while signaling overhead of DMHP used for case 2 (all MHs come from the same old PoA) is shown in Fig. 17.

Figure 16 shows the relationship between the number of mobile hosts (MHs) and the number of update packets needed for handover management of many MHs performed at the same time. As depicted by the figure, the number of update messages is increased if the number of old PoA from which MHs come is increased. But the number of update messages is not affected by the number of MHs coming from each of the old PoA. This is because the DMHP classify MHs into different groups based on the old PoA for each MH. Thus, the N-PoA exchanges only two update packets with the appropriate old PoA for each group irrespective of the number of MHs inside each group. For example, if all MHs come from two PoAs then only four update messages (packets) are needed, two packets for each group.

As shown in the Fig. 17, only two update packets are required for handover management of many MHs coming from the same PoA and attaching to the same N-PoA.

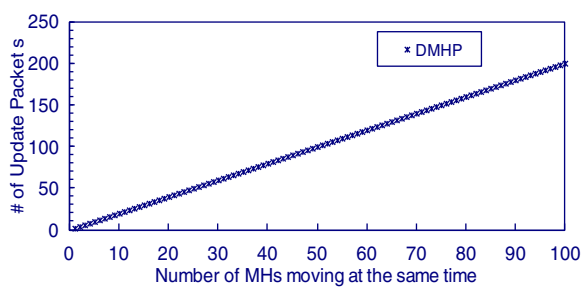

Fig. 18 Signaling overhead of DMHP for handover management of many MHs attach at the same time to the same N-PoA but each coming from different PoA

Figure 18 shows the number of update messages (packets) needed by the DMHP for handover management of many MHs attaching at the same time to the same N-PoA but each of the MH coming from the different PoA. That is the worst case where the number of groups equals the number of the MHs.

5 Conclusions

The DMHP distributes MHPs introduced by the MHP and equips them with additional functions to produce a powerful mobility management solution suitable for a flat network architecture. Thus, the DMHP reduces the air signaling overheads, maintains a stable MH locator even when the MH changes MHPs, and reduces unnecessary signaling overheads over the core network through which established sessions are communicated. Furthermore, the DMHP makes the IP handover in flat architecture transparent to the upper layer protocols and thus securely preserves the active sessions. Consequently, IP handover with good performance is achieved in flat networks without relying on any centralized mobility entity. The network-based aspect of the DMHP locally manages handover-related packets and packet routing before and after the handover, thus ensuring efficient routing. The HIP aspect, on the other hand, mainly provides its security capabilities and multi-homing insured by the HIP secure and permanent host identifier.

In DMHP, distributed entities that provide both mobility management and HIP features by the network to all IP hosts are introduced to achieve the MH IP handover with good performance in the flat network architecture. This distributed mobility solution provides a framework, for the flat network architecture, that supports a seamless vertical handover in a secure manner. The DMHP utilizes the benefits of the MHP to achieve its goal. Furthermore, DMHP employs efficient mechanisms to manage handover of many MHs to the same N-PoA either MHs come from different old PoAs or the same old PoA. The performance evaluation of the DMHP in comparison to MHP demonstrates that it does indeed perform well in flat networks with similar handover performance achieved by optimized mobility solutions developed for hierarchical networks.

Acknowledgements

This work is supported in part by Telkom, Nokia Siemens Networks, TeleSciences, and National Research Foundation, South Africa, under the Broadband Center of Excellence program.

Authors' contributions

This work is an extension of the PhD thesis research of MMM, who had designed the proposed protocol and performed simulation and analyses. HAC and NV had participated with technical discussions to provide guidance on the thesis work and the extensions. All authors read and approved the final manuscript.

Competing interests
The authors declare that they have no competing interests.

Publisher's Note

Author details
[1]Department of Information Technology, Al-Imam Muhammad Ibn Saud Islamic University, Riyadh, Saudi Arabia. [2]Huawei Technologies, Plano, Texas, USA. [3]Department of Electrical Engineering, University of Cape Town, Rondebosch, South Africa.

Received: 7 October 2016 Accepted: 30 March 2017
Published online: 18 April 2017

References

1. HA Chan et al., *Requirements of Distributed Mobility Management*, 2014. Internet Engineering Task Force (IETF) RFC 7333
2. M Muslam, HA Chan, N Ventura, LA Magagula, *Hybrid HIP and PMIPv6 (HIPPMIP) Mobility Management for Handover Performance Optimization* (in 6th International Conf. of Wireless and Mobile Communications (ICWMC), Valencia, 2010), pp. 232–237
3. MM Muslam, HA Chan, LA Magagula, N Ventura, *Network-Based Mobility and Host Identity Protocol* (IEEE Wireless Communications and Networking Conference (WCNC), Paris, 2012), pp. 2395–2400
4. S Gundavelli, K Leung, V Devarapalli, K Chowdhury, B Patil, *Proxy Mobile IPv6*, 2008. IETF RFC 5213
5. Y Liu, Y Han, Z Yang, H Wu, Efficient data query in intermittently-connected mobile ad hoc social networks. IEEE Trans. Parallel Distrib. Syst. **26**(5), 1301–1312 (2015)
6. L Yang, AMA Elman Bashar, L Fan, W Yu, L Kun, *Multi-Copy Data Dissemination with Probabilistic Delay Constraint in Mobile Opportunistic Device-to-Device Networks*, 2016, pp. 1–9. World of Wireless Mobile and Multimedia Networks (WoWMoM) 2016 IEEE 17th International Symposium on A
7. C Perkins, D Johnson, J Arkko, *Mobility Support in IPv6*, 2011. IETF RFC 6275
8. F Giust, CJ Bernardos, A De La Oliva, Analytic evaluation and experimental validation of a network-based IPv6 distributed mobility management solution. IEEE Trans. Mob. Comput. **13**(11), 2484–2497 (2014)
9. K Xie, J Lin, L Wu, *Design and Implementation of Flow Mobility Based on D-PMIPv6* (IEEE 17th International Conference on Computational Science and Engineering (CSE), Chengdu, 2014), pp. 1344–1349
10. T Condeixa, S Sargento, Centralized, distributed or replicated IP mobility? IEEE Commun. Lett. **18**(2), 376–379 (2014)
11. Y Kim, H Ko, S Pack, *Network Mobility Support in Distributed ID/Locator Separation Architectures*, 2014, pp. 521–522. IEEE 11th Consumer Communications and Networking Conference (CCNC)
12. VP Kafle, Y Fukushima, H Harai, *New Mobility Paradigm with ID/Locator Split in the Future Internet*, 2014, pp. 163–169. IEEE 11th Consumer Communications and Networking Conference (CCNC)
13. S-I Choi, S-J Koh, *Distributed Mobility Control Schemes in the HIP-Based Mobile Networks*, 2014, pp. 269–275. 16th International Conference on Advanced Communication Technology (ICACT)
14. J Laganier, L Eggert, *Host Identity Protocol (HIP) Rendezvous Extension*, 2008. RFC 5204
15. J Laganier, T Koponen, L Eggert, *Host Identity Protocol (HIP) Registration Extension*, 2008. RFC 5203
16. C Bovy, H Mertodimedjo, G Hooghiemstra, H Uijterwaal, P Van Mieghem, *Analysis of End-to-End Delay Measurements in Internet*, 2002. in Proc. of the Passive and Active Measurement Workshop-PAM'2002
17. OMNet++ open source network simulator. Official website: http://www.omnetpp.org. Accessed 30 Sept 2016