

RESEARCH

Open Access

Inter-subnet localized mobility support for host identity protocol

Muhana Muslam*, H Anthony Chan and Neco Ventura

Abstract

Host identity protocol (HIP) has security support to enable secured mobility and multihoming, both of which are essential for future Internet applications. Compared to end host mobility and multihoming with HIP, existing HIP-based micro-mobility solutions have optimized handover performance by reducing location update delay. However, all these mobility solutions are client-based mobility solutions. We observe that another fundamental issue with end host mobility and multihoming extension for HIP and HIP-based micro-mobility solutions is that handover delay can be excessive unless the support for network-based micro-mobility is strengthened. In this study, we co-locate a new functional entity, subnet-rendezvous server, at the access routers to provide mobility to HIP host. We present the architectural elements of the framework and show through discussion and simulation results that our proposed scheme has achieved negligible handover latency and little packet loss.

Keywords: HIP, mobility, micro-mobility

1. Introduction

Host mobility support is one of the key features of the next generation network which is the All-IP-based heterogeneous networks [1]. The duality problem of IP addresses [2] in simultaneously serving as both host identifier and locator in the Internet is the major issue that makes host mobility support challenging.

During a communication session, a mobile node (MN) may move within a single domain (micro-mobility) or move to a different domain (macro-mobility) [3]. These two main scenarios can be managed at different layers of the conventional TCP/IP stack [4]. Access technologies can manage intra-link mobility (L2 handoff) and may assist one to trigger L3 handoff. The IP layer solutions are most common, especially in a heterogeneous network environment. Mobile IP (MIP) [5], which is one of the IP layer solutions, extends the ability of the Internet to support the host mobility, but has security threats such as Denial of Service attack (DoS) [6].

Host identity protocol (HIP) is developed by Internet Engineering Task Force (IETF) to provide secured mobility support in a simpler manner than the other proposed solutions [6] and the popular MIP [7,8].

Mobility extension for HIP allows HIP-enabled mobile host to move with negligible handover latency (HOL) in environment where the global mobility management is acceptable but introduces long HOL and unnecessary control messages in a micro-mobility environment [9]. Such long HOL not only increases packet loss and delay but also decreases the performance of the upper layer application, particularly the real-time application such as Voice over IP. Therefore, there is the need to develop an adequate and efficient solution to reduce HOL as well as mobility-related signaling of HIP in micro-mobility environment while retaining the same level of security of HIP. The proposed solution should support mobility to allow the mobile users access their services wherever they go in a secure and efficient manner. Some issues where localized mobility management is needed have been discussed in [10].

The proposed contributions in this article are (1) introducing of network-based mobility management using HIP technology, (2) development of an architecture that can be easily extended to offer HIP service for non-HIP-enabled MN, and (3) qualitative and quantitative investigations for HIP and some widely referenced HIP-based micro-mobility solutions as well as our proposed solution.

* Correspondence: muslam@crg.ee.uct.ac.za

Department of Electrical Engineering, University of Cape Town, Rondebosch, South Africa

This article describes HIP (Section 2) and discusses the related work in HIP-based micro-mobility (Section 3). It then presents the proposed inter-subnet localized mobility solution (Section 4); and performance analysis based on analytic model (Section 5); and performance analysis based on simulation (Section 6); and conclusions in Section 7.

2. Host identity protocol

IP address has been used both as an identifier of a communication session and as a network locator; in the standard TCP/IP stack, the upper layer protocols such as TCP and UDP are bound to the IP addresses. As a MN moves and changes IP address, the reconfiguration of IP address breaks the ongoing TCP or UDP session. HIP [11] introduces a new namespace (host identity name space) to serve as host identifier to establish and maintain a communication session between the communicating parties, while the IP address serves only as a locator of the current point of attachment (PoA) of the host. In the HIP protocol stack (Figure 1), a new sub-layer (i.e., Host Identity Layer) decouples the transport layer from the inter-networking layer, thus making the ongoing communication independent of the host location. This is because the transport protocols are bound to HI [i.e., 128 host identity tags (HITs) for IPv6 application and 32 local scope identifiers for IPv4 application]. In addition, the translation between the HI and the respective IP addresses takes place at the host identity layer in both sending and receiving nodes.

2.1. HIP Base Exchange

The HIP works in two modes: the control mode or Base Exchange (BE) and the data traffic mode. In the BE, the communicating parties establish a pair of security

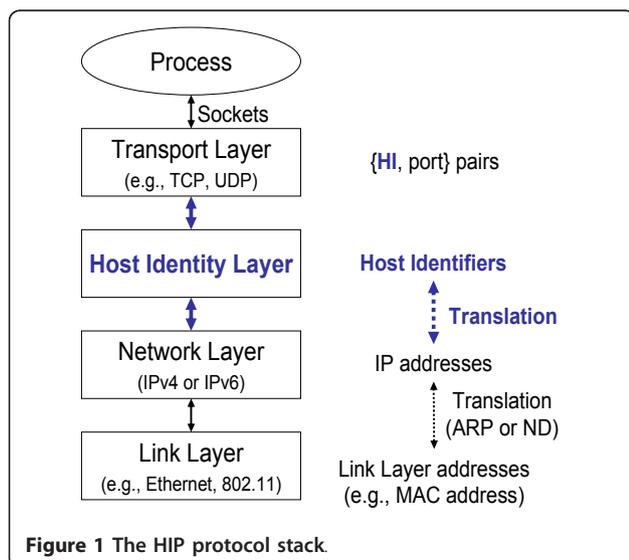


Figure 1 The HIP protocol stack.

associations (SA) between themselves [11]. The BE consists of four packages that are exchanged in two round-trip times (RTT). These packages include I1, R1, I2, and R2. The communicating parties exchange I1 and R1 in the first RTT followed by I2 and R2 in the second RTT. Figure 2 describes the establishment of the SA between two communicating parties, each having a single IP address. A node that triggers HIP SA is called an initiator (i) and the one that responds to the triggering message (I1) is called a responder (r). Upon receiving I1 packet (i.e., I1), which includes the HIT of the initiator HIT (i) and the HIT of the responder HIT (r), the responder sends R1 packet. If the initiator is not aware of the responder's HIT, then it may use the opportunistic mode by using zeros as the responder's HIT. In R1 packet, a puzzle to be solved by the initiator will be included. This is done to protect the responder against the DoS. In addition, both the initiator and the responder use the Diffie-Hellman technique to generate their keying material. An initiator received DH (r) from R1 packet and sends the puzzle solution along with its DH (i) in I2 packet. Upon receiving the I2 packet, the responder then verifies the puzzle solution and use DH (i) to generate the keying material. Furthermore, the responder confirms by R2 packet. At this end, the initiator and responder successfully exchange the packets (I1, R1, I2, and R2 packets) and establish a pair of HIP SA. Afterward, the initiator and the responder use ESP extension [12] to securely exchange data traffic between them.

2.2. Mobility and multihoming in HIP

Mobility and multihoming support for HIP is presented in a separate IETF document [13]. This extension allows the HIP-enabled MN to notify its peers about the set of new locators by exchange of three UPDATE packets. When an MN moves, it includes the new locator into an UPDATE packet and sends to its peers. Afterward, the peers of the MN can redirect the traffic to the new location of the MN after the required address check is performed. The purpose of the address check is to protect against different security threats due to mobility such as a DoS and traffic flooding. Moreover, a global

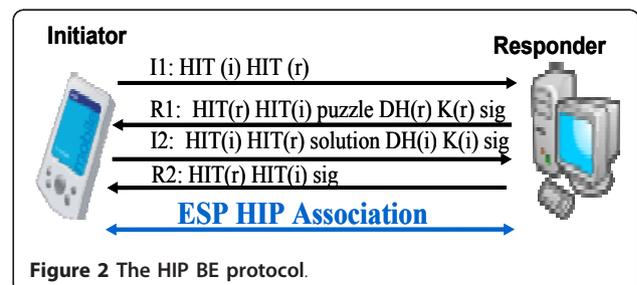


Figure 2 The HIP BE protocol.

mobility anchor point, which is the HIP rendezvous server (RVS) [14], is employed to offer stable location information for the MNs that are registered on the RVS. Therefore, any host who wants to communicate with the HIP MN can find the current location of the corresponding MN at the RVS.

The HIP also efficiently and securely provides multihoming feature, which is a feature that enables HIP MN to have more than one locator at the same time. The same procedures that were used to inform MN's peers about mobility (i.e., new locator) are used to inform MN's peers about multihoming (i.e., multiple locators at which MN can be reached at the same time). The HIP MN can also "declare" and use one of these locators as the preferred locator.

3. Related work

This section briefly describes the existing micro-mobility solutions based on HIP and their shortcomings. The HOL varies in different handover scenarios [15], for example, in macro-mobility and micro-mobility scenarios.

There is no adequate micro-mobility management solution for HIP but only some proposed solutions [16-18]. A local rendezvous server (LRVS) [16] has been utilized in the micro-mobility architecture for HIP. The LRVS extends the normal HIP RVS to perform network address translation as well as the normal RVS functions. Once the MN enters a given local domain, it detects the LRVS in the visited network either by actively initiating a service discovery procedure or passively waiting for a service announcement. Then, the MN registers itself at the LRVS. The LRVS also registers its IP address and the MN information at the RVS. The MN, therefore, notifies the LRVS instead of the correspondent node (CN) to redirect the data traffic to its new location, i.e., the new local IP (LIP) address. However, this solution does not avoid IP address configuration and re-registration at the LRVS whenever the MN moves from one subnet to another within the same domain. The IP configuration, which requires Duplicate Address Detection (DAD), adds some delay to the handover process while the re-registration takes considerable time that also contributes to the HOL. Moreover, for the registration, the MN always sends its new IP address to the LRVS even when there is a cross-over point between the old PoA and the new one. Hence, the time required to do the re-registration at the LRVS is relatively higher than that required at a topologically closer one (i.e., cross-over). Furthermore, during the registration at LRVS, the LRVS continues to forward the ongoing packets that are destined to the MN to the old Access Router (AR) that was the previous PoA for the MN. This increases packet delay and loss.

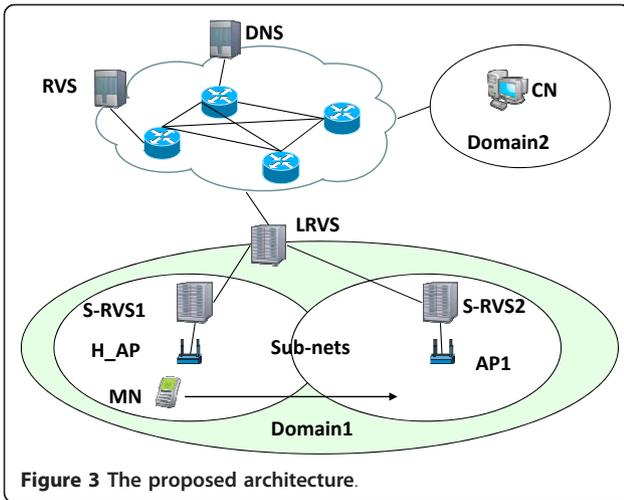
Another method for securing micro-mobility that is more reasonable for hierarchical mobility domains is presented in [17]. It focuses on the authentication of the location-binding update messages to prevent the possible security issues such as man-in-the-middle attack and DoS. It uses regional anchor point which supports the dynamic binding between the end-point identifiers and their IP addresses. Once an MN enters a given region, it does not need to register at any mobility anchor points within that region. During the SA establishment, mobility anchor points in the region learn the required security context and current location information of the MN, while the nearest anchor point (NAP) only knows the shared secret key of the communication session. The solution is based on the use of Lamport one-way hash chains and secret-splitting techniques to bind the messages of location updates (LU) together and to establish a SA between the MN and the nodes (e.g., anchor points in a domain) along the path of the MN and CN.

However, this solution behaves as a macro-mobility solution in many situations. For example, if the Lamport one-way hash chain reaches the seed value or a man-in-the-middle attack between the MN and the NAP occurs, then this scheme requires the creation of a new hash chain. Furthermore, the scheme still needs to reconfigure its LIP if the MN changes its PoA, thus affecting the HOL, signaling overhead and packet loss, as well as compromising location privacy.

Finally, a HIP-based mobility management architecture scheme which used tight coupling between the UMTS and WLAN is proposed in [18]. The architecture uses a RVS in the UMTS network to handle the handover process with a strategy to establish a new connection before terminating the previous one. However, it still suffers from the same problem that was faced by [16,17] in terms of IP configuration delay as a result of IP address changes. The signaling flow of this scheme is similar to that of the scheme in [16], who, however, use the RVS to manage the mobility in a domain rather than using the LRVS. Even though the handover performance is improved, it still needs to be optimized.

4. Proposed inter-subnet mobility solution

We propose a HIP-based micro-mobility solution with the advantages of keeping the IP addresses of the MN stable in a given domain. The mobility entities in our proposed architecture (Figure 3) are responsible for tracking the movements of the MN and the exchange of the required mobility signaling on behalf of the MN. The core functional entities are the LRVS which is proposed in [16] along with the subnet-RVS (S-RVS) that we introduce. The LRVS is responsible for maintaining the MN's "reachability" information while the S-RVS entity performs the mobility-related signaling on behalf



of a MN. S-RVS resides on the access link where the MN is attached. It is also responsible for detecting the attachments of MN to and from the access link and for initiating the update messages to the N-AP. N-AP is the

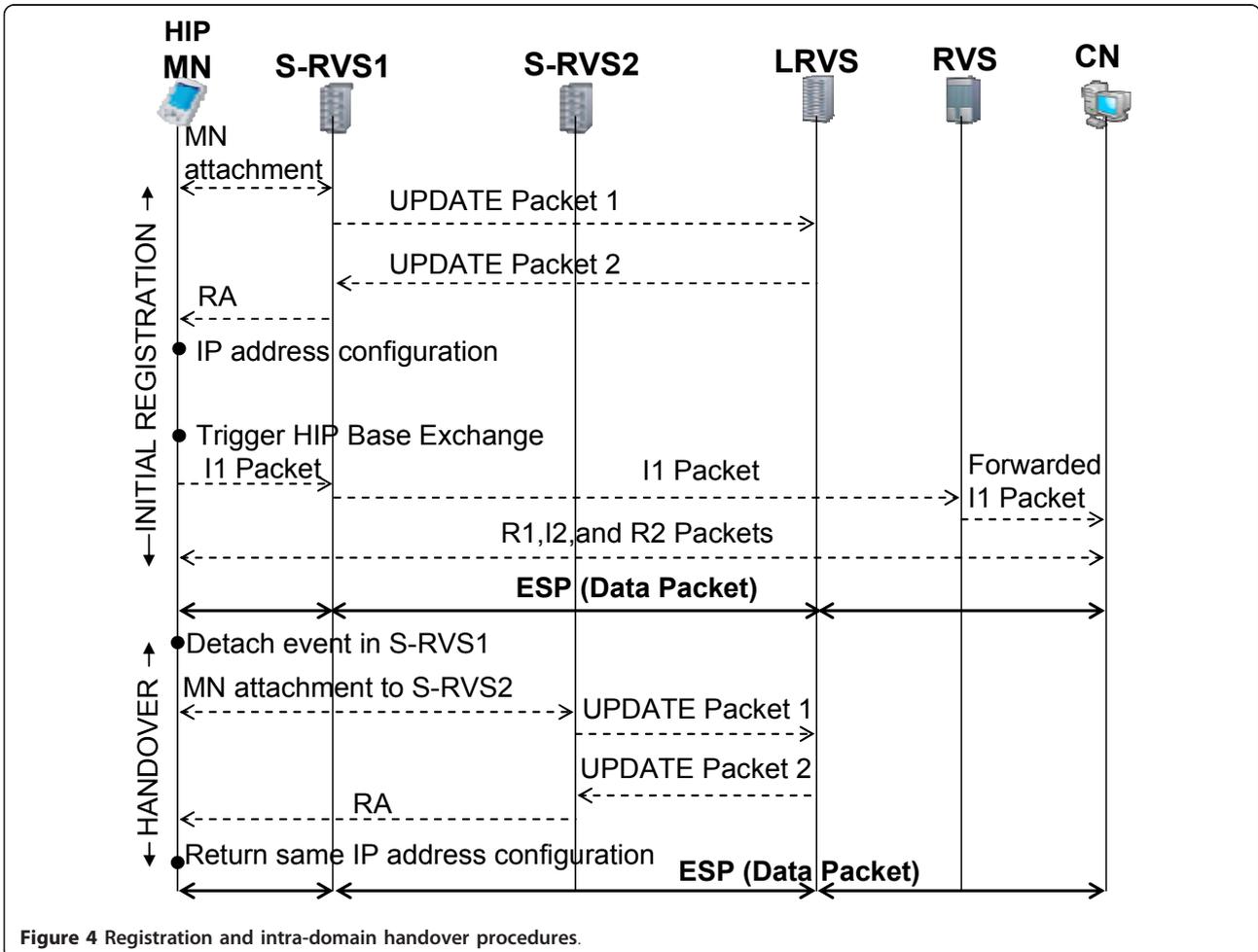
cross-over point between the old PoA and the new PoA of that MN.

The design of our scheme is based on two principles: (1) distributed caches are employed to store fresh R1 pre-computed packets; and (2) MN will use the same IP address, as it remains within a single domain.

The caching of fresh pre-computed R1 packet at LRVS optimizes the handover performance when re-keying is required because of a handover. Besides the re-keying, the HIP SA can be timeout. In both cases, the re-establishment of the HIP SA is required.

Figure 4 shows the registration and handover of MN between two wireless access networks connected to the Internet through a LRVS, which manages the mobility within a given domain. We assume that the MN and CN are registered at the RVS, which is outside the domain managed by the LRVS. The CN is a fixed HIP host in a different domain.

When a MN enters a given domain for first time, the complete process is illustrated in Figure 4: the INITIAL REGISTRATION part that is explained hereafter. The S-



RVS on the access link to which the MN is attached, i.e., S-RVS1, first detects the MN and then sends an UPDATE packet (UPDATE packet 1) with registration flag to the LRVS. The packet includes the HIT of the MN. Upon receiving the UPDATE packet 1, the LRVS responds with the UPDATE packet 2. The UPDATE packet 2 includes a network prefix that will be delivered to the MN at any subnet in the given domain. After receiving the UPDATE packet 2, S-RVS1 sends a Router Advertisement (RA) including the network prefix for the MN to configure its IP address.

If the MN intends to communicate with a HIP host (e.g., CN), it then needs first to establish a HIP SA as explained in section (IIA). In this case, the MN sends I1 (triggers HIP SA establishment) packet to the S-RVS1, which in turn forwards the packet to the LRVS. Then, LRVS further forwards the packet to the CN through the RVS.

The exchange of the remaining packets (i.e., R1, I2, and R2) goes directly (i.e., not via the RVS) between the MN and the CN. After successful exchange of these packets, a HIP SA will be established between the initiator (i.e., MN) and the responder (i.e., CN). Through the SA establishment all the S-RVSs along the path between the MN and the LRVS are aware of the SA context.

When the MN performs intra-domain handover, S-RVS1 (i.e., old S-RVS) is no longer the serving S-RVS. The new S-RVS detects the attachment of the MN and sends an UPDATE packet 1 to the LRVS. Upon receiving the UPDATE packet 1, LRVS verifies the MN and then updates the MN's binding record. Afterward, LRVS responds with the UPDATE packet 2. Using the content of the UPDATE packet 2, the new S-RVS sends an RA, which includes the same network prefix that MN employed to configure its IP address during the initial registration, to the MN. The MN, therefore, retains the same IP address configuration. This may significantly reduce the HOL and signaling overheads due to handover. It is important to note that the proposed solution is intended for IPv6 networks. In addition, the study in this article is mainly concerned about localized mobility management where the host mobility is very high, but the efficient management of inter-domain handovers is expected to be taken up in future study.

This HIP-based micro-mobility management solution reduces the HOL and signaling overheads by allowing an MN to use the same IP address (to avoid the DAD process as it remains within a single domain) and sending the MN's HIT and assigned network prefix to the other S-RVSs (e.g., S-RVS2) at an appropriate time. Then, the new S-RVS sends both the same network prefix to the MN to retain the same IP configuration, and the UPDATE packet 1 to the LRVS to set up a new path for the ongoing traffic. The use of the same IP

address supports the location privacy. Furthermore, the use of HIT in the upper layer protocol instead of IP address enables HIP host to use the established HIP associations during and after the handover, since the communication context remains the same. Moreover, reducing the time taken to perform HIP BE can also reduce the handover delay when the re-establishment of HIP SA is required. Having S-RVS also eliminates the need for a new location reachability check between the MN and its peer, because the new location of the MN is known to the serving S-RVS. The number of S-RVSs in a domain depends on the domain's size, and each subnet is managed by an S-RVS which acts as the authoritative S-RVS for that subnet. The number of MNs in each subnet must not exceed the capability of the S-RVS. This method can also manage simultaneous move of communicating parties (i.e., when the communicating parties move at the same time) and multihoming in an easy and efficient manner.

S-RVS is co-located within the ARs that are deployed in secure private networks. In addition, HIP hosts (i.e., MN and CN) still establish SA between themselves while S-RVSs only manage mobility packets using an established SA. Therefore, neither security nor reliability of HIP MN will be compromised by introducing S-RVS in a secure private network.

It is important to note that we provide a network-based micro-mobility support at HIP layer but not at IP layer as do some proposed solutions [19,20]. Solutions [19,20] are about using of PMIPv6 [21] to support HIP MNs. Yet, both solutions are using IP technology to support host mobility for HIP MN. The main difference between providing mobility supports at HIP layer and at IP layer is that the first can utilize all the HIP features, which are security, multi-homing, interoperability between IPv6/IPv4, and mobility. Furthermore, our proposed scheme can easily be extended to support host mobility using HIP technology for non-HIP MN.

5. Analytic evaluation of handover performance

The following section briefly compares the basic HOL involved in HIP, Micro-HIP, and our proposed scheme. We developed an analytic model based on explanations of Figures 5, 6, and 7 to measure HOL and mobility-related signaling overheads of HIP, Micro-HIP, and our scheme, respectively. Note that CN1 and CN2 can be in the same or in different domains. Another issue to be considered is that which one of CNs will be the first to inform is immaterial. However, the receipt of the UPDATE packets depends on the distance between the MN and the respective CN. The sequence of the UPDATE packets in Figure 5 is one of possible exchanges that can take place in real networks.

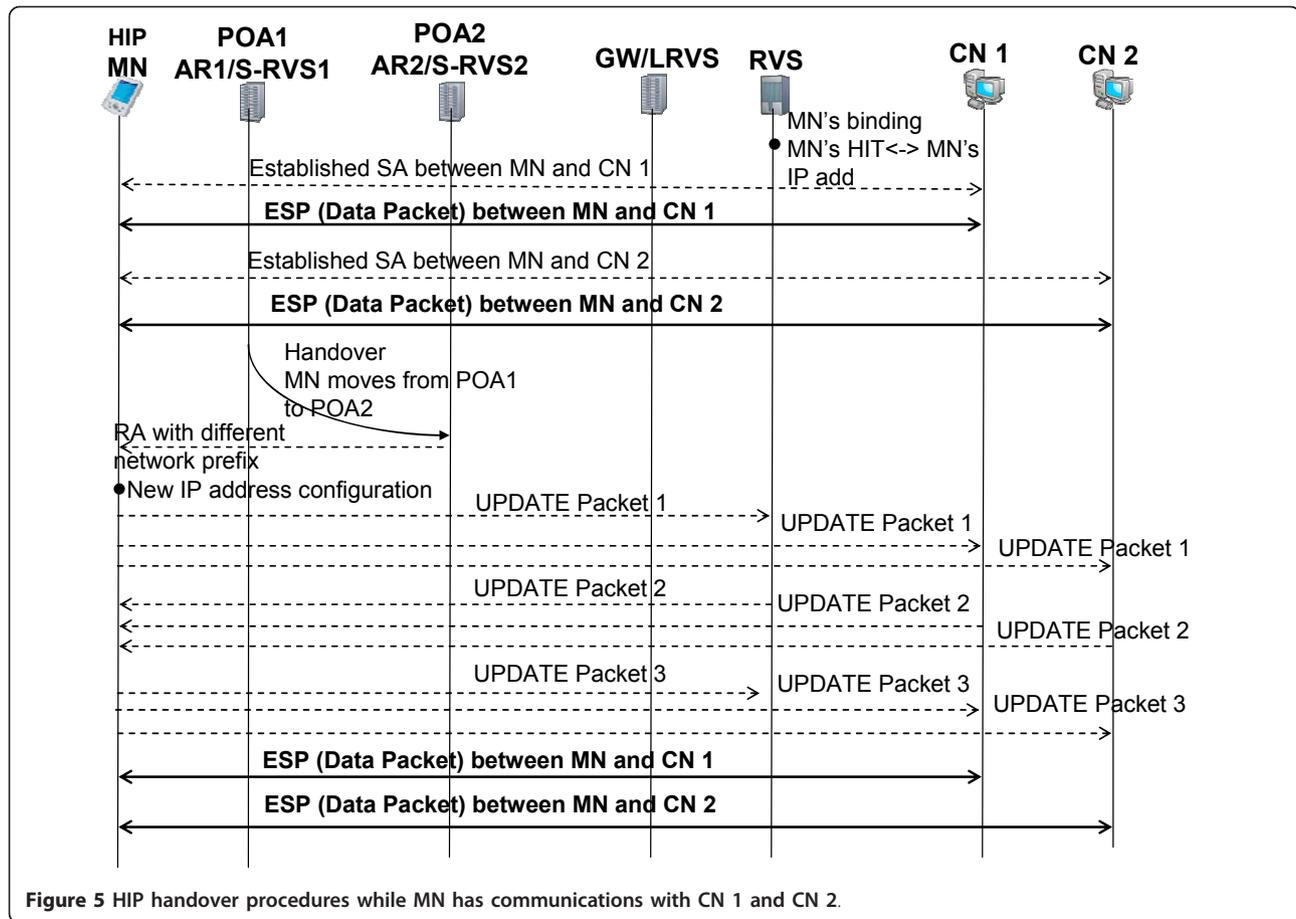


Figure 5 HIP handover procedures while MN has communications with CN 1 and CN 2.

5.1. HIP

We assumed that HIP MN registered at the RVS with binding contains the MN's HIT and IP addresses of the MN which can currently be reached. We also assumed that the MN has ongoing communications with both CN 1 and CN 2 as shown in Figure 5.

When a HIP node moves from one PoA to another, the following HOL components are involved:

- The latency due to the MN's movement detection (MD) at IP layer in MN's stack, L_{MD} .
- The latency due to the MN configuring its current IP address at the new location, L_{IP_CONF} .
- The latency due to the HIP MN sending the update message with a locator parameter (carried in the first UPDATE packet) to update the CNs, L_{LU1_CN} .
- The latency due to the sending of the second UPDATE packet from CN to MN to verify the new locator, L_{LU2_CN} .
- The latency due to the sending of the third UPDATE packet from the MN to CNs to confirm verification of the new locator, L_{LU3_CN} .

Thus, the HOL due to the basic HIP mobility management protocol is as follows:

$$L_{HIP(MN, CN_i)} = L_{MD_i} + L_{IP_CONF} + L_{LU1_CN_i} + L_{LU2_CN_i} + L_{LU3_CN_i} \quad (1)$$

where $i = 1..n$; n is the number of CNs to which MN has ongoing communications. In addition, n must be greater than or equal 1. This is because no UPDATE packets are needed when MN does not have any connection with CN (i.e., $n = 0$).

After the HOL, both CN 1 and CN 2 redirect their data traffic to the new location of the handed over MN. Yet, RVS can only direct any host that intends to establish a new communication with the handed over MN to the old POA of the MN. This continues until an MN updates its record at the RVS. The following latencies affect the required time for MN's binding update at RVS:

- The latency due to the HIP MN sending the update message with a locator parameter (carried in the first UPDATE packet) to update the RVS, L_{LU1_RVS} .
- The latency due to the sending of the second UPDATE packet from the RVS to MN to verify the new locator, L_{LU2_RVS} .

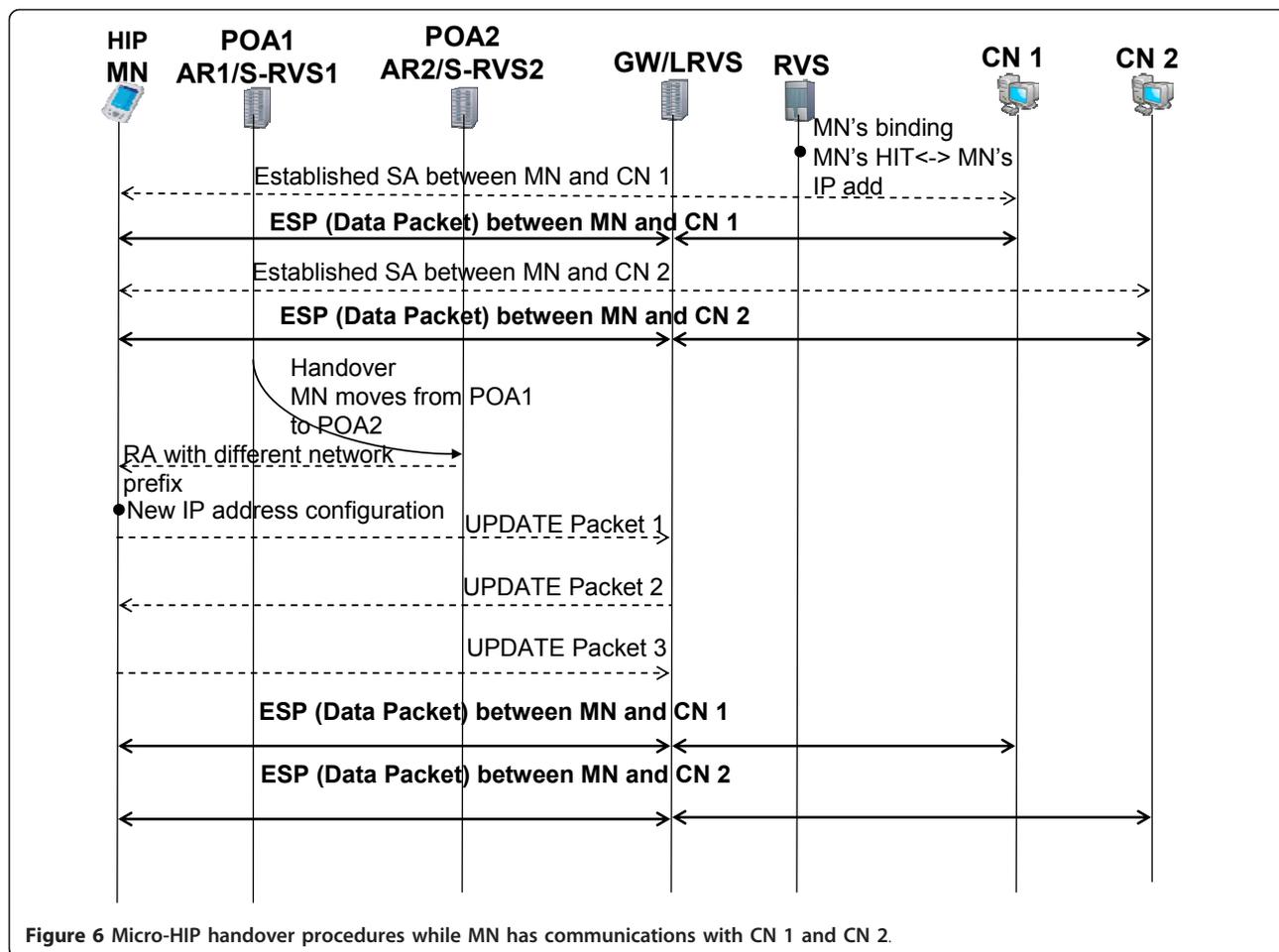


Figure 6 Micro-HIP handover procedures while MN has communications with CN 1 and CN 2.

- The latency due to the sending of the third UPDATE packet from the MN to RVS to confirm verification of the new locator, L_{LU3_RVS} .

$$L_{HIP}(MN, RVS) = L_{IP_CONF} + L_{MD} + L_{LU1_RVS} + L_{LU2_RVS} + L_{LU3_RVS} \quad (2)$$

Figure 5 shows signaling flow of the MN's handover using the HIP while the MN has ongoing communications with both CN 1 and CN 2. Having two ongoing communications, MNs have to exchange six messages (i. e., three UPDATE packets with each of the CNs). In addition, MN needs to exchange additional three UPDATE packets with RVS to update its binding. The number of messages that used to update MN's binding at the RVS with which the MN is registered and to inform the CNs, CN 1 and CN 2, with which MN has ongoing communications are nine UPDATE packets. The analytic model for the HIP shows that the number of CNs with which MN has ongoing communications significantly increases the numbers of the UPDATE packets. Having MN that has two communications with CN 1 and CN 2 as well as a binding record at RVS, the numbers of UPDATE packets can be calculated by the

following simple equation:

$$N_{UP_HIP} = 3 * (n + 1) \quad (3)$$

where n is the number of CNs to which MN has ongoing communications, while 3 indicated the number of the required UPDATE packets to inform each CN or to update the MN's binding at the RVS.

5.2. Micro-HIP

Having the same assumption to examine handover performance of the HIP, we developed another analytic model to measure HOL and mobility-related signaling overheads of Micro-HIP while an MN has two ongoing communications with both CN 1 and CN 2 as shown in Figure 6. From the figure, when an MN performs a handover from POA1 to POA2, the following HOL components are involved:

- The latency due to the MN's MD at IP layer in MN's stack, L_{MD} .
- The latency due to the IP address configuration of the MN at the new PoA, L_{IP_CONF} .

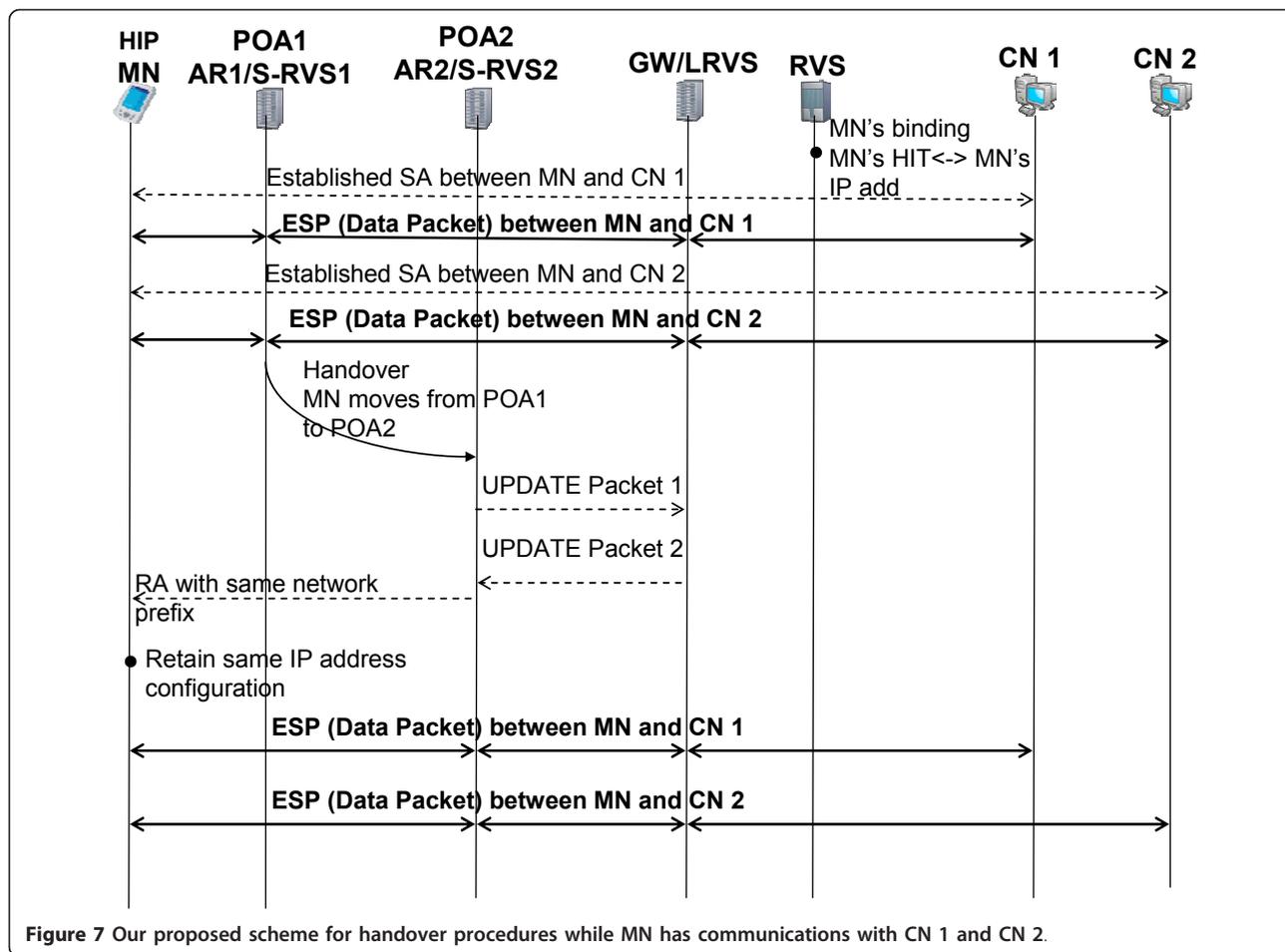


Figure 7 Our proposed scheme for handover procedures while MN has communications with CN 1 and CN 2.

- Latency due to the HIP MN sending the update message with a locator parameter (carried in the first UPDATE packet) to update the relevant components (LRVS), L_{LU1_LRVS} .
- Latency due to the sending of the second UPDATE packet from the LRVS to MN to verify the new locator, L_{LU2_LRVS} .
- The latency due to the sending of the third UPDATE packet from MN to LRVS to confirm the verification of the new locator, L_{LU3_LRVS} .

Thus, the HOL for a Micro-HIP protocol is as follows:

$$L_{\text{Micro-HIP}} = L_{\text{IP-CONF}} + L_{\text{MD}} + L_{\text{LU1_LRVS}} + L_{\text{LU2_LRVS}} + L_{\text{LU3_LRVS}} \quad (4)$$

Unlike the HIP, the use of the Micro-HIP allows the MN to only inform LRVS about the new IP address. Three UPDATE packets as shown in Figure 6 are enough to redirect the data traffic to the MN's new location. Evidently, by explanations on Figure 6 and the developed analytic models for HIP and Micro-HIP, HOL and mobility related signaling overheads of the Micro-HIP are partially optimized. Yet, the HIP and the

Micro-HIP have signaling overheads on the MN's interface and further incur the signaling overheads of the new IP configurations because of the MN's handover.

5.3. Our scheme

Figure 7 shows an explanation of handover management using our proposed scheme while the MN has ongoing communications with two CNs, CN 1 and CN 2. Again, based on the same assumption to evaluate handover performance of the HIP and the Micro-HIP, we developed an analytic model to measure HOL and mobility-related signaling overheads while the MN has ongoing communications with CN 1 and CN 2.

Our proposed scheme has the following components contributing to HOL:

- The latency due to the MN's attachment detection (AD) at IP layer in POA's stack, for which reason, we called it attachment rather than MD, L_{AD} .
- Latency due to the two way handshake readdressing protocol, between S-RVS and LRVS, $L_{\text{LU1}} + L_{\text{LU2}}$.

Thus, the HOL due to our proposed scheme is as follows:

$$L_{\text{Our scheme}} = L_{\text{AD}} + L_{\text{LU1}} + L_{\text{LU2}} \quad (5)$$

A comparison between Equations 1, 4, and 5 that describe HOL of the HIP, the Micro-HIP, and our proposed scheme shows the advantages of the last one, Equation 5. Our proposed scheme is better than those of the HIP and the Micro-HIP, Equations 1 and 4, respectively, because our proposed scheme reduces LU latency and the number of the required UPDATE packets as well as eliminates messages and latency related to the configuration of the new IP address.

Unlike the HIP and the Micro-HIP, our proposed scheme does not involve the MN in mobility-related signaling. As shown in Figure 7, the new PoA (i.e., POA2) only exchanges two UPDATE packets with LRVS to redirect the MN's traffic through POA2. To clearly show the differences between the HIP, Micro-HIP, and our scheme, we summarize the mobility-related signaling overheads in Table 1. Evidently, by the developed models, our proposed scheme overcomes the shortcomings of the HIP and the Micro-HIP solutions to efficiently manage mobility in a localized domain.

The first row in Table 1 shows that the number of binding update messages when the MN has ongoing communication sessions with the two CNs. In addition, the number of binding update messages when MN has ongoing sessions with n CNs are shown in the second row of the table. It is important to note that mobility-related signaling overheads of the plain HIP are highly affected by increasing the number of the CNs to which MN has ongoing communication sessions. In contrast, mobility-related signaling overheads of the Micro-HIP and our proposed scheme do not get affected by increasing the number of CNs. This is because the Micro-HIP and our scheme update only the network gateway, irrespective of how many CNs with which MN has ongoing communication sessions. It is also important to note that the HIP, the Micro-HIP, and our proposed scheme need not consult any third party for security purpose as they have capabilities of self-certifying because of the HIP layer. However, schemes [19,20] need to consult a third party for security purposes. This third-party security consultation incurs costs of

additional signaling overheads and adds some delay to the total HOL.

6. Simulation results

Using OMNeT++ simulator [22] and HIPSIM++ simulation framework [23], we extended our simulation model [24] to incorporate a mechanism that allows the HIP-enabled MN to use the same IP address in different sub-networks under the same LRVS. We examined the new simulation model using the same network topology and simulation scenario that we used in [24], but the simulation time extended from 5100 to 25,000 s. Table 2 shows the necessary simulation parameter configuration under which we evaluate the handover performance of the HIP, the Micro-HIP, and our proposed scheme. Similar to the simulation environment under which we examined the HIP and the Micro-HIP, to examine our proposed scheme, we deployed two IEEE 802.11b access points, the home access point (H_AP), and the access point 1 (AP1). Furthermore, we co-located two S-RVSSs, S-RVS 1 and S-RVS 2, within two ARs, AR 1 and AR 2, and partially overlapped the two sub-networks that were managed by AR 1 and AR 2. A fixed HIP CN (i.e., hipsrv), which is placed outside the access network of the MN, is used for running the UDP application and transmitting datastream at 15 kbps with a packet size of 256 bytes to the MN.

Before showing our investigation of handover performance for the HIP, the Micro-HIP, and our proposed scheme, we need to first identify the evaluated parameters and define what they mean in this simulation context. During this simulation, the HOL, the lost packets, and the signaling overhead parameters are investigated. HOL here refers to the time difference between the time when the MN is able to receive packets in the new PoA and the time when the MN was unable to receive packets in the old PoA. The lost packets refer to the number of packets that are lost from the downstream traffic during the HOL. Signaling overhead means the number of the required signaling packets per handover, which are used for LU or IP address configuration.

Using the above mentioned simulation environment, we examined the three models (HIP, Micro-HIP, and our proposed scheme). In addition, we recoded and

Table 1 Signaling overheads of HIP, Micro-HIP, and our proposed scheme

Signaling messages	HIP	Micro-HIP	Our scheme
# of UPDATE packets per handover when communicating with two CNs	9	3	2
# of UPDATE packets per handover when communicating with n CNs	$3*(n + 1)$	3	2
Signaling overheads on MN's interface	Yes	Yes	No
Signaling overheads due to configuration of new IP address	Yes	Yes	No

Table 2 Simulation parameters

Parameter	Value	Parameter	Value
Speed	1 m/s	Mobility model	Rectangle
# of POA	2	Packet flow	Bi-dir CBR
# of MN	1	UDP packet transmit rate	0.13 s
AP power	2.0 mW	Beacon freq.	0.1 s
Min router Adv. Interval	0.3 s	Max router Adv. interval	0.7 s
Grid size(m ²)	850 * 850	Packet size	256 B

deeply analyzed a hundred handoffs for each of the three models. The fluctuation in the HOL of the models over the first 20 handover (HO) instances is shown in Figure 8.

It can also be observed that there was a significant decrease in the HOL in our scheme. Our scheme achieved the lowest HOL that was in the fourth HO instance. Over the simulation time, different HO latencies other than that our proposed scheme experienced were consistently below 1.5 s. Furthermore, our scheme has stable HOL, while the HO latencies of the others (i. e., HIP and Micro-HIP) vary over the simulation time. This is because our scheme avoided DAD latency and MD latency, which are variable, but both the HIP and the Micro-HIP are still suffering from DAD latency and MD latency.

Our proposed scheme also achieved another advantage, which is the reduction of LU latency. This is because in our proposed scheme, LU is performed by an

S-RVS that is usually topologically closer to the LRVS than the MN's to the LRVS. In other words, the distance between the sender and the responder of the LU messages in our proposed scheme is shorter than the distance between the senders and the responders of the LU messages in both the HIP and the Micro-HIP. In addition, the number of the required LU messages in our proposed scheme is lesser than the LU messages of the other schemes.

To give a clear picture of how our scheme managed the HO of HIP MN, we explained a close-up view of the first HO of our proposed scheme in Figure 9. The figure shows HIP-enabled MN that was receiving UDP data traffic from its CN. CN was sending the data at 15 Kbps sending rate from outside MN's domain. Again, it is necessary to identify which HO definition will be used during the measurements and analysis. This is because HOL can be defined in many ways. Some articles including [16,25] co-relate HOL to fetching of the first data packets at the new-POA. For example, [16] refers to the HOL as the latency (time difference) between the time of receiving the first packet at the N-POA and the time of receiving the last packet at the previous PoA (P-POA).

As shown in Figure 9, the MN received the last packet in the P-POA (i.e., S-RVS1) at $X_s = 170.85$ s and the first packet in the N-POA (i.e., S-RVS2) at $X_f = 171.97$ s. The difference between X_f and X_s is typical to the HOL that mentioned above and used in [16].

From the measurements and analysis, we observed that the $HOL_{X_f-X_s}$ includes two delay components, which are not related to the components of handoff,

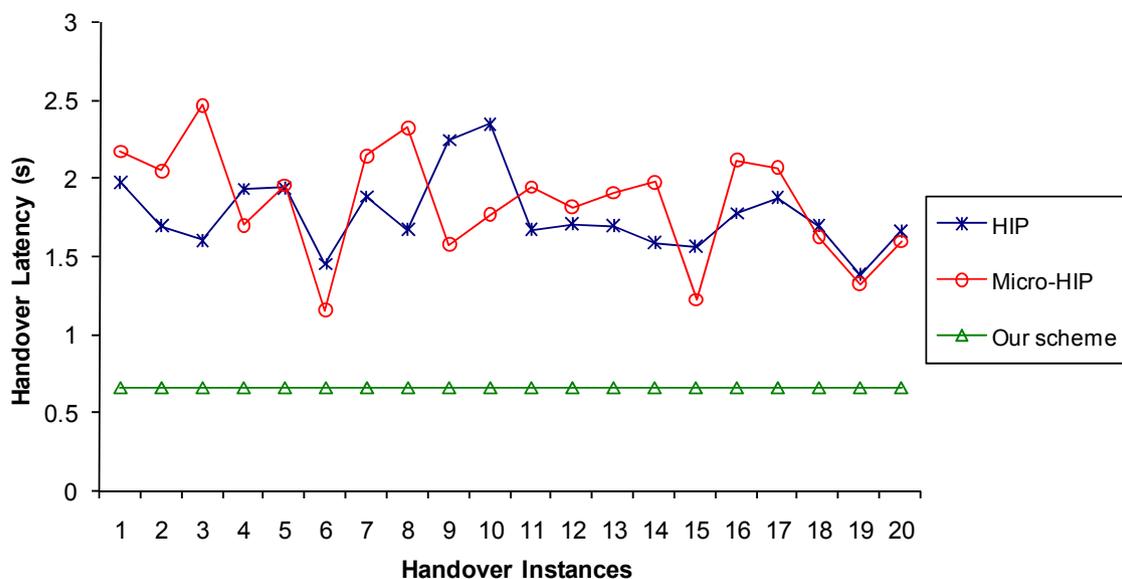
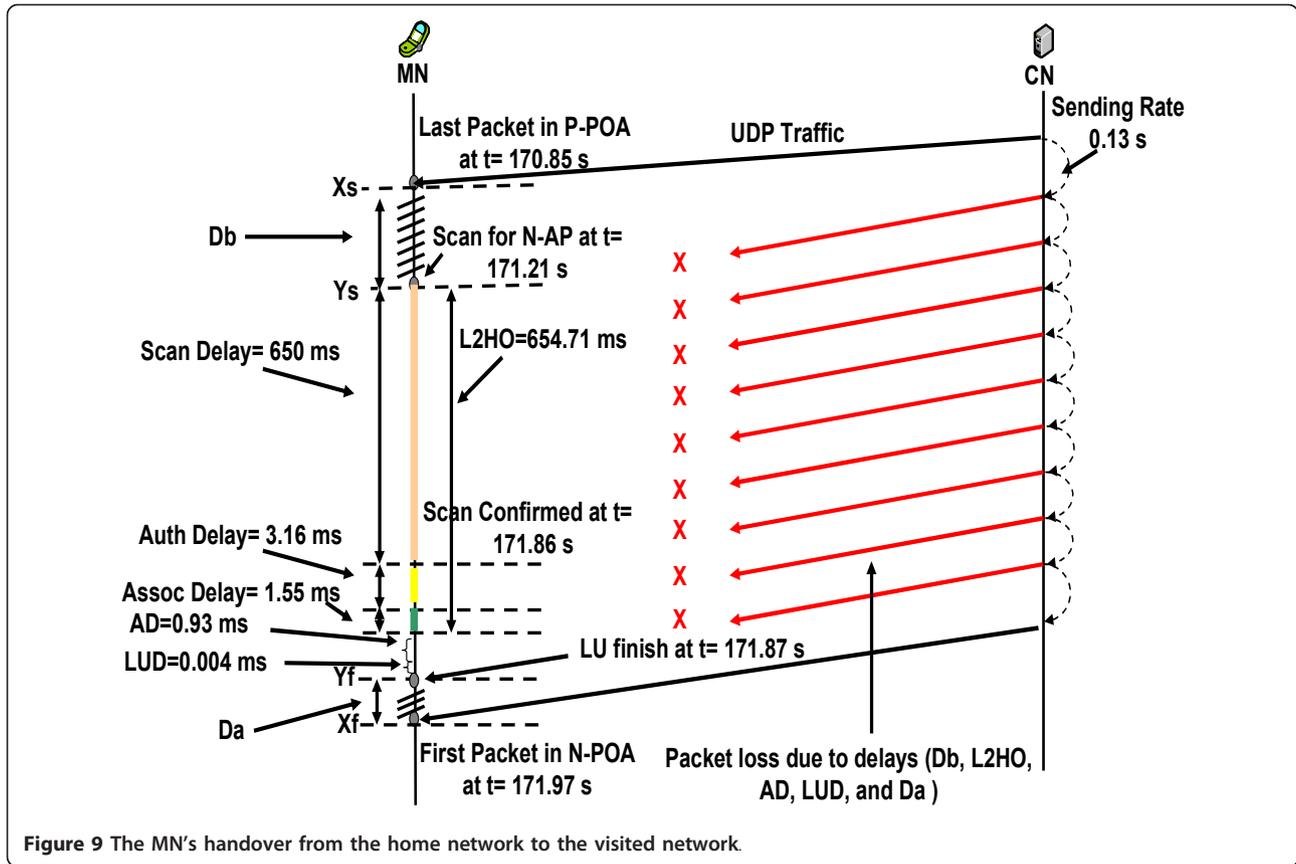


Figure 8 The first 20 handoffs for HIP, Micro-HIP, and our scheme.



but are related to HO events and other parameters. We explained the delay components in Figure 9 as shaded areas, which are the areas between Y_s and X_s , as well as area between X_f and Y_f . Therefore, we defined the HOL as the (latency) time difference between the time at which the MN becomes able to receive data packet from the N-POA and time at which the MN was unable to receive any data packet from the P-POA. In other words it is the time that the MN remains unable to receive any data due to HO processes. This definition only includes the main HO components, such as delay of scanning (SD), authentication (AuthD), and association (AssD) in the link layer, as well as the delay of attachment detection (ADD), IP configuration, and location update (LUD) in the network layer.

We used the Y_s and Y_f to indicate the points of time when the first component of HO (link layer switching) took place and when the last one (LU) finished, respectively, and also used $HOL_{Y_f-Y_s}$ to denote such delay. The $HOL_{Y_f-Y_s}$ in our scheme was only due to attachment delay (AD) and location update latency (LUD). This is because our proposed scheme has a mechanism that ensures the avoidance of a new IP configuration delay.

The co-relation and differences between the two HOL definitions ($HOL_{X_f-X_s}$ and $HOL_{Y_f-Y_s}$) are illustrated in the figure and explained hereafter. The following equations show the co-relation:

$$HOL_{Y_f-Y_s} = SD + AuthD + AssD + MDD + LUD \quad (6)$$

$$HOL_{X_f-X_s} = HOL_{Y_f-Y_s} + Db + Da \quad (7)$$

The delay before scanning (Db) and delay after LU (Da) are the delay components that are not related to the components of the HO, but these delays occurred because of HO events, and were included in the first definition of HOL. The (Db) is the time difference between the time of receiving the last packet in the P-POA and time of starting the scanning for a new access point (N-AP). In our model, Db delay was 0.36 s. The delay of Db depends on factors including data sending rate at the CN, the distance between the MN and the CN, and signal strength of the N-AP. These factors also affect the delay after (Da) LU, which is the time difference between the time of receiving the first packet at the N-POA and the time of binding update completion. In our scheme, Da was about 0.1 s. The combined delay due to both Db and Da was 0.46 s which is very high.

To our knowledge, neither macro-mobility management solutions (e.g., MIPv6 and HIP) nor micro-mobility management solutions (e.g., HMIPv6 and PMIPv6) addressed the Db and Da. Therefore, these solutions will experience such delays and incur a high HOL.

The micro-mobility management solutions usually anchor mobility in a domain of the MN or somewhere close to the MN to reduce the HOL. This implies that the CN location (i.e., How far it is from the MN?) will not affect the HOL. Furthermore, when the MN has ongoing communications with many CNs, the MN only informs the mobility anchor point instead of informing all the CNs like macro-mobility solutions. It is true that LUD will not be affected by the distance between the MN and the CN, but both Db and Da are directly affected by that. For example, in our proposed micro-mobility solution, the latency due to both Db and Da was 0.46 s, which is too high and will result in relatively large HOL. This issue as well as the handling of the non-HIP-aware node as the HIP-enabled node to enable a secured (based on HIP capabilities), efficient, and seamless HO mechanism are expected to be addressed in future studies.

Figure 10 depicts the HOL (HOL_{Yf-Ys}) that includes only the HO components for the HIP, the Micro-HIP, and our proposed scheme. This is the average of hundred handovers for each of the three models. The HOL measurements show that our proposed scheme outperformed both the HIP and the Micro-HIP. This is because, in our proposed scheme, the DAD latency is eliminated, and the LU latency is significantly reduced. Note that this HOL includes both layer 2 (i.e., about 0.66 s) and layer 3 HOLs. Layer 2's HOL was the same in the HIP, the Micro-HIP, and our proposed scheme. Layer 3 HOLs of the HIP, the Micro-HIP, and our proposed scheme were different. The difference between the HOLs of the HIP and the Micro-HIP was in the LU latency. LU latency of the Micro-HIP was shorter than

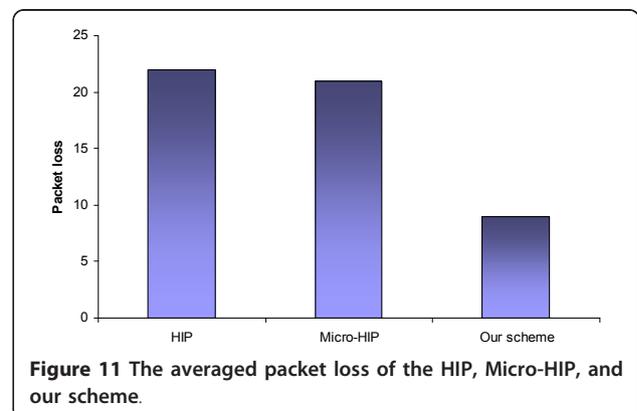
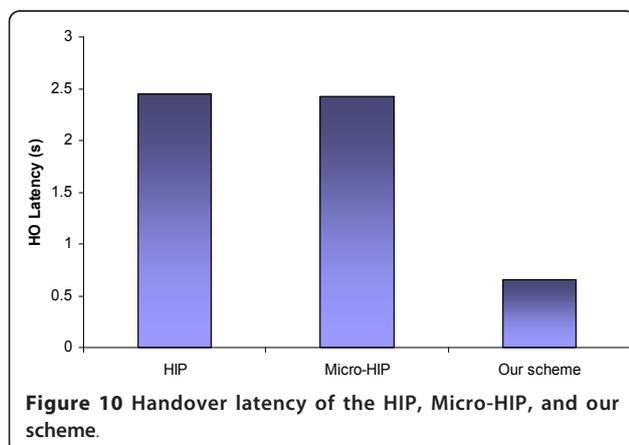
LU latency of HIP. This is because the Micro-HIP anchored mobility at the domain's gateway (i.e., LRVS) instead of informing CN, which is topologically far from the MN compared to LRVS from the MN. Unlike the HIP, the Micro-HIP eliminates signaling overheads between the domain's gateway (i.e., LRVS) and CN.

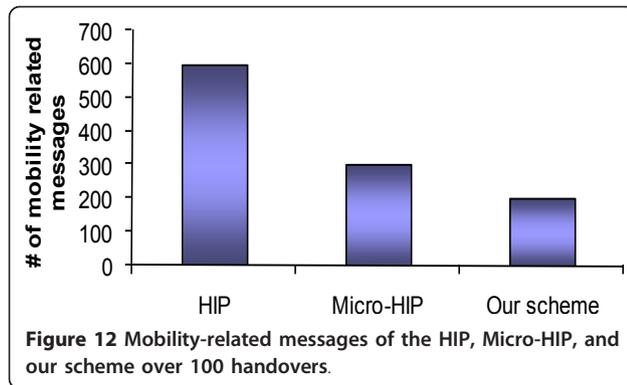
Figure 11 shows the packet loss of our proposed model (scheme) compared with the HIP and Micro-HIP. We measured the packet loss from traffic, data packets of UDP application, going between CN and MN during HOL. The inter-arrival rate of data packet was kept constant in all the cases. From the packet loss measurements, we observe that the number of packet loss is proportional to the HOL. Compared with the HIP and the Micro-HIP, our proposed scheme achieved the lowest HOL and thus the smallest number of packet loss. In our proposed scheme, there was an average of 9 lost packets per 100 handovers, whereas the HIP and the Micro-HIP lost 22 and 21 packets, respectively.

During a 25,000-s-simulation time, the number of the handover occurrences is 100. Figure 12 shows only the number of signals used for LU in the HIP, the Micro-HIP, and our proposed scheme during the entire simulation time. From the figure, it can be noted that our proposed scheme outperformed both the HIP and the Micro-HIP in terms of LU messages. This is because our scheme uses two-way LU protocol while HIP and Micro-HIP use three-way protocol for the LU. Unlike Micro-HIP and our scheme, per a handover, HIP uses three additional three UPDATE packets to update MN's binding at the RVS. Unlike the HIP and the Micro-HIP, our proposed scheme avoids all the signals related to DAD and the signal overheads related to HIP MN's interface.

7. Conclusion

We have proposed a new solution to optimize the handover performance for the HIP mobile nodes in a micro-mobility environment. We have also introduced a new





mobility functional entity, which is called the S-RVS. The S-RVS tracks the MN movement and acts on behalf of the MN whenever it moves. This reduces the HOL and the signaling overhead which in turn reduces the packet loss and delay. The proposed scheme can also support location privacy as well as optimize the HOL when re-keying is required (this will be modeled and examined). The proposed solution is modeled and implemented in OMNet++ network simulator. The analytic model and simulation results show that our scheme outperformed both the HIP and the Micro-HIP in terms of HOL and signaling overhead. This is because our scheme significantly reduced LU latency and totally avoided the DAD latency. In addition, our scheme also avoided the signaling overheads on the MN's interface. This is because the SRVS, which is co-located with the AR, performed all mobility-related function on behalf of the MN. Furthermore, our scheme ensured network-based mobility solution using HIP technology to efficiently support the MN's mobility.

Competing interests

The authors declare that they have no competing interests.

Received: 27 November 2010 Accepted: 4 August 2011

Published: 4 August 2011

References

1. FM Chiussi, DA Khotimsky, S Krishnan, Mobility management in third-generation all-IP networks. *IEEE Commun Mag* 124–135 (2002)
2. P Pacyna, Advances in mobility management for the NG internet. *China Commun.* 3(3) (2006)
3. P Reinbold, O Bonaventure, IP micro-mobility protocols. *IEEE Commun Surv Tutor* 3, 40–57 (2003)
4. D Le, X Fu, D Hogrefe, A review of mobility support paradigms for the internet. *IEEE Commun. Surv Tutor.* 8(1), 38–51 (2006)
5. C Perkin, Mobile networking through mobile IP. *IEEE Internet Comput.* 2(1), 58–69 (1998). doi:10.1109/4236.656077
6. A Gurtov, *Host Identity Protocol (HIP): Towards the Secure Mobile Internet* (Wiley and Sons, 2008) ISBN 978-0-470-99790-1
7. A Khurri, E Vorobyeva, A Gurtov, Performance of host identity protocol on lightweight hardware, in *Proceedings of ACM MobiArch* (August 2007)
8. P Jokela, T Rinta-aho, T Jokikyyry, et al, Handover performance with HIP and MIPv6, in *1st International Symposium on Wireless Communication Systems, 2004.* 3, 324–328 (2004)

9. TR Henderson, JM Ahrenholz, JH Kim, Experience with the host identity protocol for secure host mobility and multihoming. *IEEE Wirel Commun Netw.* 3, 2120–2125 (2003)
10. J Kempf, Problem statement for network-based localized mobility management (NETLMM), in *IETF, RFC 4830* (April 2007)
11. R Moskowitz, P Nikander, Host identity protocol (HIP) architecture, in *IETF, RFC4423* (May 2006)
12. P Jokela, R Moskowitz, P Nikander, Using the encapsulating security payload (ESP) transport format with the host identity protocol (HIP), in *IETF, RFC 5202* (April 2008)
13. P Nikander, T Henderson, End-host mobility and multihoming with the host identity protocol, in *IETF, RFC 5206* (April 2008)
14. J Laganier, L Eggert, Host identity protocol (HIP) rendezvous extension, in *IETF, RFC 5204* (April 2008)
15. S Yankov, S Wiethoelter, Handover blackout duration of layer mobility management schemes. *TKN Technical Report*, Berlin (May 2006)
16. S Novaczki, L Bokor, S Imre, Micromobility support in HIP: survey and extension of host identity protocol, in *Proceedings of the IEEE Mediterranean Electrotechnical Conference (MELECON 2006)*, pp. 651–54 (May 2006)
17. YJ Melén, P Nikander, et al. Re-thinking security in IP-based micro-mobility, in *Proceedings of the Information Security Conference (ICS'04)*, Palo Alto, CA, USA, pp. 318–329 (2004)
18. J So, J Wang, A HIP-based mobility management for UMTS/WLAN integrated networks, in *Australian Telecommunication Networks and Applications Conference (ATNAC 2006)* (2006)
19. M Muslam, HA Chan, N Ventura, LA Magagula, Hybrid HIP and PMIPv6 (HIPPMIP) mobility management for handover performance optimization, in *6th International Conference on Wireless and Mobile Communications, 2010, ICWMC*, pp. 232–237 (2010)
20. G Iapichino, C Bonnet, Host identity protocol and proxy mobile IPv6: a secure global and localized mobility management scheme for multihomed mobile nodes, in *Global Telecommunications Conference, 2009. GLOBECOM 2009, IEEE*, pp. 1–6 (November 30 2009 - December 4 2009)
21. S Gundavelli, K Leung, V Devarapalli, K Chowdhury, B Patil, Proxy mobile IPv6, in *IETF RFC 5213* (August 2008)
22. OMNet++ open source network simulator Official website: <http://www.omnetpp.org/>
23. L Bokor, S Novaczki, LT Zeke, G Jeney, Design and evaluation of host identity protocol (HIP) simulation framework for INET/OMNet++, in *Proceedings of the 12th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM 2009)*, Tenerife, Canary Islands, Spain 124–133 (2009). ISBN:978-1-60558-616-8
24. M Muslam, HA Chan, N Ventura, Host identity protocol extension supporting localized mobility management, in *CCNC 2011 PerNets Workshop, Las Vegas, Nevada* (2011)
25. K-S Kong, W Lee, Y-H Han, M-K Shin, H You, Mobility management for all-IP mobile networks: mobile IPv6 vs. proxy mobile IPv6. *IEEE Wirel Commun.* 15(2), 36–45 (2008)

doi:10.1186/1687-1499-2011-55

Cite this article as: Muslam et al.: Inter-subnet localized mobility support for host identity protocol. *EURASIP Journal on Wireless Communications and Networking* 2011 **2011**:55.

Submit your manuscript to a SpringerOpen® journal and benefit from:

- Convenient online submission
- Rigorous peer review
- Immediate publication on acceptance
- Open access: articles freely available online
- High visibility within the field
- Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com