An ILNP-Based Solution for Future Heterogeneous Wireless Networks

Musab Muhammad Isah, Christopher Edwards
School of Computing and Communications,
Infolab 21, Lancaster University,
Lancaster, UK.
Email: m.isah@lancaster.ac.uk, c.edwards@lancaster.ac.uk

***Abstract*— Utilization of the different wireless interfaces (Cellular, Wi-Fi and WiMAX) that come with many of the Mobile Nodes today is central to improving Quality of Experience and Quality of Service in future networks. Although the interfaces are of different technologies as are the access links, the core/backbone networks are now based on IP infrastructure. Efforts to simplify network handover between these technologies – termed vertical handover (VHO) – have not been successful with IP due its mechanism for managing nodes' identity and location. Researchers have defined and implemented some solutions that proposed the separation of identity of a Mobile Node from its location, and among those proposals is the *Identifier Locator Network Protocol* (ILNP). In this work, we propose a Linux-based implementation of the ILNPv6 protocol – an instance of the ILNP that is compatible with IPv6 – on laboratory testbed. We also proposed an Information Server managing a defined geographical location we called AREA, to augment some of the shortfalls that we observed with ILNP. We believe that this combination provides the necessary ground for achieving seamless VHO in heterogeneous wireless environments of the future.**

Keywords—Locator Identifier Split; Identifier Locator Network Protocol (ILNP); Vertical Handover; Heterogeneous Wireless Networks; MIP; Information Server (IS); Mobility

I. INTRODUCTION

According Cisco Visual Networking Index, 2013 [1], the average smartphone usage grew to 81 percent and represented 92 percent of global mobile traffic in the year 2012. These smartphones come with atleast two interfaces, and the report shows that 33 percent of the total traffic was offloaded (*Offloading* is a technique of moving traffic flows from one wireless interface of a device to another) from Cellular to Wi-Fi or Femtocell network signifying the importance of utilizing the different interfaces. The proliferation of multi-interface *Mobile Nodes* (MN) is posing new challenges and opportunities to the wireless networks of today especially in enabling seamless VHO. In the near future, MNs will need to switch ongoing voice or data sessions between their heterogeneous interfaces. Achieving seamless VHO is essential to improve the *Quality of Experience* (QoE) from the users' perspective, and *Quality of Service* (QoS) on the side of the providers especially in locations with several network *Point of Attachments* (PoA). The users expect to have an *Always Best Connected* (ABC) [2] service, i.e the best possible connection to support applications in use, and remain globally reachable, anytime, anywhere. Actualizing this ABC paradigm, to a large extent, depends on the ability to utilize all the available wireless technologies in any particular area at a time. With the 3 popular wireless technologies – Cellular, Wi-Fi and WiMAX – tending towards IP-based core networks (Wi-Fi networks have always been IP-based), the communication protocols in use need to be able to efficiently handle and utilize Internet connectivity provided by the different interfaces in a multi-technology environment.

What makes it difficult to switch between these interfaces, even though they may all be connected to the Internet, has to do with 'session continuity'. Transport-layer session states are identified using sockets; a combination of source and destination IP addresses, application port number of the transport protocol in use, and an ephemeral port number chosen by the source device protocol stack. The implication of having these sockets is that as soon as any of the IP addresses changes because of a change in PoA (or for any other reason), that session has to be discarded and another one initiated with the new IP address. To efficiently solve this problem, changes have to be made in the network and transport layers to impact the way sockets are formed on the stack. The transport layer sessions have to be maintained independent of any change of location of the MN during the session's lifetime to ensure continuous end-to-end connectivity.

In trying to solve the session continuity problem, and other shortcomings identified with the current IP addressing architecture, network layer approaches generally termed '*Locator Identifier* (Loc/ID) split' have been proposed to change the way the IP addresses are used at the network and transport layers of the TCP/IP protocol stack. In the Loc/ID split field, the dual role of IP address (identifying and locating a node) is decoupled to form a separate *Locator* for determining MN's position on a network and an *Identifier* to provide a (unique) identity for the node. This is necessary in mobile environments to ensure session continuity when an MN moves from one network (Location) to another. One such Loc/ID mechanism is the *Identifier Locator Network Protocol* (ILNP), which forms the basis of this paper. The protocol supports mobility by design, which is significant in enabling seamless VHO between different wireless access technologies. This paper presents a proposed ILNP implementation to demonstrate how the protocol, with

This research is funded by Petroleum Technology Development Fund (PTDF), Nigeria. Reference *PTDF/E/OSS/PHD/IMM/500/11*

support from an IS, enables VHO in a heterogeneous wireless environment.

The rest of this paper is arranged as follows: section II presents the related work in the area of Loc/ID Split focusing on 3 different approaches. Section III is an overview of ILNP and how it compares to IP. Section IV discusses the mobility issues hindering the actualization of seamless VHO in today's networks and how our ILNP-based solution is set to tackle them. This is then followed by Discussion, Future Work and Conclusion.

II. Related Work

There are several efforts in the research community, apart from ILNP, which are aimed at decoupling the dual role of identifying and locating a node using a single IP address. The solutions can be broadly classified as *Map-and-Encapsulate*, such as *Mobile IP* (MIP), *Locator/ID Separation Protocol* (LISP) and *Host Identity Protocol* (HIP) or Address Rewriting, such as GLI Split, *Six/One Router* and ILNP[1]. Although one may argue that MIP (and the several extensions) is not a Loc/ID split mechanism because both the *Home Address* (HoA) and the *Care of Address* (CoA) are use at some points for routing, it is nevertheless, about the only mobility solution on the Internet that has some deployments on live networks.

A. Mobile IPv6 (MIPv6) and extensions

Mobile IP comes in two major variants, MIP [3] for IPv4 network, and MIPv6 [4] for IPv6. The main idea behind the development of the protocol is to allow location-independent routing so that MNs can be reached irrespective of their current location on the Internet. MIPv6 (and MIP) uses the concept of HoA acquired from a *Home Agent* (HA, or through other means) by an MN for locating and identifying the node while on *Home Network* (HN). When the MN moves to *a Foreign Network* (FN), it configures a CoA (to serve as its new *Locator*) and sends a *Binding Update* (BU) to its HN for the HA to bind the MN's HoA with the CoA.

A packet destined to the MN is sent to the HN, and the HA intercepts and tunnels the packet using the MN's CoA to the FN. Replies can be sent directly to the *Corresponding Node* (CN) by the MN with no recourse to the HA. Subsequent message exchanges can be achieved directly between the MN and the CN if the *Route Optimization* feature of the IPv6 protocol is utilized. The standard handover procedure with MIPv6 involves *Movement Detection*, CoA configuration and BU.

Several extensions for MIPv6 were developed to improve these standard procedures and for the protocol to work in different scenarios, including *Hierarchical Mobile IPv6* (HMIPv6) [5]; *Fast Mobile IPv6* (FMIPv6) [6]; *Proxy Mobile IPv6* (PMIPv6) [7]; and the NEtwork MObility (NEMO) protocol [8].

[1] Address rewriting is not necessary with ILNP but may be introduced for the purpose of Traffic Engineering (TE), Network Mobility or site Multihoming

Mobile IP and its extensions have not seen wide deployment as hoped by the designers of the protocol despite the soaring number of mobile devices in use today. One of the reasons is the complexity of the protocols as the original IP was designed to handle static end points; hence mobility is not achieved by design but an added feature. There is also the problem of scalability with the protocols as global mobility solutions.

B. Locator/ID Separation Protocol (LISP) Mobile Node

LISP MN [9] is an approach defined to enable mobility with the LISP protocol [10]. An MN is equipped with Ingress/Egress Tunnel Router's (ITR/ETR, i.e border router's) functionality. The MN uses a centralized mobility anchor in the form of a *Map-Server* (MS) which advertises the *Endpoint Identifier* (EID) prefix that covers the MN's EID - the Node Identity (NI) - and enables the roaming node to be discovered. The MN acquires this EID from a block reserved for MNs much in the same way that numbers are allocated to mobile phones. Once an MN moves to a new network, it obtains a new *Routing Locator* (or RLOC, which determines the position of a node on the global network) and registers with the connected network. It updates the MS with its new RLOC to ensure that up to date EID-to-RLOC mapping is published on the *Mapping System* in use (LISP ALT/NERD/DDT/CONS etc) and all correspondence, henceforth, is established using the new RLOC.

LISP requires each MN to have an RLOC, which is mapped to the node's EID by the MS. The Mapping System is an added level of indirection on the Internet, and with the high rise in mobile devices, as shown in [1], each needing an RLOC to be mobile on a LISP network, the protocol is not likely to scale. And because mobility in LISP is not by design, it is likely to have the same complexity in deployment as the MIP.

C. Host Identity Protocol (HIP)

HIP [11] is a host-based Loc/ID split mechanism that introduces a new namespace, *Host Identifier* (HI), a sub-layer between Network and Transport layers of the TCP/IP protocol stack. HI is a public cryptographic key from a public/private key pair, and is usually represented by a 128-bit one-way hash of itself called *Host Identity Tag* (HIT) in the form of an IPv6 address. HIT is used to identify a device rather than an interface on the device and the host that provides the private key pair during *Base Exchange* (session initiation) proves ownership of the HI. The IP address at the network layer is used for routing purposes and the HIT is used by the transport and other upper layer protocols.

Base Exchange is a four-way handshake between the two communicating nodes and is mandated in the protocol to initiate communication. The mapping between the HITs and IP addresses is provided using a *RendezVouS Server* (RVS), and, using a HIP UPDATE message, an MN updates the RVS and the CN every time its IP address changes due to movement [12]. The DNS can serve as the RVS and may be used by the initiator of the communication to resolve the responder's FQDN (*Fully Qualified Domain Name*) to its HIT and IP address. Alternatively, the DNS may provide

responder's HIT and IP address of the RVS serving the *responder*.

The problem with using HIT is that an MN loses its identity with a change in its public/private key pair, and a loss or compromise of the key would force a change in the pair. HIP also requires the use of RVS for optimum performance which introduces another level of indirection on the Internet. HIP protocol does not support network mobility.

III. OVERVIEW OF ILNP

ILNP [13] is a protocol that proposes the replacement of the 128 bits IPv6 address with two distinct namespaces, *Locator* 'L' and *Identifier* 'I' (as NI). The values of *Locator* and *Identifier* together form what is known as *Identifier-Locator Vector* (I-Lv), an IPv6 address equivalent. The *Locator* serves as the name of a single IP sub-network and not any specific host on the network. It is 64 bits in size and analogous to the address prefix for routing in IPv6. The unique *Identifier* (uniqueness can be globally/locally scoped) is derived from the MAC address of the MN's interface (although use of other means to generate the *Identifier* is not precluded) in the form of IEEE *Extended Unique Identifier* (EUI) 64 address [14].

The EUI, in ILNP, identifies an MN and not a single interface on the device. An MN may have and use more than one *Identifier* and/or *Locator* at a time, but any transport layer session must maintain a single *Identifier* throughout the lifetime of the session. All layers above the network will only use the *Identifier* or the FQDN in forming transport and application layer sessions respectively as shown in Table III.1.

Layer	**IP**	**ILNP**
Application	FQDN and IP Addresses	FQDN
Transport	IP address	Identifier
Network	IP address	Locator
Physical Interface	IP address	MAC address

Table III.1 IP vs ILNP address usage on TCP/IP protocol stack

ILNP uses DNS as the rendezvous server to provide mapping of *Locator*(s)-to-*Identifier*(s). A single query to the DNS by the MN using the FQDN of the CN would yield the *Identifier* and the *Locator*(s) of the CN - the *mapping* only needs to be stored on the DNS if the CN is configured to provide a service. The MN uses the *Secure Dynamic DNS Update* [15] to update the DNS about its current location every time it changes a *Locator*. As a performance enhancement, ICMP *Locator Update* (LU) [16] message is defined in the protocol, and is sent as a notification of *Locator* change from the MN to the CN.

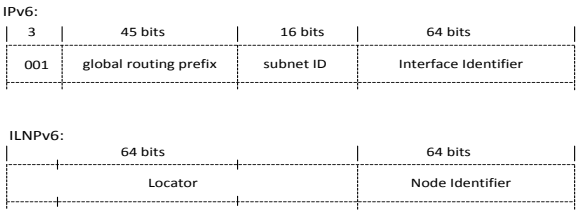

Figure III.1 A comparison of IPv6 and ILNPv6 address formats

ILNPv6 is an instance of ILNP protocol that is backward compatible with IPv6; Figure III.1 compares IPv6 and ILNPv6 address formats. Both protocols use the high-order 64 bits for routing purposes albeit in a different way, but the low-order 64 bits identifies a node with ILNPv6 and an interface with IPv6. ILNP was not designed only to solve mobility issues but also claims to solve the problems observed with the routing architecture by the IRTF RRG (Routing Research Group). The group, after studying the several Loc/ID split proposals submitted to it, states its reasons for recommending ILNP[2] to the IETF in RFC 6115 [17]:

"*We recommended ILNP because we find it to be a clean solution for the architecture. It separates location from identity in a clear, straightforward way that is consistent with the remainder of the Internet architecture and makes both first-class citizens. Unlike the many map-and-encap proposals, there are no complications due to tunneling, indirection, or semantics that shift over the lifetime of a packet's delivery*".

IV. ILNP-BASED SOLUTION

A. Mobility Issues

One of the obvious challenges in harmonizing mobility between the different wireless technologies is the use of different mobility protocols. Although the entire network protocols standardized for use in these technologies, with the exception of GTP (GPRS Tunneling Protocol [18]), are based on the IP architecture, they use different mechanisms of operation. The cellular operators in particular have stuck to network-based mobility mechanisms (especially the GTP and the PMIP) to ensure that mobility is transparent to the MN. Although this has worked over the years, one can argue that it gives no choice whatsoever to the subscriber, who in the near future would need to participate in mobility decision by being able to choose an access network of the available links in a particular environment, which is vital in realizing the ABC dream. Centralizing heterogeneous mobility with PMIP is problematic as it introduces a single point of failure (the *Local Mobility Anchor* (LMA)) in a domain. GTP use, on the other hand, is restricted to cellular networks alone.

Apart from unifying the different access networks to use a similar mobility protocol, it is necessary for the protocol to support both the network-based and host-based mobility operations and allows both to be used interchangeably or concurrently when the need arises. Another factor hindering heterogeneous mobility is the use of IP address to identify an interface rather than the node itself. Although MIP and its several extensions may provide session continuity by separating location (CoA) from Identity (HoA), a change in interface means a change in identity; hence, a loss in connectivity.

We believe ILNP is the ideal choice because of its crisp handling of *Identifiers* and *Locators* and utilizing the reliable DNS as the *Mapping System* rather than introducing a new

[2] The Group also recommends two other solutions for routing architecture: *Evolution* and Automating *Renumbering*

system as required in LISP [10] and HIP [11] protocols. For Cellular and WiMAX networks, ILNP can handle *network-based* mobility by providing all zeros *Locator* value in a *Router Advert* sent to the MN and rewriting the source *Locator* part of the outbound packets at the gateways, obviating the need for the MN to update its location. *Client-based* mobility is also supported by providing the *Locator* value in the *Router Advert*, enabling the MN to update its location on the network with the DNS and/or the CN. ILNPv6 is fully compatible with IPv6 and can be used in Wi-Fi networks as a direct replacement of the latter. This also allows for dual stack approach – allowing IPv4 nodes on ILNPv6 network – for incremental deployment.

The issue of the IP address being bound to an Interface does not exist with ILNP as NI identifies the node itself and not any of its interface(s). ILNP does not have an additional overhead on its packet header as do LISP and HIP; both protocols use 128 bits for *Identifier* and 128 bits for *Locator*, as opposed to ILNP's 128 bits for the two namespaces.

B. The Solution

The proposed solution involves developing the ILNPv6 protocol on Linux/x86 systems as only one implementation [19] is available on this platform – a FreeBSD/x86 research demonstration implementation is available from St Andrews University [20]. A network consisting of an ILNPv6-enabled MN and CN, a DNS server, and ILNP-aware Gateways, would be implemented on a testbed to monitor the effects of changing *Locators* as MN moves across an area as shown in Figure V.1. The basis for comparison would be an MIPv6 network.

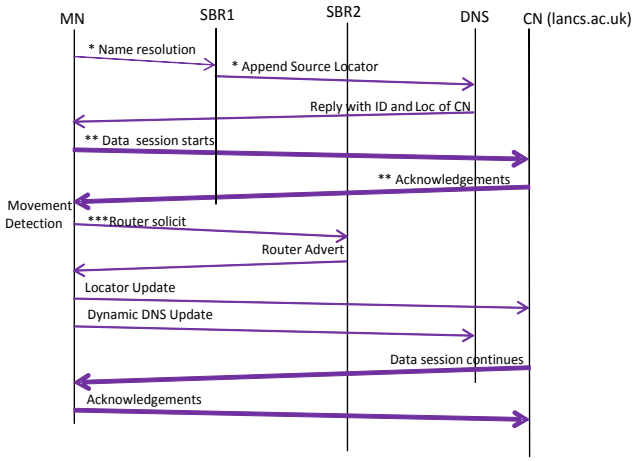

Figure IV.1 ILNP session establishment and Handover

* MN initiates a DNS name resolution for the CN's (*lancs.ac.uk*) NI and *Locator* using the MN's NI as source *Identifier* and zeros in source *Locator* field. SBR1 intercepts the packet and appends the *Locator* in the source field and forwards the query to the DNS. In a situation where the MN is provided with the source *Locator* prior, it completes the packet before sending it directly to the DNS.
** As soon as the DNS provides the *Identifier* and the *Locator* values of the CN, data session is established in the same way as the conventional TCP/IP would, the TCP 3-way handshake to the webserver in this instance. An ILNP nonce is used by the nodes in the session initiation messages to indicate ILNP capability.
*** Once the node roams to a foreign network, or finds another link using a different interface, it sends a *Router Solicit* message to SBR2 (new network/location) to enable the MN register with the network. SBR2 replies with *Router Advert* message after the necessary security checks and layer 2 message exchanges. The MN associates with the new network and updates its location with the DNS and the CN.

The handover process explained above will ensure session continuity as the MN's upper layers of the TCP/IP stack are not aware of any change in *Locator*, and the NI does not change irrespective of the active interface. But there is still *Movement Detection* delay as with MIPv6 as MN scans, associates, and receive router advert from the new *Locator*.

Our proposal stands to make a lot of difference in such a scenario (and many highlighted below) with the introduction of *Information Server* (IS), which is a database of wireless access links available over a defined geographical location we called AREA. An AREA-IS is provided as an independent service within an AREA and serves as a means by which MNs obtain information about target PoA prior to handover. The server also controls attachment to PoAs based on some outlined policies to ensure that none is over-utilized within an area. The server stores a list of all the PoAs within its AREA, and the PoAs regularly update the server when there is attachment or detachment of MNs. For each PoA, the server will have the following information (a) bandwidth capacity (b) PoA's home network and access technology type (c) geographical location and coverage (d) utilisation status - number and identities of MNs connected at any given time and the resources being utilized. Parameters 'a to c' need only to be captured once in the server unless there is a configuration change, for instance an upgrade by the provider.

Despite the qualities of ILNP outlined earlier and the improvement it will bring when compared to MIP-based protocols, the introduction of AREA-IS is necessary for the following reasons:

1. Although the Transport layer sessions in ILNP are formed with the *Identifiers*, and as such are maintained during the handover, the packets sent before the CNs learn of the MNs new location are dropped by the old *Locators*, which causes packet loss in handover. With the AREA-IS in place, the packets will be forwarded to the current PoA or another AREA-IS serving the MN.

2. As with the above point, ILNP may have a problem recovering from simultaneous mobility – where the two endpoints are sufficiently mobile and may handover at the same time. The packets sent at this point may likely be dropped as both nodes wait for the DNS to update the *Identifier*/*Locator* mapping. With AREA-IS, the packets are forwarded to the serving PoA or another AREA-IS.

3. The time taken to complete the layer 3 handover process, especially movement detection, further increases the handover delay. As stated earlier, the AREA-IS will avail an MN with information about the target PoA in the surrounding area. The MN can use its current connection to exchange Layers 2 and 3 handover messages (such as authentication, *Router Solicit/Advert* etc) and send the LU message to the CN just prior to handover; and then to the DNS afterwards as shown in Figure IV.3.

4. The real-time update of utilization status of the different PoAs can be used by the AREA-IS for bandwidth management and QoS. The AREA-IS will only provide information about PoAs that are currently under-utilized within the area to the MNs, and/or the links that have the capacity to handle applications currently run by the user. This ensures load balancing between the different access links within an area.

5. As stated earlier, when ICMP LU message sent by an MN after a handover is not received by the CN, the CN can retrieve such information from the DNS, we argue that the DNS updates are not fast enough for the information to be available in such a short spell of time. Delay sensitive applications will benefit immensely from the use of AREA-IS.

Below is a sketch of the proposed network topology.

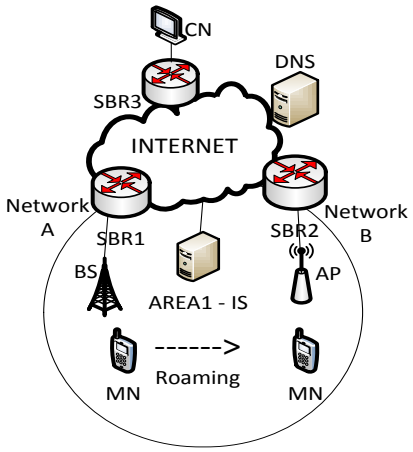

Figure IV.2 ILNP Area with Information Server

A PoA can forward a packet destined to one of its formerly attached MN to the AREA-IS. The AREA-IS can either forward the packet to the MN through its current PoA or to another AREA-IS that that MN recently roamed to. The amount of time to cache information about a formally attached MN by the PoA or the AREA-IS is just about the time it takes the DNS updates to be carried out. Once this time elapsed, incoming packets destined to that MN is dropped by the PoA or the AREA-IS.

The first functionality that the AREA-IS provides to the MN is to make information about links within a given environment available. Figure IV.3 shows how this functionality is provided in a handover process with ILNP supported by an AREA-IS.

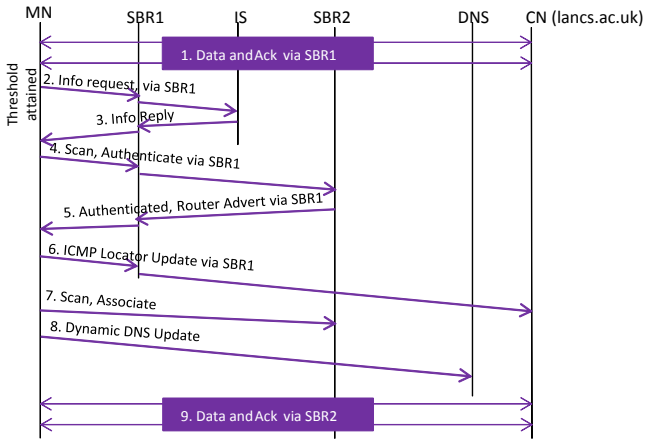

Figure IV.3 Information Server-Supported Handover in ILNP Network

The steps defined are as follows:

1. The MN's in Network-A have an established data session with the CN via SBR1.

2. Once the *Received Signal Strength* (RSS)[4] of the current access link has dropped to a certain pre-set threshold, the MN contacts SBR1 to request for information on PoAs within the area. SBR1 forwards this request to the AREA-IS serving the AREA.

3. AREA-IS replies with the requested information, including the channel frequencies for the MN to scan.

4. The MN scans the access channel(s) and chooses (if more than one PoA is provided) a target PoA. It sends authentication and Route Solicitation messages to the target network via SBR1.

5. The target network authenticates the MN and responds with the Route Advertisement message for the MN to learn of the target Locator value.

6. Just before handoff, the MN sends ICMP LU message to the CN.

7. The MN, then scans and associates with the new PoA. Both authentication and movement detection processes are skipped, and the MN has already formed its I-Lv.

8. The MN uses a Dynamic DNS Update to update its new *Locator* value with the DNS.

[4] A different parameter can be used, such as QoS. A user may also decide to connect to another available link during application run.

9. All communication is now routed via SBR2.

V. DISCUSSION AND FUTURE WORK

We intend to implement ILNP on a laboratory testbed consisting of a Cellular/WiMAX and a Wi-Fi access links. We decided to opt for a testbed implementation because it is more desirable in this case than simulation and mathematical modeling, as we attempt to closely study the behavior of the new protocol. Much of the simulation systems reviewed – NS2, OPNET and OMNET – have focused more on the radio links and not the network and upper layers of the TCP/IP stack, and it will be difficult to capture the original behavior of the protocol using simulation. Mathematical modeling is not the ideal path in this research as one of the main aims of the work is to develop and implement the protocol on the target platform using real machines.

To evaluate the performance of the protocol, we will compare it with the well-established MIPv6 by running multimedia applications such as voice and video. We will use metrics such as connection setup time, number of control packets, end-to-end delay, handover delay and packet loss. We will also demonstrate compatibility between ILNPv6 and IPv6-based MNs by establishing a communication session between the two end systems.

In the course of this research, we hope to answer the following questions: How significant is the improvement brought about by the ILNPv6 protocol with the elimination of HA, DAD, triangular routing and tunneling as compared to MIPv6, in terms of packet loss and delay in handover, and global reachability of an MN? How would the introduction of AREA-IS as an intelligent handover enabler into an ILNP network enhances seamless vertical handover for multi-interface devices within a defined geographical area? And what impact will global reachability of the MN as provided by ILNP protocol have on services such as a mobile webserver hosting, and peer-to-peer file sharing?

CONCLUSION

This paper proposed an ILNP-based solution for utilizing heterogeneous wireless access links in a particular area, which can be achieved by unifying the network protocol in use. We explained that ILNP can support both network and client-based mobility management necessary to harmonize the mobility of the 3 popular wireless technologies. We have also hypothesized on the added advantage of using AREA-IS in a defined location to provide MN with up to date information of the available wireless networks to help in choosing the access link to roam to. The AREA-IS will also deliver packets to MN, which would have been dropped by SBR as a result of the MN's change of PoA. We believe that ILNP provides an elegant way of handling mobility in wireless networks and if complimented with an intelligent handover mechanism in the form of an AREA-IS, it will significantly enhance the users' mobility experience.

REFERENCE

[1] "Cisco Visual Networking Index: White paper," Cisco Systems Inc., San Jose, CA, 06 February, 2013.

[2] E. Gustafsson and A. Jonsson, "Always Best Connected," *IEEE Wireless Communications,* vol. 10, no. 1, pp. 49 - 55, 2002.

[3] C. Perkins, "IP Mobility Support for IPv4," RFC 3344, IETF, Aug 2002.

[4] D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6," RFC 3775,, IETF, Jun 2004.

[5] H. Soliman, K. Elmalki and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management," RFC 5380, IETF, Oct 2008.

[6] R. Koodli, "Mobile IPv6 Fast Handovers (FMIPv6)," RFC 5268, IETF, Jun 2008.

[7] S. Gundavelli, K. Leung, V. Devarapalli Wichorus, K. Chowdhury and B. Patil, "Proxy Mobile IPv6 (PMIP)," RFC 5213, IETF, Aug 2008.

[8] V. Devarapalli, R. Wakikawa, A. Petrescu and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol," RFC 3963, IETF, Jan 2005.

[9] D. Farinacci, D. Lewis, D. Meryer and C. White, "LISP Mobile Node," Internet-Draft, draft-meyer-lisp-mn-08, Oct 2012.

[10] D. Farinacci, V. Fuller, D. Meyer and D. Lewis, "The Locator/ID Separation Protocol (LISP)," RFC 6830, IETF, Jan 2013.

[11] R. Moskowitz, P. Nikander, P. Jokela and T. Henderson, "Host Identity Protocol," RFC 5201, IETF, Apr 2008.

[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 & TUTORIALS,* vol. 12, no. 2, pp. 186 - 204, Second Quarter, 2010.

[13] R. J. Atkinson and S. N. Bhatti, "Identifier-Locator Network Protocol (ILNP) Architectural Description," RFC 6740, IETF, Nov 2012.

[14] IEEE, "IEEE Guidelines for 64-bit Global Identifier (EUI-64)," [Online]. Available: http://standards.ieee.org/develop/regauth/tut/eui64.pdf. [Accessed 5 Oct 2012].

[15] B. Wellington, "Secure Domain Name System (DNS) Dynamic Update," RFC 3007, IETF, Nov 2000.

[16] R. J. Atkinson and S. N. Bhatti, "ICMP Locator Update Message for the Identifier-Locator Network Protocol for IPv6 (ILNPv6)," RFC 6743, IETF, Nov 2012.

[17] T. Li, "Recommendation for a Routing Architecture," RFC 6115, IETF, Feb 2011.

[18] "3rd GPP; Technical Specification Group Core Network and Terminals; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface (Release 11)," 3GPP TS 29.060 V11.6.0 (2013-03), 2013.

[19] J. Bi, Y. Wang and K. Gao, "Implementation Experience of Identifier-Locator Network Protocol for IPv6 (ILNPv6)," Internet Draft, draft-bi-rrg-ilnpv6-implementation-experience-00, 28 Apr 2013.

[20] S. N. Bhatti, R. J. Atkinson and J. Klemets, "Integrating challenged networks," in *MILITARY COMMUNICATIONS CONFERENCE (MILCOM)*, 2011.