Performance Comparison of IPv6 Multihoming and Mobility Protocols

Charles Mugga, Dong Sun, Dragos Ilie
School of Computing
Blekinge Institute of Technology (BTH)
Karlskrona, Sweden
E-mail: {chmu11, sudo11}@student.bth.se, dragos.ilie@bth.se

***Abstract*—Multihoming and mobility protocols enable computing devices to stay always best connected (ABC) to the Internet. The focus of our study is on handover latency and rehoming time required by such protocols. We used simulations in OMNeT++ to study the performance of the following protocols that support multihoming, mobility or a combination thereof: Mobile IPv6 (MIPv6), Multiple Care-of Address Registration (MCoA), Stream Control Transmission Protocol (SCTP), and Host Identity Protocol (HIP). Our results indicate that HIP shows best performance in all scenarios considered.**

Keywords-IPv6; mobility; multihoming; performance.

I. INTRODUCTION

Modern computing devices such as laptops, tablets, smart phones, PCs and broadband routers are typically equipped with multiple networks interfaces (e. g. , 3G, WiFi) that enable users to stay always best connected (ABC) to the Internet [1]. What *best connected* means is intimately tied to the needs of a particular user: for some, it means being connected over the interface that offers the highest data rate, while for others connectivity during movement may be more important. Such scenarios are supported by cooperation between multihoming and mobility management protocols at layer 3 (L3) and layer 2 (L2) handover mechanisms [2].

More specifically, horizontal handover allows a mobile node (MN) to change its link-layer point of attachment among networks using the same radio access technology (RAT). Similarly, vertical handover enables nodes to switch between networks based on different RATs. We will refer to these handovers as *L2 handovers* when they are transparent to L3 and above.

In certain situations, a node can be forced to reconfigure its IP address after a handover. For example, this happens when the handover occurs between networks under different administrative domains, where each domain manages its own set of network prefixes. In this situation, the handover requires assistance from L3 (i. e. , it is not longer transparent to the network layer). This type of scenario is called a *L3 handover* and is handled by mobility management protocols.

Multihoming is the ability to be simultaneously connected to multiple (home) networks. In practice, this means that each network interface is assigned an IP address from a different network, or that one interface is assigned multiple IP addresses corresponding to different networks. Benefits of multihoming include fault tolerance, load sharing, and bandwidth aggregation. The fault tolerance scenario, where communication over an unreachable network is reconfigured to go over another home network, is similar to a L3 handover. However, here we will use the term *rehoming* to emphasize that multihoming is handling this scenario.

Mobility and multihoming are generally considered as two separate concepts and thus are handled by different protocols. However, they both propose a mechanism for session survivability, which can be used to provide seamless connectivity. In our study, we focus on the performance of host-based mobility and multihoming protocols with emphasis on time to recover from link failures. The type of failures addressed here are due to node mobility or caused by stopped or failing router interfaces. Host-based mobility means that the MN is fully involved in mobility-related signaling. This is in contrast to network-based mobility, where dedicated entities are in charge of signaling and no mobility-specific features are required for MNs.

This paper is organized as follows. Section II provides an overview of several multihoming and mobility protocols (i. e. , HIP, MIPv6, SCTP, and MCoA), in terms of their modes of operation, benefits and drawbacks. Related work is described in Section III. Section IV discusses the basics of our simulation testbed and the particular simulation scenarios used here. Section V defines the performance metrics relevant to our study (i. e. , handover latency and rehoming time). Section VI elaborates on the simulation results. Finally, Section VII provides a summary and proposes future work to improve the performance of the studied multihoming and mobility protocols.

II. MOBILITY AND MULTIHOMING PROTOCOLS

This section provides an overview of IPv6 mobility and multihoming management protocols that were part of our study. Our main selection criteria was the availability of the protocol as OMNeT++ simulation model. A more comprehensive list of mobility and multihoming protocols can be found in [3]. Based on the functionality supported, each studied protocol was allocated to one of the following three categories: mobility management, multihoming management and combined multihoming-mobility management.

A. Mobility Management

The Mobile IPv6 (MIPv6) protocol was designed and incorporated in IPv6 during the base specification of IPv6, thus providing L3 integrated mobility management [4]. MIPv6 introduces a new element in the network architecture, the home agent (HA), which is responsible for maintaing communication

 ISBN: 978-1-61208-318-6

while the MN is visiting a foreign network. MIPv6 enables mobility by requiring a MN to use two addresses: the home address (HoA) and the care-of address (CoA) [5]. The HoA is a unique address from the home network address space. Its purpose is to be used as node identifier for the MN. When the MN visits a foreign network, it is assigned a CoA from the address space used by that network. The MN informs its HA whenever the CoA changes. The CoA identifies the topological location of the MN in the network graph, allowing packets to be routed to it.

Typically, a correspondent node (CN) always uses the HoA as destination address when sending data to the MN. The packets are received by the HA, which forwards them to the MN's CoA. The HA forwards also packets going in the opposite direction — from the MN to the CN. However, when both the MN and CN support route optimization, they can communicate directly using the CoA [6][7].

The strongest asset of MIPv6 is that it rests on over two decades of research and experimentation. As a result the protocol is mature and available for many platforms. Simultaneous L3 handover of the MN and CN is also supported. Some of MIPv6's drawbacks are the reliance on a third entity, the HA, high signaling overhead and some security issues related to return routability [5][8].

B. Multihoming Management

The Stream Control Transmission Protocol (SCTP) is a reliable connection-oriented layer 4 (L4) protocol developed by IETF [9]. SCTP is designed to transport Public Switched Telephone Network (PSTN) signaling messages over IP networks. However, the protocol supports a broader range of applications and features. In particular, SCTP supports multihoming, which allows the use of multiple IP addresses for a single association between two SCTP endpoints.

The SCTP association is a broader concept than the TCP connection. During association startup, SCTP provides the means for each SCTP communicating entity to provide the other entity a list of transport addresses (i. e. , multiple IP addresses in combination with an SCTP port) through which that entity can be reached and from which it will originate SCTP packets. These addresses are used as endpoints for different streams. SCTP regards each IP address of its peer as one "transmission path" towards that endpoint. The association spans transfers over all of the possible source-destination combinations that may be generated from each endpoint's list. One of the combinations is selected as initial primary path. If the primary path is considered unreliable, then the packets can be retransmitted on a backup path. Also, the primary path can be replaced with one of the backup paths [4].

Integrated multistreaming and multihoming are the main advantages of SCTP. An important drawback is that applications must be developed with specific support for SCTP (i. e. , the applications must use SCTP sockets) [10] . Consequently, old applications cannot use SCTP unless they are modified. Simultaneous rehoming is possible only for the set of addresses negotiated during association initialization.

C. Combined Multihoming-Mobility Management

Our study contains two protocols that support both mobility and multihoming. The first one, HIP, integrates both features. The second one, Multiple Care-of Address Registration (MCoA), is a multihoming extension for MIPv6.

The HIP specification introduces a new name space, the host identity name space or HIP layer, located between L3 and L4 in the TCP/IP stack [11][12]. The purpose of the HIP layer is to provide a mapping between host identifiers and IP addresses. A host identifier is the public cryptographic key from a public/private key pair that is used to uniquely identify a node. From an operational point of view it is more convenient to work with the hash of the host identifier, which is called a Host Identity Tag (HIT). Applications use HITs to open sockets to and communicate with other hosts. The IP addresses, (i. e. , the locators) are used only for routing purposes. The set of IP addresses associated with a HIT can change over time, for example due to L3 handover or rehoming. These changes are transparent to the applications above the HIP layer.

The advantages associated with HIP include integrated mobility and multihoming, low signaling overhead and transparency to legacy user-level applications [12][13][14]. Furthermore, HIP can handle simultaneous rehoming and simultaneous L3 handover.

HIP's main drawback is the introduction of a new layer to the well-established TCP/IP stack. This requires complex modifications to the operating system running on HIP nodes [8]. Also, in order to support highly mobile nodes, the system requires a rendezvous server (RVS) for location management [15].

Multihoming in MIPv6 can be supported by the MCoA extension, which allows the MN to register multiple CoAs with the HA [4][16]. As a result, the MN can maintain concurrent paths with its CNs by assigning more than one CoA to its network interfaces.

The main advantages of MCoA is that it requires relatively small changes to MIPv6 in order to enable multihoming. One drawback is that the protocol can switch to another CoA only when it detects failures in the communication between the HA and the MN, but is unable to do so for communication between the HA and the CN [17]. Another drawback is that the current specification does not state if multiple addresses can be used at the same time or if one must, for example, choose a single address based on link characteristics [4].

III. Related Work

Magagula et al. [7] discussed handover approaches used by various MIPv6-related mobility management protocols and proposed a handover coordination mechanism based on Proxy Mobile IPv6 (PMIPv6) [18]. The authors used ns-2 simulations to show that their proposed mechanism was more successful than plain PMIPv6 and Mobile IPv6 fast handovers (FMIPv6) [19] in decreasing the handover delay and the packet losses.

Zekri et al. [2] highlighted some of the main technical challenges in providing seamless vertical handover in heterogeneous wireless networks. The article provides a survey on the vertical mobility management process and mainly focuses on decision-making mechanisms. The authors also point out the main research trends and challenges, such as enhancing network availability and QoS, green networking, and solutions for healthcare applications. The main challenges discussed deal with the coexistence of heterogeneous wireless networks.

A comprehensive survey of protocols supporting end-host as well as site multihoming can be found in [4]. The evaluation of multihoming solutions provided there is based on the degree of fulfillment of multihoming goals (i. e. , resilience,

 ISBN: 978-1-61208-318-6

ubiquity, load sharing, and flow distribution). The authors did not explicitly point out the best or worst protocols in terms of performance, but instead they illustrated that each protocol comes with its own advantages and drawbacks. Additionally, they argued that an efficient multihoming protocol cannot be coupled with a single layer, but instead it must be the result of cooperation between multiple layers that act in a concerted manner to meet the same goals. From an end-site perspective, multihoming proposals should not focus only on routing scalability. Instead, they should incorporate native support for the diverse multihoming goals rather than relying on extensions.

In [6], Jokela et al. compared the handover performance of MIPv6 and HIP in a heterogeneous IPv6 network environment. They configured a network environment consisting of a wireless 802.11b network as well as a GPRS network. In their experiment, the MN received a stream of TCP data from a server while performing handover between the two networks. Their measurement results show that the recovery time was 8.05 s for MIPv6 and 2.46 s for HIP.

Ratola et al. [8] compared MIPv6, HIP, and SCTP in terms of architecture, security, and known problems. The purpose of their comparison was to determine which layer (L3, L3.5, or L5) would be best suited for mobility. Based on their comparison, the authors suggest that mobility should be implemented in a new layer between the network and transport layers. In this respect, HIP seems to be a good L3.5 solution for mobility that solves several security, mobility, and multihoming issues at the same time.

Dhraief et al. [20] proposed a novel framework, called MIPSHIM6, that combines SHIM6 [21] and MIPv6, in order to enable both host mobility and host multihoming. In MIPSHIM6, the mobility management is delegated to MIPv6 and the multihoming management to SHIM6. The authors evaluated this framework on a real testbed. They setup an experiment where a MN boots up in a foreign network, binds with its HA and initiates a secure copy (scp) session with a CN. During the next step, the MN establishes a SHIM6 context with the CN . The authors arranged for a HA failure to occur 60 s after the scp session was started. At that point the MN rehomes to the path defined by the SHIM6 context. Unfortunately, there is no data in the paper to indicate how well this solution performs in terms of rehoming time. The TCP throughput plot shown in the paper indicates that it takes 10–15 s for the TCP throughput to increase to the level before the HA failure.

IV. Testbed and Simulation Scenarios

Our performance study was conducted under the OMNeT++ simulation environment. OMNeT++ is a modular, discrete-event simulation framework based on the C++ programming language [22]. It can be used for modeling wired and wireless communication networks, protocols, multiprocessors, distributed or parallel systems, queuing networks and for validating hardware architectures. OMNeT++ is open-source, and it can be used either under the GNU General Public License or under its own license that also makes the software free for non-profit use [23].

We have chosen OMNeT++ because it has an extensive array of modules required by our study, such as HIPSim++ [24] for HIP, the SCTP module [25] from the INET framework, MCoA++ [26] for MCoA and xMIPv6 [27] for MIPv6. The mobility and multihoming features supported by each protocol are summarized in Table I. Note that mobility support in MCoA++ is provided through the xMIPv6 module.

TABLE I: Multihoming and mobility management protocols

Protocol	Mobility	Multihoming
SCTP	No	Yes
MIPv6	Yes	No
MCoA	Yes	Yes
HIP	Yes	Yes

To evaluate the performance of the protocols described in Section II we designed five simulation scenarios: two for mobility and the remaining three for multihoming. The mobility scenarios investigate the handover latency experienced in the case when the MN is using MIPv6 and HIP, respectively. The multihoming scenarios investigate the rehoming time when the host is using HIP, MCoA, and SCTP, respectively.

A. Mobility Scenario for MIPv6

The simulated network topology for this scenario is shown in Figure 1. The rectangle in the background depicts a 850 m by 850 m movement area available for mobile nodes.

The home access point `AP_Home` is connected to the router `Home_Agent` that plays the role of the home agent. Together, they define the home network. The foreign network consists of the foreign access point `AP_1` that is attached to the router `R_1` acting as foreign agent. The coverage areas for `AP_Home` and `AP_1` are overlapped at the boundaries to allow for continuous wireless connectivity. There is approximately 300 m between `AP_Home` and `AP_1`. The bit rate for the backbone links connecting `R_2` to `Home_Agent` and `AP_1` to `R_1` is configured to 1 Gbps. The links between the access points and respective routers are configured as 100 Mbps Ethernet.

The MN is programmed to move from its home network to the foreign network in a straight line at a speed of 1 m/s, resembling a moving pedestrian scenario. The router advertisement (RA) message interval is set to a random number in the range 0.03–0.07 s.

During the simulation, the CN sends every 50 ms a ping packet (i. e. , a ICMP echo message) to the MN. The MN replies to each ping with a ICMP echo reply message. This represents background traffic.

We have configured all MIPv6 nodes to use route optimization, thus avoiding to forward traffic through `Home_Agent`.

B. Mobility Scenario for HIP

The simulated network topology for this scenario is shown in Figure 2. The topology is identical to the one described in Section IV-A with the exception of two additional nodes: the RVS host and the DNS server denoted by `rvs` and `dnssrv`, respectively. The RVS host is a HIP node that allows the MNs to store their actual HIT-to-IP address associations and to make them available to potential communication partners. The DNS server resolves domain names to HITs and IP addresses and also provides RVS information for mobile HIP hosts.

Similar to the MIPv6 scenario, the MN moves from the home network to the foreign network at a constant speed of

 ISBN: 978-1-61208-318-6

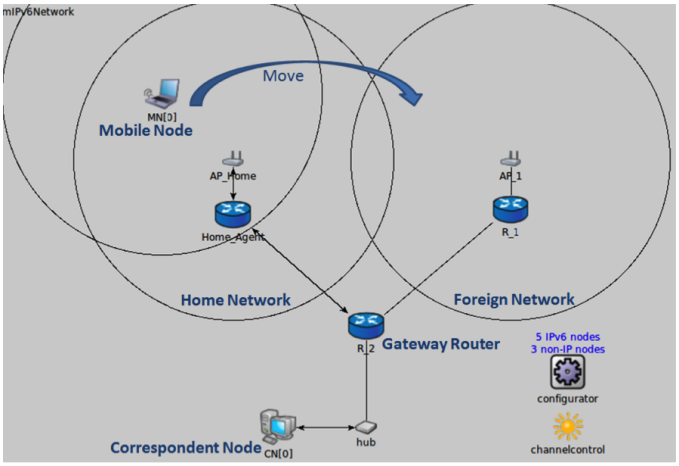

Figure 1: Simulation environment for MIPv6 and MCoA scenarios

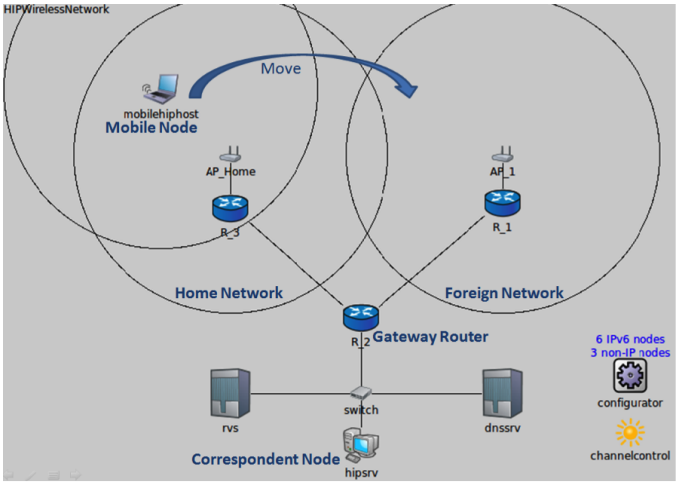

Figure 2: Simulation environment for HIP scenarios

1 m/s. At the start of the simulation, a HIP association is established between the MN and CN. After the association is successfully established, an IPSec Security Association pair is created between MN and CN. At this point, the MN starts to send to the stationary CN (*hipsrv*) one UDP ping request every 50 ms. The reason for using UDP pings is that it was not possible to get the ICMP ping module to work in HIPSim++. We have configured the size of the UDP ping packets to be equal to that of ICMP ping packets and have no reason to suspect any noticeable impact on the simulation results.

MN's movement towards the edge of the home network eventually results in a handover that enables the MN to associate with the foreign access point.

C. Multihoming Scenario for HIP

The topology used here is similar to the one shown in Figure 2, which was used for the HIP mobility scenario. The difference is that in this scenario the MN is equipped with an additional wireless network interface. Our intention is that this scenario should resemble a situation where the MN can

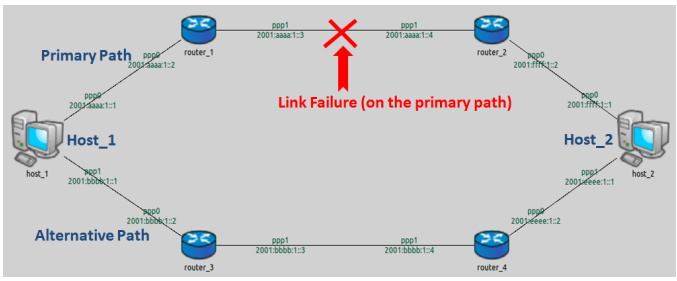

Figure 3: Simulation environment for SCTP

connect to a CN over the (preferred) WiFi interface denoted here by `IF_WiFi` and fallback on the 3G interface, `IF_3G`, when it loses the WiFi connection.

While the MN moves towards the edge of its home network, the signal strength from the home access point `AP_Home` becomes weaker, causing the node to scan for new access points on both its interfaces. We have arranged so that the MN is unable to find another access point over `IF_WiFi`. At some point, the MN will receive the beacon signal from `AP_1` over `IF_3G` and will rehome to the foreign network reachable over the 3G interface.

As explained before, a UDP ping session is established from the MN to the CN. The RA interval is set to a random value between 0.03 s and 0.07 s. The MN is moving away from the home access point at a constant speed of 1 m/s.

D. Multihoming Scenario for MCoA

The MCoA multihoming network topology is similar to the one for MIPv6 shown in Figure 1. The MN is configured to use two interfaces, `IF_WiFi` and `IF_3G`, as explained in the previous section.

The MN is sending every 50 ms an ICMP Echo message to the CN, while moving at speed of 1 m/s.

E. Multihoming Scenario for SCTP

The network topology used to investigate the multihoming capability of SCTP protocol is shown in Figure 3. The SCTP hosts are equipped with two interfaces.

Because SCTP does not have mobility support and also because its mobile extension, mSCTP [28], is not yet available for OMNeT++, we have configured all nodes to use wired interfaces. Therefore, we only tested the multihoming ability of SCTP for data transfer between two stationary hosts.

The links between the routers, `router_1`, `router_2`, `router_3`, and `router_4` form the core network. All these links are configured for 1 Gbps data rate. The Ethernet interfaces of the hosts are configured to use a data rate of 100 Mbps.

The simulation setup aims to study the fault tolerance feature of SCTP when a link on the primary path fails at a random time during data exchange between the hosts. We configured `Host_1` to transfer 10 MB of data to `Host_2`, such that `Host_1` acts as the client and `Host_2` as the server. The size of the transfered data is a tradeoff between keeping the simulation time short and having a long time range where the failure event can occur.

 ISBN: 978-1-61208-318-6

After the endpoints establish a SCTP association, the path consisting of routers `router_1` and `router_2`, is designated as the primary path and the path using the remaining routers, `router_3` and `router_4`, is designated as the alternative path. We have arranged for a link failure to occur on the primary path between `router_1` and `router_2`. The failure event occurs at a time drawn from a uniform distribution between 5.3 s and 7.5 s. This range is well within the time window required to transfer the 10 MB file. The link failure is detected by SCTP, which then redirects the communication through the alternative path.

V. Simulation Metrics

In terms of performance metrics, we measured the rehoming time for multihoming protocols and handover latency for mobility protocols, respectively. For HIP, which supports both multihoming and mobility [13], we collected statistics for both metrics.

A. Handover latency

We define the *MIPv6 handover latency* as the elapsed time between the moment when the MN disassociates from the old access point and the instant when the MN receives the binding acknowledgement (BA) message from the CN [3]. The BA message is sent from the CN to the MN when route optimization is used. Its purpose is to confirm registration of the new CoA. This metric is composed of the following delay components: L2 handover, router discovery, duplicate address detection, home registration, return routability, and correspondent node registration [5][27].

In the case of HIP, every time a HIP-enabled MN changes address it notifies the CN through a sequence of three UPDATE messages. Thus, we define the *HIP handover latency* as the time elapsed from the moment when the MN disassociates from the old access point and until the MN sends out the third UPDATE packet while connected to the new access point [3]. The latency consists of the following delay components: L2 handover, router discovery, duplicate address detection, and peer notification of IP address change (by exchanging three UPDATE messages with the CN).

B. Rehoming time

For a multihomed mobile node with two interfaces, the onset of rehoming is triggered when the MN comes out of range of the old access point, which is connected through the first interface. We therefore define the *HIP rehoming time* as the interval from the moment when the MN starts scanning for the new access point on the second interface until it sends the third UPDATE packet while connected to it. The HIP rehoming time computed this way includes the delays due to L2 handover, configuration of new IPv6 address and HIP update message procedures.

In MCoA++, multihomed MNs use both interfaces simultaneously. When the MN detects a signal from a new access point, it immediately sets up a connection with the new access point via the second interface, which is assigned a new IPv6 address. In our simulation scenario, the ICMP echo requests are sent over the MN's old interface and the replies are received over the new interface. We define the *MCoA rehoming time* as the time elapsed from the moment the MN starts scanning for the new access point over the second interface to the time when the MN receives the BA. The MCoA rehoming time consists of L2 handover, configuration the new of IPv6 address and MCoA signaling procedures.

The *SCTP rehoming time* is defined as the time elapsed between the instant when a failure occurs on the primary path until the moment when data is exchanged on the alternative path.

TABLE II: Performance results with 95% confidence interval

Protocol	Handover latency (s)	Rehoming time (s)
SCTP	N/A	0.99 ± 0.0100
MIPv6	3.32 ± 0.0880	N/A
MCoA	3.32 ± 0.0880	1.66 ± 0.0909
HIP	2.27 ± 0.0922	0.41 ± 0.0004

VI. Performance Results and Analysis

In this section, we present the performance results from our results and share some reflections related to them. Table II shows the statistical mean values for handover latency and rehoming observed in our simulations. We provide also the corresponding 95% confidence intervals. Note that MCoA is a multihoming extension of MIPv6, where the mobility performance of MCoA is similar to that of MIPv6.

Looking at simulation results from the mobility scenarios we can observe that the HIP protocol has an average handover latency of 2.27 s compared to 3.32 s for MIPv6. The higher latency for MIPv6 can be explained by its long signaling phase. In our experiments, MIPv6 required 1.038 s to complete signaling, which is 1 s higher than the time required for HIP signaling. HIP signaling consists of only 3 UPDATE messages exchanged between the MN and CN. In contrast, MIPv6 signaling requires 8 messages, some exchanged between the MN and HA and some between the MN and CN

For multihoming protocols, the results indicate that HIP again has the best performance in terms of the lowest average rehoming time of 413 ms. This is less than half of the SCTP rehoming time (992 ms) and almost a quarter of the MCoA rehoming time (1656 ms). The main reason behind the high performance shown by HIP is proactive IPv6 address configuration. This means that the MN establishes and configures a new IPv6 address on `IF_3G` before it breaks the connection to the home network, hence, performing a soft handover (make-before-brake). When rehoming takes place, it does only a L2 handover followed by HIP signaling, resulting in a very low latency. On the other hand, the rehoming time for MCoA includes L2 handover delay, IPv6 address configuration delay and MCoA signaling latency. The address configuration delay is in fact the largest contributor to the MCoA rehoming time.

VII. Conclusion and Future Work

Our simulation results indicate that HIP has the best performance in both the multihoming and the mobility scenarios. The main reason is HIP's low signaling overhead during handovers and rehoming events. Moreover, HIP implements soft handovers during rehoming events, which decreases the rehoming time by a large factor.

We think that the results presented in this paper indicate that HIP is a suitable component for providing seamless connectivity to mobile and multihomed nodes.

 ISBN: 978-1-61208-318-6

Our future work in the short term will focus on developing missing simulation models for OMNeT++, for protocols such as SHIM6 [4] and mSCTP. This will allow us to extend our current work into a more complete performance analysis of mobility and multihoming protocols. For the longer term, we look forward towards improving the performance of the existing multihoming and mobility protocols.

ACKNOWLEDGMENT

Special thanks go to Dr. Kostas Pentikousis and Mr. Bruno Sousa for their assistance and technical help they provided during our simulations with MCoA.

REFERENCES

[1] E. Gustafsson and A. Jonsson, "Always best connected," IEEE Wireless Communications Magazine, Feb. 2003, pp. 49–55.

[2] M. Zekri, B. Jouaber, and D. Zeghlache, "A review on mobility management and vertical handover solutions over heterogeneous wireless networks," Computer Communications, vol. 35, no. 17, Oct. 2012, pp. 2055–2068.

[3] C. Mugga and D. Sun, "A solution combining both multihoming and mobility in IPv6 heterogeneous environment," Master's thesis, Blekinge Institute of Technology (BTH), Karlskrona, Sweden, Sep. 2013, MEE: 10035.

[4] B. Sousa, K. Pentikousis, and M. Curado, "Multihoming management for future networks," Mobile Networks and Applications, vol. 16, no. 4, Aug. 2011, pp. 505–517.

[5] C. E. Perkins, D. B. Johnson, and J. Arkko, RFC 6275: Mobility Support in IPv6, IETF, Jul. 2011. [Online]. Available: http://tools.ietf.org/html/rfc6275 [retrieved: Dec., 2013]

[6] P. Jokela, T. Rinta-aho, T. Jokikyyny, J. Wall, M. Kuparinen, H. Mahkonen, J. Meln, T. Kauppinen, and J. Kauppinen, "Handover performance with HIP and MIPv6," in Proceedings of Wireless Communication Systems, Mauritius, Sep. 2004, pp. 324–328.

[7] L. A. Magagula, H. A. Chan, and O. E. Falowo, "Handover approaches for seamless mobility management in next generation wireless networks," Wireless Communications and Mobile Computing, vol. 12, no. 16, Nov. 2012, pp. 1414–1428.

[8] M. Ratola, "Which layer for mobility? - comparing mobile IPv6, HIP and SCTP," in HUT T-110-551 Seminar on Internetworking. Sjökulla, Finland: Helsinki University of Technology, Apr. 2004.

[9] R. R. Stewart, RFC 4960: Stream Control Transmission Protocol, IETF, Sep. 2007. [Online]. Available: http://tools.ietf.org/html/rfc4960 [retrieved: Dec., 2013]

[10] A. Dhraief, T. Ropitault, and N. Montavont, "Mobility and multihoming management and strategies," in 14th Eunice Open European Summer School, Brest, France, Sep. 2008.

[11] R. Moskowitz, P. Nikander, P. Jokela, and T. R. Henderson, RFC 5201: Host Identity Protocol, IETF, Apr. 2008. [Online]. Available: http://tools.ietf.org/html/rfc5201 [retrieved: Dec., 2013]

[12] P. Nikander, A. Gurtov, and T. R. Henderson, "Host identity protocol (HIP): Connectivity, mobility, multi-homing, security, and privacy over IPv4 and IPv6 networks," IEEE Communications Surveys and Tutorials, vol. 12, no. 2, Second Quarter 2010 2010, pp. 186–204.

[13] P. Nikander, T. R. Henderson, C. Vogt, and J. Arkko, RFC 5206: HIP Mobility and Multihoming, IETF, Apr. 2008. [Online]. Available: http://tools.ietf.org/html/rfc5206 [retrieved: Dec., 2013]

[14] T. R. Henderson, P. Nikander, and M. Komu, RFC 5338: Using the Host Identity Protocol with Legacy Applications, IETF, Sep. 2008. [Online]. Available: https://tools.ietf.org/html/rfc5338 [retrieved: Dec., 2013]

[15] J. Laganier and L. Eggert, RFC 5204: Host Identity Protocol (HIP) Rendezvous Extension, IETF, Apr. 2008. [Online]. Available: http://tools.ietf.org/html/rfc5204 [retrieved: Dec., 2013]

[16] R. Wakikawa, V. Devarapalli, G. Tsirtsis, T. Ernst, and K. Nagami, RFC 5648: Multiple Care-of Addresses Registration, IETF, Oct. 2009. [Online]. Available: http://tools.ietf.org/html/rfc5648 [retrieved: Dec, 2013]

[17] A. Dhraief and A. Belghith, "Suitability analysis of mobility and multihoming unification," in Proceedings of ICWUS, Sousse, Tunisia, Oct. 2010, pp. 1–6.

[18] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, RFC 5213: Proxy Mobile IPv6, IETF, Aug. 2008. [Online]. Available: http:// tools.ietf.org/html/rfc5213 [retrieved: Dec., 2013]

[19] R. Koodli, RFC 5568: Mobile IPv6 Fast Handovers, IETF, Jul. 2009. [Online]. Available: http://tools.ietf.org/search/rfc5568 [retrieved: {Dec., 2013}]

[20] A. Dhraief, I. Mabrouki, and A. Belghith, "A service-oriented framework for mobility and multihoming support," in Proceedings of MELECON, Medina Yasmine Hammamet, Tunisa, Mar. 2012, pp. 489–493.

[21] A. García-Martnez, M. Bagnulo, and l. van Beijnum, "The shim6 architecture for ipv6 multihoming," IEEE Communications Magazine, vol. 48, no. 9, Sep. 2010, pp. 152–157.

[22] A. Varga and R. Hornig. OMNeT++ community site. [Online]. Available: http://www.omnetpp.org [retrieved: Dec., 2013]

[23] ——, "An overview of the OMNeT++ simulation environment," in Proceedings of Simutools, Marseille, France, Mar. 2008, pp. 1–10.

[24] L. Bokor. HIPSim++: A host identity protocol (HIP) simulation framework for INET/OMNeT++. [Online]. Available: http://www.ict-optimix.eu/index.php/HIPSim [retrieved: Aug., 2013]

[25] I. Rüngeler, M. Tüxen, and E. P. Rathgeb, "Integration of SCTP in the OMNeT++ simulation environment," in Proceedings of Simutools, Marseille, France, Mar. 2008, pp. 1–8.

[26] B. Sousa, M. Silva, K. Pentikousis, and M. Curado, "A multiple care of address model," in Proceedings of Computers and Communications, Kerkyra, Greece, Jun. 2011, pp. 1–6.

[27] F. Z. Yousaf, C. Bauer, and C. Wietfeld, "An accurate and extensible mobile IPv6 (xMIPV6) simulation model for OMNeT++," in Proceedings of Simutools, Marseille, France, Mar. 2008, pp. 1–8.

[28] S. J. Koh, Q. Xie, and S. D. Park, Mobile SCTP (mSCTP) for IP Handover Support, IETF, Oct. 2005, draft-sjkoh-msctp-01.txt.

 ISBN: 978-1-61208-318-6