Analysis of Locator Identity Split Protocols in Providing End-host Mobility

Avinash Mungur
Department of Computer Science and Engineering
University of Mauritius, Reduit, Mauritius

Abstract- The current IP architecture is not designed for end-to-end mobility because of the overloaded semantics of the IP address. The IP address is used to both identify and locate a host. This dual role of the IP address hinders mobility. Several Locator Identity split proposals have been developed to decouple the IP address. These proposals fall into two categories, map-and-encap and address rewriting approaches. The former uses tunneling for forwarding packets and the latter uses address translation. This paper analyses how end-host mobility is supported by the two categories of schemes. A set of mobility criteria have been identified, and both map-and-encap and address rewriting approaches have been evaluated based on these criteria. The purpose of the paper is to find out which of the two approaches can best support end-host mobility. The analysis is triggered by the fact that nowadays almost all mobile devices have Internet capabilities and users will naturally want to connect to the Internet and they will want their established connections not to be interrupted while changing network. Thus this paper contributes to an analysis of the Location Identity Split Protocols in support for end-host mobility against a set of identified mobility criteria.

Keywords – Future Internet, Locator Identity Split Protocols, End Host Mobility, LISP-MN, IVIP, HIP, ILNP

I. INTRODUCTION

The current TCP/IP stack uses the IP address to identify an endpoint host as well as to serve as a network topological locator. Due to the overloaded semantic of the IP address, end-host mobility is not handled efficiently. For example, when a node is moving and is changing network, ongoing sessions do not survive because there is a change in IP address. As a result ongoing communication has to be re-established when a host moves from one network to another unless a protocol such as Mobile IP [1] has been deployed. As a result of the dual role of the IP address, several proposals have been developed to decouple the actual semantic of the IP address. Those proposals are based on the concept of the Locator Identity Split which separates the endpoint identification and locator functions of the IP address. Hence an IP address does not necessarily need to both identify and locate the node within these proposals. The Locator Identity Split proposals are categorised as either map-and-encap or address rewriting scheme [2]. The proposals differ in how the indirection is achieved, either through the use of tunneling or address rewriting. In a map-and-encap scheme, packets are delivered using a tunneling mechanism where packets are encapsulated with an extra IP header when routed in the network. Examples are LISP [3] and IVIP [14] and they both provide support for end-host mobility. Address rewriting schemes do not make use of encapsulation. Instead the address in the IP header is rewritten. Examples are HIP [8], ILNP [10], Shim6 [12], Six/one Router [13] and GSE [16]. Only HIP and ILNP inherently provide an end-host mobility solution among the latter examples. Therefore to be able to qualitatively assess the end-host mobility provided by the Locator Identity Split protocols, a set of mobility criteria needs to be specified. The mobility criteria specified in this paper are general enough so that is can be used by protocols other than Locator Identity Split protocols to ensure that end-host mobility is being supported in the protocols. Therefore to successfully support end-host mobility, a Locator Identity Split protocol should strive to the meet the mobility criteria discussed in this paper. A survey of the Locator Identity Split protocols have been performed in [17] explaining how the protocols work in general, but the survey does not tackle in depth the issue of end-host mobility as detailed in this paper.

The rest of this paper is structured as follows: Section II outlines the identified mobility criteria. Section III provides an overview of four Locator Identity Split protocols which support end-host mobility. Section IV provides a qualitative evaluation of the four protocols based on the identified mobility criteria and Section V concludes this paper.

II. MOBILIY CRITERIA

When designing an IP mobility protocol for mobile node (MN), certain criteria need to be met in order to achieve a good level of communication or an acceptable level of packet flow between MNs. The criteria should either be

implemented by the network or the MN or both. If these criteria are met, the MN will always be reachable and ongoing sessions will still survive despite the nodes being mobile. The mobility criteria are as follows:

- **Packet Forwarding**: refers to the delivery of packets to and from the MN. With mobility, packets need to be forwarded on routes or paths where the latency is close to the shortest path provided by the IP routing infrastructure. The way in which packets are being delivered by the protocol should ideally not increase the latency.
- **Route Update**: refers to how quickly the new route is updated in the network after the MN moves to another point of attachment, so that the MN is reachable and packets can be routed successfully to the MN. A route is considered to be updated if the MN is reachable after moving to a new point of attachment.
- **Efficient Handover**: during handover, as far as possible, the packet loss should be minimised and be performed without long delays. Soft handovers should also be catered. For example, a make-before-break approach is suitable in which the MN can migrate to the new point of attachment before breaking from its old one, resulting in an efficient and smooth transition.
- **Support for Sleep Mode**: in sleep mode, the MN does not regularly need to update the network with its current location in order to get packets delivered to itself, as it is the case when the MN is in active mode [18]. Mechanisms such as IP paging [19] could help to locate the MN in sleep mode. This will result in efficient battery power management of the MN, whilst decreasing the signaling overhead in the network.
- **Security**: the protocol should ensure that appropriate measures are used to deal with any new security vulnerabilities and also ensure that the level of security is no poorer than that supported within existing networks.
- **Robustness**: the protocol should be resilient against network failures and it should not have any single point of failure that will result in the protocol being unusable.
- **Concurrent Movement**: the ability for both end-hosts to be able to move simultaneously without breaking any ongoing sessions.
- **Deployment**: the protocol should be deployable in the current Internet architecture and it should be able to interact with a legacy infrastructure. The cost and effort in deploying the protocol has to be considered.
- **Scalability**: the protocol has to support a large number of MNs and cope efficiently with the potential for the MNs to be frequently changing location. As a result of frequent movement, efficiently managing the handover latencies is important to avoid significant packet loss.

III. Overiew of Locator Idenity Split Protocols In Support For End-Host Mobility

This section provides an overview of four Locator Identity Split protocols which provide support for end-host mobility; mainly LISP in the form of LISP-MN, IVIP, HIP and ILNP. LISP and IVIP are chosen because they employ a map-and-encap scheme whereas HIP and ILNP use a rewriting approach. These four protocols will then be qualitatively evaluated against the identified mobility criteria in section IV.

A. LISP

Locator Identifier Seperation Protocol (LISP) has "*two address spaces: one used within a domain (the EID space) and one used to transit between domains (the RLOC space)*" [7]. End host systems only know about the EID, (Endpoint Identifier), which is in fact an IP address and it is globally unique. Depending on which version of LISP[1] is being used, the EID can be routable between domains. For example in LISP 1 and LISP 1.5, the EID is a routable address across domains for bootstrapping purposes where as in LISP 2 and LISP 3, the EID is only routable within a local site. RLOC (Routing Locators) are IP addresses assigned to routers known as "Tunnel Routers" [3] and these IP addresses are globally routable. Tunnel Routers are responsible for mapping EIDs to one or more RLOCs after doing an EID-to-RLOC mapping lookup. In LISP when a packet is generated, the source and destination address are EID addresses. A packet destined to an EID destination in another domain will pass through a Tunnel Router, known as the Ingress Tunnel Router (ITR), which will first map the destination an EID to a RLOC, which is the entry router of the destination domain and is known as the Egress Tunnel Router (ETR). At the ITR, an EID-to-RLOC mapping database is necessary for doing the appropriate mapping. Currently the database use to hold the binding between the EID-to-RLOC is the LISP delegated database tree (LISP-DDT) [23]. Then after retrieving the RLOC, the ITR will encapsulate the packet by adding an outer header to the packet and setting the outer header destination address to the

[1] There are a number of LISP variants. The different variants depend on whether the EID is routable or not. With LISP 1, 1.5, the EID is routable address, whereas LISP 2, 3, the EID is not globally routable but only routable within a local site. LISP 2 uses DNS for EID-to-RLOC mapping and LISP 3 uses a different mapping database illustrated in LISP-CONS[20], LISP-APT [21], LISP-ALT [5], LISP-NERD [22]

RLOC. When the packet arrives at the ETR, the ETR will decapsulate the packet by removing the outer header and will forward the packet based on the inner IP header.

B. LISP-MN

To provide end-host mobility in LISP, LISP Mobile Nodes (LISP-MN) [4] has been developed. LISP-MN needs to implement both the ITR and the ETR functionality, and require LISP as its underlying network. "*All packets the LISP mobile node originates are LISP encapsulated, and all packets received by a LISP mobile node will be LISP encapsulated*" [4]. Since the LISP-MNs implement the ETR functionality, they need to always communicate their EID-to-RLOC mapping to a configured Map-Server (MS) [4] each time they roam into a new network. The MS will then publish the mapping in the LISP-ALT [4] database such that the LISP-MNs remain reachable for new connections.

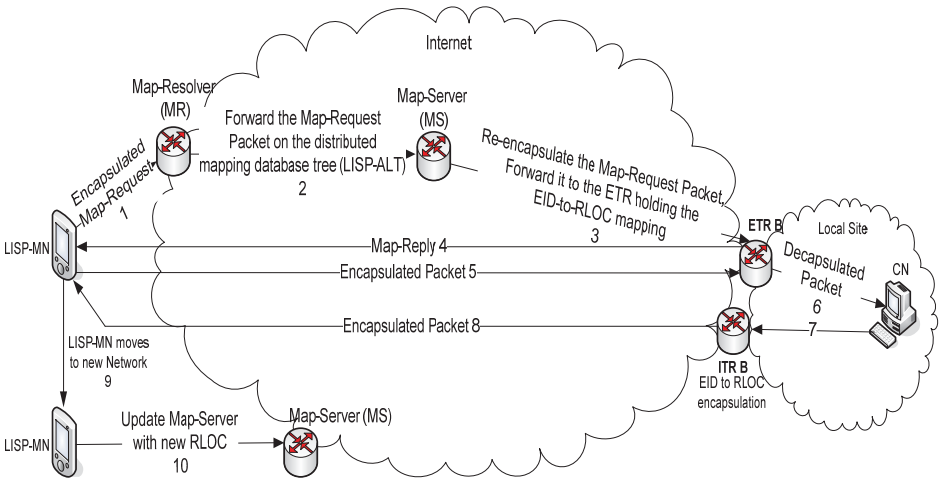

Figure 1. LISP-MN

Figure 1 illustrates an example when a LISP-MN is communicating with a correspondent node (CN) located in Local Site B. The LISP-MN will first send an encapsulated Map-Request [4] message to the Map-Resolver [4] to retrieve the EID-to-RLOC mapping for the CN (1). The Map-Resolver will decapsulate the packet and will forward it on to the distributed mapping infrastructure (2) in order to be forwarded to the relevant Map-Server, which knows the ETR that possesses the mapping for the EID contained in the Map-Request packet (3). ETR B will decapsulate the packet and will send a Map-Reply [3] to the LISP-MN which contains the mapping resolution for the EID-CN to RLOC (4). The LISP-MN will cache this mapping and can then start sending encapsulated data packets (5) to ETR B. Decapsulated packets are forwarded to the CN (6). The ITR B will need to perform the EID-MN-to-RLOC resolution to acquire the RLOC value for the LISP-MN (7). In this instance, the same procedure as (1) to (2) is performed. When the ITR B learns the RLOC value for the LISP-MN, it caches the value and will subsequently encapsulate packets for the LISP-MN (8). When the LISP-MN moves and acquires a new RLOC value (9), it needs to update its MS (10) so that new connections can be established. The ITR B (11) needs to refresh its cache to avoid having stale record, by sending a Map-Request packet after a pre-defined timeout value.

C. IVIP

The author best describes Internet Vastly Improved Plumbing (IVIP) as a "*global system of routers and collection of databases which control the tunneling of some of these routers*" [14]. IVIP also has the concept of an ITR and ETR, where packets at the ITR are encapsulated and are sent to an ETR which decapsulates them. The databases (Query Server database, IVIP database) in IVIP act as the mapping infrastructure and are responsible for updating the ITRs with the relevant EID-to-RLOC mapping. IVIP has another ETR called the Translating Tunnel Router (TTR) used for mobility [15].

In Figure 2, a MN makes a two-way tunnel with the TTR (1) which is used for forwarding incoming packets to the MN, and to forward outgoing packets from the MN to an ITR. The TTR is effectively acting as a Mobile IP Home Agent [] with the exception that the MN is able to connect with a TTR which is close to its access network. Therefore no fixed Home Agent is required. The TTR forwards the packets to the ITR A (2). When the CN needs to send packets to the MN, the packets pass through the ITR B and tunnel to the TTR (3), and then the packets are decapsulated at the TTR and re-encapsulated with the MN address. The packet is then forwarded to the MN where it is decapsulated before being handed to the IP layer.

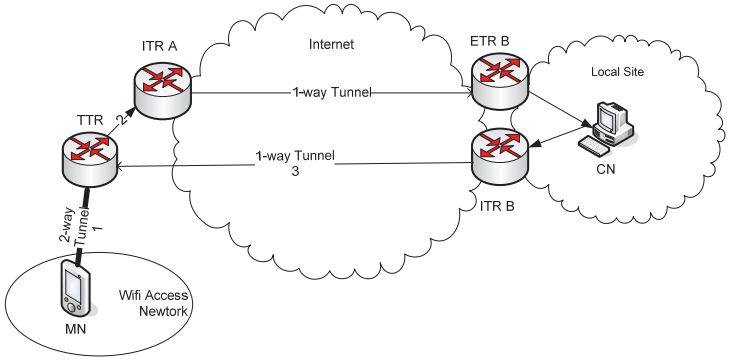

Figure 2. IVIP Network

D. HIP

Host Based Identity Protocol (HIP) achieves a Locator Identity Split by introducing a new cryptographic public key namespace in the TCP/IP stack, known as the Host Identifier (HI) [6][17]. In HIP, a host is identified by the HI which is a public key. The HI does not identify a particular interface but identifies the node. The IP address is used as a network topological locator for routing only. HIP uses Domain Name Server (DNS) and also a rendezvous server (RVS) [6] which holds the latest IP address for a given HI.

Figure 3 shows how a connection is set up in HIP. A CN queries the DNS to retrieve the RVS IP address of the MN (1) (2). Then the CN will initiate a 4-way handshake with the MN. The first packet during the handshake is sent to the RVS (3), which will forward it to the MN (4). When the MN receives this packet it will reply directly to the CN (5), and from now on packets will be forwarded directly between the MN and CN (6) without passing through the RVS in order to complete the handshake and to allow data to flow. When the MN moves, it will update its RVS with its new address (7) and it will send an Update message (8) to the CN.

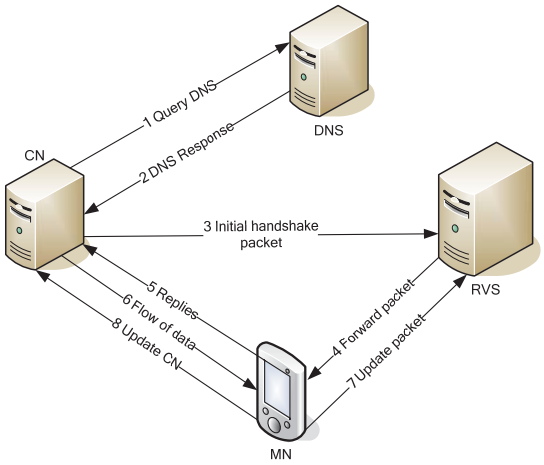

Figure 3. HIP Connection SetUp

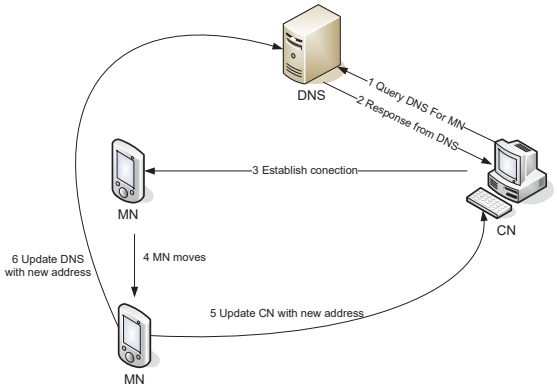

Figure 4. ILNP

E. ILNP

Identifier Location Network Protocol (ILNP) [10] splits an IPv6 address into two parts. The upper 64 bits is the Locator which is used for routing and the lower 64 bits is used for identifying the host. The identifier used in ILNP does not identify a particular interface in the host, but identifies the node itself. ILNP uses DNS to store the mapping between the Locator and Identifier, by introducing 4 different Resource Records (RR) [11]. One of the main RR is the L record which locates the network in the topology. To identify the node within a network L, the Identifier I is used, such that the combination L:I forms a 128 bit IPv6 address. For connection establishment, the transport layer will bind to I using an ILNP layer within the stack to make the appropriate mapping between the L and I value. By updating the L resource record appropriately, ILNP can provide end-host mobility. When a MN moves, a Binding Update message is used to update the CN, and the DNS is also updated with the MN's new location.

Figure 4 shows how ILNP works. When a CN needs to communicate with a MN, it contacts the DNS (1). The DNS will reply with the address of the MN (2). The transport layer at the CN will bind with the I value. The packet is sent to the MN, and the connection will be established (3). When the MN moves (4), it will update its L DNS record (6) and also send a Binding Update to the CN (5). The ILNP layer at the CN will make the appropriate changes so that ongoing communication will not cease.

IV. QUALITATIVE EVALUATION

In this section, we provide a qualitative evaluation of the approaches reviewed in section III, by evaluating each protocols with the identified mobility criteria of section II. The aim is to analyse the two approaches, map-and-encap or address rewriting, in terms of supporting end-host mobility.

A. Packet Forwarding

In LISP-MN, packets are forwarded using tunnels, and utilise UDP encapsulation. The encapsulation overhead for introducing a LISP UDP header during the tunneling process may result in an increase in latency, and would increase the size of the packet which could exceed the path Maximum Transmission Unit (MTU). The LISP-MN, either when sending controls packets (e.g. Map-Request) or data packets, could in certain situations, be encapsulated with more than one UDP header during a communication session. Moreover, if LISP-MN employs "*Recursive Tunneling*" [3], this will also increase the size of the packets, and if the packets exceed the path MTU, the packet will be dropped. Furthermore, at the LISP-MN, the lookup for an EID-to-RLOC will introduce a latency for the first data packets until the LISP-MN caches the mapping.

For IVIP, the MN needs to make a two-way tunnel with the TTR and uses IP-in-IP encapsulation. The TTR will then forward packets to the ITR, which will perform the mapping between the CN destination address and the ETR to use, and the ITR will send the encapsulated packets to that ETR. The lookup latency will be less compared to LISP-MN because IVIP uses a "*fast hybrid pull push mapping system*" [24]. However, IVIP will have the same encapsulation overhead as LISP-MN. Also in IVIP, establishing the two-way tunnel with the TTR, this may increase the connection setup time for the first packet.

In HIP, since the IP address is used for routing, the underlying routing infrastructure is used. However the overhead in connection set up, which involves cryptographic operation, might increase the latency considerably. In the 4-way handshake, a puzzle challenge needs to be solved. Depending on the complexity of the puzzle [8], a substantial amount of time can be spent solving it. This problem may be intensified on mobile devices with limited CPU power which has the potential to lead to a slow connection establishment. However, not all rewriting schemes employ procedures that will yield a high delay. For example ILNP uses less demanding cryptographic procedures for authentication, such as the generation of a random number. Also HIP packets do not use additional headers that will increase the size of the packets.

ILNP uses the existing routing infrastructure for routing packets. However delay can be incurred during route establishment due to the authentication process but the delay will be less than in HIP. This is because ILNP resolves a domain name for a CN only once by doing a DNS lookup to obtain the hosts IP address. HIP first queries the DNS to obtain the IP address of the rendezvous server. The rendezvous server will then resolve the HI to obtain the IP address of the CN. The time spent in resolving an address is therefore less for ILNP than HIP. Furthermore, delay is incurred where there is an expensive pre-session connection establishment as it is in HIP.

Map-and-encap approaches will in general have an encapsulation overhead for each and every packet which will affect the packet size and length. Also there is an inefficient use of wireless resources because packets are constantly encapsulated. As for the rewriting schemes, each of them uses the underlying routing infrastructure to route the packet. There is no encapsulation overhead. However in the rewriting schemes, the overhead will come in establishing the connection. As these schemes are not using the IP address as the Identifier, but only for routing, there should be a way to authenticate both endpoints. Depending on the mechanism used for authentication, delay will be experienced before actually forwarding the packets. This delay is only experienced during set up, and subsequent packets will be forwarded normally without any overhead.

B. Route Update

When a LISP-MN roams from one network to another and acquires a new RLOC value, it needs to update its MS with the new EID-to-RLOC mapping, and also ensures that all the ITRs refresh their cache entry with the new LISP-MN mapping This would avoid the ITRs using stale mappings. The MS acts as an anchor point for the LISP-MN to receive all the new EID-to-RLOC mappings from the LISP-MN. The MS also responds to the Map-Requests on behalf of the LISP-MN to avoid the LISP-MN wasting resources in processing the requests. However for any ongoing communications, the peer tunnel routers (ITR) need to be refreshed. The authors of [4] proposed that the

LISP-MN enables the Solicit-Map-Request (SMR) bit in the data packets such that if the peer tunnel router is an ITR, it will send a Map-Request to retrieve the new mapping. However the latter solution only works if the peer tunnel router is both an ITR and an ETR. If the peer tunnel router is exhibiting only ETR functionality, then it will not request the new mapping. In this situation, the authors suggest that a Time to Live (TTL) value is associated with the cache entry in the peer ITRs. The TTL value suggested is in the range of 1-2 minutes. When this TTL expires, the ITR will send a Map-Request to request for an EID-to-RLOC mapping. However assuming that during the TTL interval the LISP-MN has moved to another network and has a new EID-to-RLOC mapping, then there is a good probability that packets destined to the LISP-MN will still be encapsulated with the old EID-to-RLOC mapping present at the peer ITR. Hence the packets will be dropped until the TTL expires and the peer ITR sends a Map-Request. If the TTL is too low, there will be frequent transmission of Map-Request packets which will potentially needlessly overload the network. The critical aspect is to be able to identify an ideal TTL value.

For IVIP, whenever the MN moves across subnet and gets a new address, the MN needs to establish a new 2-way tunnel with the closest TTR with that address [15]. It may happen that the MN node selects the same TTR as it was previously connected to. As a result, there will not be any mapping update at the ITR, since the same TTR is used to tunnel packets to the MN. Therefore, there will not be any packet loss. If the MN changes TTR, an update at the new ITR needs to take place. The mapping update will be done within a short space of time due to the use of the different types of databases efficiently disseminating the mapping to the ITRs. The MN will wait until the 2-way tunnel with the new TTR is established before breaking from its old one so as to avoid packet loss while switching between TTRs.

For HIP, when the MN changes its point of attachment, it sends an UPDATE [6] packet to the CN and to its RVS. There are no major changes in the routing infrastructure as is the case with LISP-MN, and also no packet loss. In ILNP, in the case of node movement, dynamic updating is used to update the Locator value in the DNS, and also an update packet is sent to the CN so to avoid packet loss.

Depending on how fast the ITR completes its mapping lookup for a particular destination EID, map-and-encap schemes can support Route Updates with minimal delay and packet loss when the MN moves, as demonstrated by IVIP. LISP-MN needs to define a suitable TTL value at the ITR such that it can refresh its cache optimality. As for rewriting schemes, appropriate mechanisms (such as informing the CN) have been included so that it is the responsibility of the end-point to perform the Route Update.

C. Efficient Handover

To support fast and smooth handover, a make-before-break approach has to be supported in order to minimise packet loss. In this approach before the MN totally breaks its attachment with the old network, the MN can perform “attachment” procedures with a new network. To enable this approach, a MN needs to simultaneously listen to the old and new network, such that the MN can still communicate with the CN via the old network, and with the new network the MN can acquire its new address and perform the Route Update process. The MN should have more than one radio channel such that one radio channel will listen to the old network and another one will listen to the new network. After the Route Update process, the CN will be able to forward packets to the new address of the MN. This approach minimises packet loss during the handover and allows for a smooth transition.

If a LISP-MN possesses two radio channels, on the old channel it can still receive data packets while on the new channel it can send its new RLOC to its MS. All the peer ITRs will still have the “old” mapping for the LISP-MN and data will still reach the LISP-MN on its old channel. The ITR will only request the new mapping from the MS if either the SMR bit is flagged or the TTL at the ITR expires. The LISP-MN will still need to use its old channel to receive data until all the peer ITRs update their cache. If the peer ITRs do not acquire the new mapping during the handover, data will not flow onto the new channel. Efficient handover is not achieved if the TTL value is used at the peer ITRs because they are not updated during the handover. Ideally while the LISP-MN is performing the handover, the LISP-MN could use the new channel to trigger all the peer ITRs to send a Map-Request.

IVIP provides a handover mechanism which is handled by the TTR. When the MN acquires a new Care-of-Address, it will establish a two-way tunnel with the TTR, while still maintaining the old tunnel so that packets are still received. Once the new tunnel is set up, the old tunnel can be discarded. This process requires efficient TTR management.

In HIP, there is no such provision for handovers, although such mechanisms can be implemented. A HIP MN needs to be able to listen on different channels. When the MN gets a new Locator value, it can update its CN and RVS through the old channel and it can receive packets on the new channel. Extra consideration has to be made to treat out of order packets.

ILNP provides a soft handover mechanism such that it can still communicate with its old channel while acquiring network access on its new channel and thus start the process of updating its CN and DNS.

Both LISP-MN and HIP do not provide any efficient handover mechanism, but they can be introduced. In LISP-MN, it is important that the ITRs are triggered to perform a Map-Request during the handover procedure otherwise the ITR will still contain the old mapping.

From the handover perspective, whether we are using a map-and-encap or a rewriting scheme, the MN needs to have a mechanism where it can listen on different channels and configure its interface(s). The MN should be able to move the traffic from one interface to another. The MN needs to have a driver which supports two radio channels and two MAC addresses in order to perform the handover because most drivers in the MNs currently support only one radio channel with only one MAC address.

D. Support for Sleep Mode

Neither LISP-MN, IVIP, HIP nor ILNP have considered a mechanism for a MN to be in sleep mode [18][19]. Considering IVIP is a router based approach, a paging mechanism can be integrated so as to page a MN in dormant mode within the network. In IVIP, a basic paging mechanism could be used in conjunction with the TTR.

LISP-MN can implement a paging mechanism which can page the MN. The paging mechanism will need to extract the EID of the LISP-MN from the encapsulated data packets. To send page messages, the paging solution needs to use LISP encapsulated packets. Hence a paging solution for LISP-MN will need to perform encapsulation and decapsulation.

HIP can also integrate a paging solution, for example, in the instance where a MN is under the coverage of an old access router, and the MN is in sleep mode and moves to a new access router. When data packets are delivered, they will be delivered to the old access router. The old access router will fail to deliver the packets for that MN, and the failure in delivering the packets would ideally start the paging process. But the old access router will not initiate the paging because it does not know which data to use from the packet to start the paging process. The packets do not include an identifier value which will state to which MN the packets are destined to. HIP does not include the HI information in the packets which makes it difficult to know which MN the packets belong to. Therefore, paging a HIP node might be difficult to implement.

With ILNP, the packet has the Identifier embedded in the destination address, which is unique within the site; therefore a paging mechanism can easily use this Identifier to page for the MN. However, in ILNP, duplicate address detection (DAD) is *"scrapped"* [11], because of the Identifier having a high probability of being unique. However, it is still possible that there may be a collision with the Identifier. For example, the MN moves to a new access router and performs an autoconfiguration process. If the MN has not yet informed its CN of its new address, in-flight packets will still be delivered to the old access router, which will trigger the paging process. The page packet will contain the Identifier of the MN and the MN having the Identifier will respond to the page request. But since DAD has not been performed, it may happen that two nodes have the same Identifier value and both will response to the page request. Thus in ILNP, using the Identifier for paging might not yield the correct outcome.

E. Security

Security aspects are very important, especially when the nodes are mobile. Since LISP-MN uses LISP as its underlying network it will have the same security concerns as are evident with LISP. For example LISP cannot protect against spoofed source addresses since in a LISP header, the outer source address is that of the ITR. An attacker can spoof the outer source address. Moreover, an ITR can be the victim of a malicious or legitimate cache "attack". For example if the ITR needs to do a lookup (EID-to-RLOC) for multiple destination EIDs, the cache might not hold all the mappings depending on the cache size, which may result in a denial of service. It is malicious if an attacker is targeting the ITR but legitimate if there are a number of users communicating with different nodes on different networks. In the context of LISP-MN, since the MS is an essential part of the infrastructure for responding to Map-Request messages, the MS could be a target for attackers to send unsolicited versions of such messages.

In the case of IVIP, to prevent the source address from being spoofed in the outer header packets, ITR uses the source address of the inner header to be the source address in the outer header. Thus the source address in the inner and outer header are the same. If the source addresses are not the same, the packets have been tampered with and can be discarded. However IVIP can still be a victim of a cache attack. For rewriting schemes, attacks against spoof packets can be limited by having proper end-to-end mutual authentication mechanisms and source IP verification processes discussed in the sections F and G respectively.

Moreover section H provides a brief discussion on the privacy and anonymity for both the map-and-encap and rewriting approaches in order to have a complete discussion on the security aspect.

F. End-to-end mutual authentication

The end-to-end mutual authentication issue is potentially greater in a rewriting scheme than in a map-and-encap scheme. In a rewriting scheme, since we have decoupled the location from the identity, there should be a way to authenticate the endpoint before starting the actual flow of communication. We need to make sure that we are communicating with the node that possesses the Identifier. In the map-and-encap scheme the host is still using the original overloaded IP address as the EID and hence the *"host's identity is implicitly authenticated by the routing infrastructure. That is, since the hosts are identified with IP addresses, and since IP addresses are the fundamental piece of data used in routing, the very definition of the internetwork assures that the IP packets are indeed sent to the intended hosts*" [8]. However there should be a way for authenticating both endpoints because source addresses are easily spoofed. This is why HIP introduces the 4-way handshake protocol and ILNP has a lightweight cryptographic generated number or uses IPSec to mutually authenticate the end-point. Map-and-encap schemes should also provide end-to-end authentication by using cryptographic procedures or by employing IPsec in order to prevent tampering of the source address.

G. Source IP verification

Both types of scheme need to allow verification of the source IP address. Therefore a return routeability protocol is needed. Such a protocol will be used when the MN moves and is sending an updated locator value to the CN. The CN needs to verify if the source address is reachable before using it.

H. Privacy and anonymity

In both types of scheme, there should be a way to preserve the privacy and anonymity of the communicating parties. In the map-and-encap schemes, since the EID is an IP address, it still provides some element of privacy and anonymity. The EID is not revealing the identity of the participants in a communication. However when two LISP-MNs are communicating we can track approximately the location of a LISP-MN. This is because the encapsulated packets contain the EID for identifying the LISP-MN and the RLOC which is identifying the network the LISP-MN is in. As the LISP-MN is roaming, the EID found in the packets will remain the same however the packets will be encapsulated with the new RLOC value. An eavesdropper can, by monitoring the packets, infer where the LISP-MN is moving assuming the eavesdropper already knows which network the RLOC belongs to. In the case of IVIP, the TTR sits in front of the MN, i.e. even though the MN is changing location, the packets are delivered to the MN's TTR first and then the TTR delivers the packets to the MN. Hence if an attacker is monitoring the packet traffic, he/she will not be able to trace the exact location since the TTR is providing another level of indirection.

With the rewriting schemes, some proposals require that the Identifiers explicitly identify the host globally, and this certainly compromises the privacy and anonymity of the node. To provide some level of privacy, another level of indirection can be used. In HIP, the RVS provides this element of privacy since the MN "hides" behind it. It is analogous to the Mobile IP Home Agent [1] [9]. However to provide an element of anonymity, a host can have multiple Host Identifiers.

I. Robustness

In both the map-and-encap schemes and rewriting schemes, there is a need for a mapping infrastructure so that the Identifier can be mapped to the Locator. If the mapping infrastructure is down, then it will be impossible to start a communication. So if the LISP-ALT database of LISP-MN, the RVS of HIP or the DNS for ILNP are down, there is a problem. The mapping infrastructure is the main point of failure, and there must be redundant mapping infrastructures that can still deliver the same service upon failure of one of the mapping elements.

J. Concurrent Movement

When both peer nodes are mobile, there are situations where the MNs move simultaneously and both the nodes miss the update packet. To cater for such scenarios, an "agent" is needed to forward the packets to the MNs. Such scenarios are independent of which type of scheme is being used. For IVIP, the TTR will need to manage it. For HIP, the RVS is used. In the case of ILNP, the DNS can be used as a forwarding agent, in the sense that if the MN session times out due to the fact that it missed a Location Update, the MN can perform a lookup at the ILNP layer, based on the Identifiers, to retrieve the address and maintain the connection. In LISP-MN, the MS serves as the agent. If both the LISP-MNs are roaming, the LISP-MN needs to send a Map-Request to retrieve the mapping of the CN from the MS. Hence the LISP-MN will retrieve the new mapping in case the CN has moved or both LISP-MNs have moved simultaneously.

K. Deployment

LISP and IVIP are router based approaches and are situated at the edge of a network. Interaction between a LISP upgraded network and a non-upgraded network will require a proxy to be able to bridge the gap. Also, stack modification is required in the LISP-MN to provide the ITR/ETR functionality. For IVIP, "*Open ITRs in the DFZ*" [15] have to be deployed, which will tunnel packets sent from networks without ITRs to the TTR, and MNs also require a stack upgrade.

HIP is a host based approach and stack modification is required. It requires API modification in order to make sockets bind to the HI instead of the IP address. Also HIP depends on IPsec to be operational. DNS needs to be modified to add a new resource record for the HI value. Endpoints need to be HIP aware to set up connections. As for ILNP, it works only with IPv6 addresses, requires a host stack upgrade and the DNS to be modified. End-hosts need to be ILNP aware for initiating communication.

With the map-and-encap schemes, deployment incentives are much stronger compared to a rewriting scheme because interaction with legacy networks can be achieved. However for both the map-and-encap and rewriting schemes, host stack modification is required. Rewriting schemes can be deployed easily, if they are able to provide support for legacy infrastructure systems.

L. Scalability

The protocol needs to scale efficiently when the number of MNs increases and the nodes are changing network frequently. For LISP-MNs, each time they roam they need to update their MSs. Consequently all the peer ITRs which have the previous cached mapping need to refresh their cache entries by issuing Map-Requests and waiting for Map-Replys. The LISP-MNs also need to refresh their cache when they roam. As a result, as the number of LISP-MNs increases and they change networks more frequently, delay will be incurred in forwarding data packets. The delay incurred is the time in processing the Map-Request and in delivering the Map-Reply each time the LISP-MNs move. This delay could make the LISP-MN architecture scale poorly.

With IVIP, the number of tunnels created between the TTR and MN will increase, which will degrade the network performance. Management of the tunnels, created by the increasing number of MNs will be the key problem in terms of scalability. If the tunnels are not managed properly, IVIP will scale poorly.

In a rewriting scheme, those solutions which use DNS to handle mobility, like in ILNP, need to cater for a large number of Dynamic Updates, and the DNS needs to reflect the change quickly through efficient caching. The DNS needs to refresh its cache with the latest address of the MN. To limit the scaling DNS cache issue, HIP MNs update the RVS when roaming.

Both schemes, in order to cope with an increasing number of moving MNs, are ultimately dependent on how their mapping service reacts to an influx of updates. However, poor degradation is likely to be experienced with map-and-encap schemes due to the usage of encapsulation which will make inefficient use of network resources, with delays incurred because of frequent lookups at the mapping infrastructure.

V. CONCLUSION

In this paper, we evaluated the two major approaches to Locator Identity splitting, map-and-encap and address rewriting, in terms of providing end-host mobility. To evaluate the Locator Identity split approaches, we identified a set of mobility criteria that a solution or protocol needs to possess in order to effectively provide end-host mobility. The whole purpose of the evaluation was to analyze how the two approaches best fulfils the mobility criteria. We used suitable protocols that best represent the map-and-encap and address rewriting approaches as shown in Table 1 in order to conduct the evaluation.

From the discussion in the section IV, it can be said that map-and-encap approaches suffer mostly from the tunneling process. Every packet has to be encapsulated and decapsulated when transiting the network. Another concern is the added latency in performing a look up at the mapping infrastructure when the node is mobile. Furthermore since map-and-encap mechanisms are router based, they are easily deployable but the MNs still need to be upgraded. Also with a tunnel approach, packet headers are hidden from intermediate routers. Functionality like caching and quality of service differentiation become difficult to implement. Furthermore, in the map-and-encap approaches, a true Locator Identity Split has not been achieved because the IP addresses are still semantically overloaded. On the other hand, address rewriting schemes do not suffer from the encapsulation overhead. The main concerns with address rewriting schemes are the inherent security implications.

Table -1 Summary Table

	Map-and-Encap		Address Rewriting	
	LISP-MN	**IVIP**	**ILNP**	**HIP**
Packet Forwarding	Tunneling	Tunneling	Rewriting	Rewriting
Route Update	Map-Server Update ITR Update	ITR update	DNS Update & Locator Update	Update Packet
Handover	No	Yes	Yes	Yes
Support for Sleep Mode	No	No	No	No
Security[2]	Medium	Medium	Medium	High
Robustness	Map-Server/Resolver, LISP-ALT	Mapping System	DNS	DNS, RVS
Concurrent Movement	Map-Server	TTR	DNS	RVS
Deployment	Map-Server and LISP Architecture	TTR is necessary	DNS modification	DNS modification, RVS and IPsec are necessary
Scalability	Wait for processing of Map-Request	Depends on Mapping infrastructure	Depends on DNS	Depends on DNS and RVS
Router/Host Approach	Both	Both	Host Based	Host Based

REFERENCES

[1] D. Johnson, C.Perkins and J. Arkko, "Mobility Supporting IPv6," Network Working Group, Internet Engineering Task Force, RFC 3775, June 2004.

[2] G. Huston, "Architectural Approaches to Multi-Homing For Ipv6", Network Working Group, Internet Engineering Task Force, RFC 4177, September 2005

[3] D . Farinacci, V. Fuller, D. Meyer and D. Lewis, "Locator/ID Separation Protocol (LISP)", Network Working Group, Internet Engineering Task Force, RFC 6830, January 2013.

[4] D. Farinacci, D. Lewis, D. Meyer and C. White, "LISP Mobile Node", Network Working Group, Internet Engineering Task Force, draft-meyer-lisp-mn-15.txt, July 2016.

[5] V. Fuller, D. Farinacci, D. Meyer and D. Lewis, "LISP Alternative Topology (LISP+ALT)", Network Working Group, Internet Engineering Task Force, RFC 6836, January 2013.

[6] P. Nikander, T. Henderson, C. Vogt and J. Arkko, "End-Host Mobility and Multihoming with the Host Identity Protocol", Network Working Group, Internet Engineering Task Force, RFC 5206, April 2008.

[7] D. Meyer, "Update on Routing and Addressing at IETF 69", Internet Engineering Task Force Journal, Internet Society, vol. 3(2), Geneva, Switzerland, October 2007.

[8] P. Nikander, J. Ylitalo, and J. Wall, "Integrating Security, Mobility, and Multi-homing in a HIP way", in Proc *Network and Distributed Systems Security Symposium (NDSS'03)*, San Diego, CA, USA, Feb. 2003.

[9] X.P. Costa, R. Schmitz, H. Hartenstein, M. Liebsch, "A MIPv6, FMIPv6 and HMIPv6 handover latency study: analytical approach", in Proc *IST Mobile and Wireless Telecommunications Summit 2002*, Greece, June 2002.

[10] R. Atkinson, "ILNP Concept of Operations", Internet Engineering Task Force, draft-rja-ilnp-intro-11.txt, July 2011.

[11] R. Atkinson, S. Bhatti and S. Hailes, "A Proposal for Unifying Mobility with Multi-Homing, NAT, & Security",in *5th ACM Int. Workshop on Mobility Management and Wireless Access (MobiWAC)*, Chania, Crete, October 2007.

[12] E. Nordmark and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6", Network Working Group, Internet Engineering Task Force, RFC 2009, June 2009.

[13] C . Vogt, "Six/One Router: A Scalable and Backwards Compatible Solution for Provider-Independent Addressing", in *ACM Int. Workshop on Mobility in the Evolving Internet Architecture (MobiArch)*, Seattle, WA, USA, Aug 2008.

[14] R. Whittle, "Ivip (Internet Vastly Improved Plumbing) Architecture", Network Working Group, Internet Engineering Task Force, draft-whittle-ivip-arch-04.txt, March 2010.

[15] R . Whittle and S. Russert, (2008 Oct). TTR Mobility Extensions for Core-Edge Separation Solutions to the Internet's Routing Scaling Problem [Online]. Available: http://www.firstpr.com.au/ip/ivip/TTR-Mobility.pdf

[16] M. O'Dell, "GSE - An Alternate Addressing Architecture for IPv6", Network Working Group, Internet Engineering Task Force, draft-ietf-ipngwg-gseaddr-00.txt, Feb 1997.

[17] Komua, Mohit Sethia and Nicklas Beijara, "A survey of identifier–locator split addressing architectures", Computer Science Review, Elsevier, vol. 17, pp. 25-42, August 2015.

[18] E. N. Onwuka, "A Paging Design For Mobile Cellular Internet Enhanced By Locality In User-Behavior", Scientific Research and Essay vol.3 (10), pp. 460-466, October 2008.

[2] The level of security: low means lower than current Internet security, medium means the same level as the current Internet, High means higher than the actual current Internet security standards

[19] Ramachandran Ramjee, Li Li, Tom La Porta, and Sneha Kasera, "IP Paging Service for Mobile Hosts ", in Proc. of *International Conference on Mobile Computing and Networking, MOBICOM'2001*, Rome, Italy, July 2001.

[20] S. Brim, N. Chiappa, D. Farinacci, V. Fuller, D. Lewis, and D. Meyer "LISP-CONS: A Content Distribution Overlay Network Service for LISP," Network Working Group, Internet Engineering Task Force, draft-meyer-lisp-cons-04.txt, April 2008.

[21] D. Jen, M. Meisel, D. Massey, L. Wang, B. Zhang, and L. Zhang, "APT: A Practical Transit Mapping Service", Network Working Group, Internet Engineering Task Force, draft-jen-apt-01.txt, Nov 2007.

[22] E. Lear and Cisco Systems GmbH, "NERD: A Not-so-novel EID to RLOC Database," Network Working Group, Internet Engineering Task Force, RFC 6837, January 2013.

[23] V. Fuller, D. Lewis, V. Ermagen, A. Jain and A. Smirnov, "LISP Delegated Database Tree", Network Working Group, Internet Engineering Task Force, draft-ietf-lisp-ddt-07.txt, May 2016.

[24] R. Whittle, "Ivip Mapping Database Fast Push", Network Working Group, Internet Engineering Task Force, draft-whittle-ivip-db-fast-push-04.txt, March 2010.