J. Kempf
K. Leung
P. Roberts
K. Nishida
G. Giaretta
M. Liebsch

Internet Draft
Document: draft-kempf-netlmm-nohost-req-00.txt

Expires: January, 2006

July, 2005

Requirements and Gap Analysis for IP Local Mobility (draft-kempf-netlmm-nohost-req-00.txt)

Status of this Memo

Abstract

In draft-kempf-netlmm-nohost-ps, the problems with using global IP mobility management protocols for local mobility and some problems with existing localized mobility management protocols are described. In this document, we explore requirements for localized mobility management in more detail. An extensive gap analysis against the protocols illustrates where existing protocols are able to fulfill the requirements and where they are lacking.

Table of Contents

1.0 Introduction

In draft-kempf-netlmm-nohost-ps [1], the basic problems that occur when a global mobility protocol is used for managing local mobility are described, and two basic approaches to localized mobility management - the host-based approach that is used by most IETF protocols and the WLAN switch approach are examined. The conclusion from the problem statement document is that neither approach has a complete solution to the problem. While the WLAN switch approach is most convenient for network operators and users because it requires no host support, the proprietary nature limits interoperability and the restriction to a single wireless link type and wired backhaul link type restricts scalablity. The IETF host-based protocols require host software stack changes that may not be compatible with all global mobility protocols, and also require specialized and complex security transactions with the network that may limit deployability.

This document develops more detailed requirements for a localized mobility management protocol and analyzes existing protocols against those requirements. In Section 2.0, we review a list of requirements that are desirable in a localized mobility management solution. Section 3.0 performs a gap analysis against the requirements of proposed solutions to localized mobility management. Section 4.0 briefly outlines security considerations. Finally, in Section 5.0, a recommendation is made for the development of a network-based approach to localized mobility management.

1.1 Terminology

Mobility terminology in this draft follows that in RFC 3753 [2] and in [1]. In addition, the following terms are used here:

Host-Based Approach
A host-based approach to localized mobility management requires binding between a local care-of address and a regional care-of address at a mobility anchor within the localized mobility management domain. The binding is maintained by the mobile node and requires software in the mobile node's stack to perform the binding. The localized mobility service is authorized with the mobility anchor point separately from network access. An example is HMIPv6 [19]. A mobility anchor is a kind

of localized mobility management domain gateway. The regional care-of address is fixed at the mobility anchor while the local care-of address on the access router changes when the mobile node moves to a new IP link.

Micromobility Approach

A micromobility approach to localized mobility management requires host route propagation from the mobile node to a collection of specialized routers in the localized mobility management domain along a path back to a boundary router at the edge of the localized mobility management domain. A boundary router is a kind of localized mobility management

domain gateway. Localized mobility management is authorized with the access router, but reauthorization with each new access router is necessary on IP link movement, in addition to any reauthorization for basic network access. The host routes allow the mobile node to maintain the same IP address when it moves to a new IP link, and still continue to receive packets on the new IP link.

Edge Mobility Approach

In the edge mobility approach to localized mobility management, the access routers update bindings between the mobile node's care-of address and the mobile node's current IP link. The bindings are maintained at an edge mobility anchor point. No host involvement is required beyond movement detection. The mobile node requires no special authorization for localized mobility management service beyond the authorization required for basic network access. A mobile node's IP address does not change when the mobile node moves from one access router to another within the coverage area of the edge mobility anchor point, because the mobility anchor and access routers take care of changing the routing.

2.0 Requirements for Localized Mobility Management

Any localized mobility solution must naturally address the three problems described in [1]. In addition, the side effects of introducing such a solution into the network need to be limited. In this section, we address requirements on a localized mobility solution including both solving the basic problems and limiting the side effects.

Some basic requirements of all IETF protocols are not discussed in detail here, but any solution is expected to satisfy them. These requirements are interoperability, scalability, and minimal requirement for specialized network equipment. A good discussion of their applicability to IETF protocols can be found in [3].

Out of scope for the initial requirements discussion are QoS, multicast, and dormant mode/paging. While these are important functions for mobile hosts, they are not part of the base localized mobility management problem. In addition, mobility between localized mobility management domains is not covered here. It is assumed that this is covered by the global mobility management protocols.

2.1 Handover Performance Improvement (Requirement #1)

Handover packet loss occurs because there is usually latency between when the wireless link handover starts and when the IP link handover completes. During this time the mobile node is unreachable at its former topological location on the old IP link where correspondents are sending packets and to which the routing system is routing them. Such misrouted packets are dropped. This aspect of handover performance optimization has been the subject of an enormous amount of work, both in other SDOs, to reduce the latency of wireless link handover, and in the IETF and elsewhere, to reduce the latency in IP link handover. Many solutions to this problem have been proposed at the wireless link layer and at the IP layer.

Note that a related problem occurs when traffic packets are not routed through a global mobility anchor such as a Mobile IP home agent. Route optimized Mobile IPv6 [4] and HIP [5] are examples. A loss of connectivity can occur when both sides of the IP conversation are mobile and they both hand over at the same time. The two sides must use a global mobility anchor point, like a home agent or rendezvous server, to re-establish the connection, but there may be substantial packet loss until the problem is discovered.

In both cases, the loss of accurate routing caused the connection to experience an interruption which may cause service degradation for real time traffic such as voice

2.2 Reduction in Handover-related Signaling Volume (Requirement #2)

Considering Mobile IPv6 as the global mobility protocol (other mobility protocols require about the same or somewhat less), if a mobile node is required to reconfigure on every move between IP links, the following set of signaling messages must be done:

1) Movement detection using DNA [6] or possibly a link specific protocol,
2) Any link layer or IP layer AAA signaling, such as 802.1x [7] or PANA [8].
   The mobile node may also or instead have to obtain a router certificate using SEND [9], if the certificate is not already cached,
3) Router discovery which may be part of movement detection,
4) If stateless address autoconfiguration is used, address configuration and
   Duplicate Address Detection (unless optimistic Duplicate Address Detection [10] is used). If stateful address configuration is used, then
   DHCP is used for address configuration,
5) Binding Update to the home agent,
6) If route optimization is in effect, return routability to establish the binding key,
7) Binding Update to correspondent nodes for route optimization.

Note that Steps 1-2 will always be necessary, even for intra-link mobility, and Step 3 will be necessary even if the mobile node's care-of address can remain the same when it moves to a new access router.

This is a lot of signaling just to get up on a new IP link. Furthermore, in

some cases, the mobile node may need to engage in "heartbeat signaling" to keep the connection with the correspondent or global mobility anchor fresh, for example, return routability in Mobile IPv6 must be done at a maximum every 7 minutes even if the mobile node is standing still.

2.3 Location privacy (Requirement #3)

Location privacy in the context of IP mobility refers to hiding the geographic location of mobile users. Although general location privacy issues have been discussed in [12], the location privacy referred to here focuses on the IP layer and involves the basic property of the IP address that may change due to the mobility. The location information should not be revealed to nor deduced by the correspondent node without the authorization of the mobile node's owner. Since the localized mobility management protocol is responsible for the MN mobility within the local mobility management

domain, it should conceal geographical movement of the mobile node.

The threats to location privacy come in a variety of forms. Perhaps least likely is a man in the middle attack in which traffic between a correspondent and the mobile node is intercepted and the mobile node's location is deduced from that, since man in the middle attacks in the Internet tend to be fairly rare. More likely are attacks in which the correspondent is the attacker or the correspondent or even mobile node itself are relaying information on the care-of address change to someone. The owner of the correspondent or mobile node might not even be aware of the problem if an attacker has installed spyware or some other kind of exploit on the mobile node and the malware is relaying the change in care-of address to an attacker.

Note that the location privacy referred to here is different from the location privacy discussed in [14][15][16]. The location privacy discussed in these drafts primarily concerns modifications to the Mobile IPv6 protocol to eliminate places where an eavesdropper could track the mobile node's movement by correlating home address and care of address.

2.4 Efficient Use of Wireless Resources (Requirement #4)

Advances in wireless PHY and MAC technology continue to increase the bandwidth available from limited wireless spectrum, but even with technology increases, wireless spectrum remains a limited resource. Unlike wired network links, wireless links are constrained in the number of bits/Hertz by their coding technology and use of physical spectrum, which is fixed by the PHY. It is not possible to lay an extra cable if the link becomes increasingly congested as is the case with wired links.

Some existing localized mobility management solutions increase packet size over the wireless link by adding tunneling or other per packet overhead. While header compression technology can remove header overhead, header compression does not come without cost. Requiring header compression on the wireless access points increases the cost and complexity of the access points, and increases the amount of processing required for traffic across the wireless link. Since the access points tend to be a critical bottleneck in wireless access networks for real time traffic (especially on the

downlink), reducing the amount of per-packet processing is important. While header compression probably cannot be completely eliminated, especially for real time media traffic, simplifying compression to reduce processing cost is an important requirement.

2.5 Reduction of Signaling Overhead in the Network (Requirement #5)

While bandwidth and router processing resources are typically not as constrained in the wired network, wired networks tend to have higher bandwidth and router processing constraints than the backbone. These constraints are a function of the cost of laying fiber or wiring to the wireless access points in a widely dispersed geographic area. Therefore, any solutions for localized mobility management should minimize signaling within the wired network as well.

2.6 No Extra Security Between Mobile Node and Network (Requirement #6)

Localized mobility management protocols that have signaling between the host and network require a security association between the host and the network entity that is the target of the signaling. Establishing a security association specifically for localized mobility service in a roaming situation may prove difficult, because provisioning a mobile node with security credentials for authenticating and authorizing localized mobility service in each roaming partner's network may be unrealistic from a deployment perspective. Reducing the complexity of host to network security for localized mobility management can therefore reduce barriers to deployment.

Removing host involvement in localized mobility management also limits the possibility of DoS attacks on network infrastructural elements. In a host based approach, the host is required to have a global or restricted routing local IP address for a network infrastructure element, the mobility anchor point. The network infrastructural element therefore becomes a possible target for DoS attacks, even if hosts are properly authenticated. A properly authenticated host can either willfully or inadvertently give the network infrastructural element address to an attacker.

In summary, ruling out host involvement in local mobility management simplifies security by removing the need for service-specific credentials to authenticate and authorize the host for localized mobility management in the network and by limiting the possibility of DoS attacks on network infrastructural elements.

2.7 Support for Heterogeneous Wireless Link Technologies (Requirement #7)

The number of wireless link technologies available is growing, and the growth seems unlikely to slow down. Since the standardization of a wireless link PHY and MAC is a time consuming process, reducing the amount of work necessary to interface a particular wireless link technology to an IP network is necessary. A localized mobility management solution should ideally require minimal work to interface with a new wireless link technology.

In addition, an edge mobility solution should provide support for multiple wireless link technologies within the network in separate subnets. The edge mobility solution should also support handover between different wireless link technologies.

2.8 Support for Unmodified Hosts (Requirement #8)

A localized mobility management solution should be able to support any host that walks up to the link and has a wireless interface that can communicate with the network, without requiring localized mobility management software on the host. This approach has been extremely successful in the wireless LAN switching market, because it reduces the burden of host software installation on the user. In addition, being able to accommodate unmodified hosts enables a service provider to offer service to as many customers as

possible, the only constraint being that the customer is authorized for network access.

As a practical matter, there may be some constraints that require some configuration on the host. The host must have some kind of global mobility protocol if it is to move from one domain of edge mobility support to another, although no global mobility protocol is required if the host only moves within the coverage area of the localized mobility management protocol. Also, every wireless link protocol requires handover support on the host in the physical and MAC layers. Information from the MAC layer to the IP layer on the host may be necessary to trigger signaling for IP link handover. The localized mobility solution should be able to accommodate wireless link protocols with host handover support.

Another advantage of minimizing host changes for localized mobility management is that multiple global mobility management protocols can be supported with a localized mobility management solution that does not have host involvement. While Mobile IPv6 is clearly the global mobility management protocol of primary interest going forward, there are a variety of global mobility management protocols that might also need support, including proprietary protocols needing support for backward compatibility reasons. Within IETF, both HIP and Mobike are likely to need support in addition to Mobile IPv6, and Mobile IPv4 support may also be necessary.

2.9 Support for IPv4 and IPv6 (Requirement #9)

While most of this document is written with IPv6 in mind, localized mobility management is a problem in IPv4 networks as well. A solution for localized mobility that works for both versions of IP is desirable, though the actual protocol may be slightly different due to the technical details of how each IP version works. From Requirement #8 (Section 2.8), minimizing host support for localized mobility means that ideally no IP version-specific changes would be required on the host for localized mobility, and that global mobility protocols for both IPv4 and IPv6 should be supported. Any IP version-specific features would be confined to the network protocol.

3.0 Gap Analysis

This section discusses a gap analysis between existing proposals for solving localized mobility management and the requirement sin Section. 2.0.

3.1 Mobile IPv6 with Local Home Agent

One option is to deploy Mobile IPv6 with a locally assigned home agent in the local network. This solution requires the mobile node to somehow be assigned a home agent in the local network when it boots up. This home agent is used instead of the home agent in the home network. The advantage of this option is that the no special solution is required for edge mobility - the mobile node reuses the global mobility management protocol for that purpose - if the mobile node is using Mobile IPv6. One disadvantage is that Mobile IP has no provision for handover between home agents. Although such handover should be infrequent, it could be quite lengthy and complex.

The analysis of this approach against the requirements above is the following.

Requirement #1: If the mobile node does not perform route optimization, this solution reduces, but does not eliminate, IP link handover related performance problems.

Requirement #2: Similarly to Requirement #1, signaling volume is reduced if no route optimization signaling is done on handover.

Requirement #3: Location privacy is preserved for external correspondents, but the mobile node itself still maintains a local care-of address which a worm or other exploit could misuse. If the mobile node does perform route optimization, location privacy may be compromised, and this solution is no better than having a remote home agent.

Requirement #4: If traffic is not route optimized, the mobile node still pays for an over-the-air tunnel to the locally assigned home agent. The overhead here is exactly the same as if the mobile node's home agent in the home network is used and route optimization is not done.

Requirement #5: If the localized mobility management domain is large, the mobile node may suffer from unoptimzed routes since handover and mobility between home agents is not supported.

Requirement #6: A local home agent in a roaming situation requires the guest mobile node to have the proper credentials to authenticate with the local home agent in the serving network. In addition, as in Requirement #3, the local home agent's address could become the target of a DoS attack if revealed to an attacker. So a local home agent would provide no benefit for this requirement.

Requirement #7: This solution supports multiple wireless technologies in separate IP link subnets. No special work is required to interface a local home agent to different wireless technologies.

Requirement #8: The host must support Mobile IPv6 in order for this option to work. So host stack changes are required and other IP mobility protocols are not supported.

Requirement #9: This solution requires separate locally assigned home agents

for Mobile IPv4 and Mobile IPv6 since the local home agent should have MIP functions or IPv4 or IPv6 in conjunction with IP version of global mobility protocol, or some way to register an IPv4 care of address to home address mapping in an Mobile IPv6 home agent. While there are a couple of proposals currently active in the IETF for this (see [17] for one), it is not clear at this point whether they will be adopted for standards track development.

3.2 Hierarchical Mobile IPv6 (HMIPv6)

HMIPv6 [19] provides the most complete localized mobility management solution available today as an Internet RFC. In HMIPv6, a localized mobility anchor called a MAP serves as a routing anchor for a regional care-of address. When a mobile node moves from one access router to another, the

mobile node changes the binding between its regional care-of address and local care-of address at the MAP. No global mobility management signaling is required, since the care-of address seen by correspondents does not change.
This part of HMIPv6 is similar to the solution outlined in Section 3.1; however, HMIPv6 also allows a mobile node to hand over between MAPs.

Handover between MAPs and MAP discovery requires configuration on the routers. MAP addresses are advertised by access routers. Handover happens by overlapping MAP coverage areas so that, for some number of access routers, more than one MAP may be advertised. Mobile nodes need to switch MAPs in the transition area, and then must perform global mobility management update and route optimization to the new regional care-of address, if appropriate.

The analysis of this approach against the requirements above is the following.

Requirement #1 This solution shortens, but does not eliminate, the latency associated with IP link handover, since it reduces the amount of signaling and the length of the signaling paths.

Requirement #2 Signaling volume is reduced simply because no route optimization signaling is done on handover within the coverage area of the MAP.

Requirement #3 Location privacy is preserved for external correspondents, but the mobile node itself still maintains a local care-of address which a worm or other exploit could access by sending the local care-of address to third malicious node to enable it to track the MNÆs location.

Requirement #4 The mobile node always pays for an over-the-air tunnel to the MAP. If the mobile node is tunneling through a global home agent or VPN gateway, the wired link experiences double tunneling. Over-the-air tunnel overhead can be removed by header compression, however.

Requirement #5 From Requirement #1 and Requirement #4, the signaling overhead is no more or less than for mobile nodes whose global mobility management anchor is local. However, because MAP handover is possible, routes across large localized mobility management domains can be improved thereby improving wired network resource utilization by using multiple MAPs and handing over, at the expense of the configuration and management

overhead involved in maintaining multiple MAP coverage areas.

Requirement #6 In a roaming situation, the guest mobile node must have the proper credentials to authenticate with the MAP in the serving network. In addition, since the mobile node is required to have a unicast address for the MAP that is either globally routed or routing restricted to the local administrative domain, the MAP is potentially a target for DoS attacks across a wide swath of network topology.

Requirement #7 This solution supports multiple wireless technologies in separate IP link subnets.

Requirement #8 This solution requires modification to the hosts. In addition, the HMIPv6 design has been optimized for Mobile IPv6 hosts, and is not a good match for other global mobility management protocols.

Requirement #9 Currently, there is no IPv4 version of this protocol; although there is an expired Internet draft with a design for a regional registration protocol for Mobile IPv4 that has similar functionality.

3.3 Combinations of Mobile IPv6 with Optimizations

One approach to local mobility that has received much attention in the past and has been thought to provide a solution is combinations of protocols. The general approach is to try to cover gaps in the solution provided by MIPv6 by using other protocols. In this section, gap analyses for MIPv6 + FMIPv6 and HMIPv6 + FMIPv6 are discussed.

3.3.1 MIPv6 + FMIPv6

As discussed in Section 3.1, the use of MIPv6 with a dynamically assigned, local home agent cannot fulfill the requirements. A fundamental limitation is that Mobile IPv6 cannot provide seamless handover (i.e. Requirement #1).
FMIPv6 has been defined with the intent to improve the handover performance of MIPv6. For this reason, the combined usage of FMIPv6 and MIPv6 with a dynamically assigned local home agent has been proposed to handle local mobility.

Note that this gap analysis only applies to localized mobility management, and it is possible that MIPv6 and FMIPv6 might still be acceptable for global mobility management.

The analysis of this combined approach against the requirements follows.

Requirement #1 FMIPv6 provides a solution for handover performance improvement that should fulfill the requirements raised by real-time applications in terms of jitter, delay and packet loss. The location of the home agent (in local or home domain) does not affect the handover latency.

Requirement #2 FMIPv6 requires the MN to perform extra signaling with the access router (i.e. exchange of RtSolPr/PrRtAdv and FBU/FBA). Moreover, as in standard MIPv6, whenever the mobile node moves to another IP link, it must send a Binding Update to the home agent. If route optimization is

used,
the mobile node also performs return routability and sends a Binding Update
to each correspondent node. Nonetheless, it is worth noting that FMIPv6 should result in a reduction of the amount of IPv6 Neighbor Discovery signaling on the new link.

Requirement #3 The mobile node mantains a local care-of address. If route optimization is not used, location privacy can be achieved using bi-directional tunneling. However, as mentioned in Section 3.1, a worm or other malware can exploit this care of address by sending it to a third malicious node.

Requirement #4 As stated for Requirement #2, the combination of MIPv6 and FMIPv6 generates extra signaling overhead. For data packets, in addition to

the Mobile IPv6 over-the-air tunnel, there is a further level of tunneling between the mobile node and the previous access router during handover. This tunnel is needed to forward incoming packets to the mobile node addressed to the previous care-of address. Another reason is that, even if the mobile node has a valid new care-of address, the mobile node cannot use the new care of address directly with its correspondents without performing route optimization to the new care of address. This implies that the transient tunnel overhead is in place even for route optimized traffic.

Requirement #5 FMIPv6 generates extra signaling overhead between previous the access router and the new access router for the HI/HAck exchange. Concerning data packets, the use of FMIPv6 for handover performance improvement implies a tunnel between the previous access router and the mobile node that adds some overhead in the wired network. This overhead has more impact on star topology deployments, since packets are routed down to the old access router, then back up to the aggregation router and then back down to the new access router.

Requirement #6 In addition to the analysis for Mobile IPv6 with local home agent in Section 3.1, FMIPv6 requires the mobile node and the previous access router to share a security association in order to secure FBU/FBA exchange. So far, only a SEND-based solution has been proposed and this requires the MN to use autoconfigured Cryptographically Generated Addresses (CGAs)[20]. This precludes stateful address allocation using DHCP, which might be a necessary deployment in certain circumstances. Another solution based on AAA is under study but it could require extra signaling overhead over the air and in the wired network and it could raise performance issues.

Requirement #7 MIPv6 and FMIPv6 support multiple wireless technologies, so this requirement is fufilled.

Requirement #8 The host must support both MIPv6 and FMIPv6, so it is not possible to satisfy this requirement.

Requirement #9 Work is underway to extend MIPv6 with the capability to run over both IPv6-enabled and IPv4-only networks [17]. FMIPv6 only supports IPv6. Even though an IPv4 version of FMIP has been recently proposed, it is not clear how it could be used together with FMIPv6 in order to handle fast handovers across any wired network.

3.3.2 HMIPv6 + FMIPv6

HMIPv6 provides several advantages in terms of local mobility management. However, as seen in Section 3.2, it does not fulfill all the requirements identified in Section 2.0. In particular, HMIPv6 does not completely eliminate the IP link handover latency. For this reason, FMIPv6 could be used together with HMIPv6 in order to cover the gap.

Note that even if this solution is used, the mobile node is likely to need MIPv6 for global mobility management, in contrast with the MIPv6 with dynamically assigned local home agent + FMIPv6 solution. Thus, this solution should really be considered MIPv6 + HMIPv6 + FMIPv6.

The analysis of this combined approach against the requirements follows.

Requirement #1 HMIPv6 and FMIPv6 both shorten the latency associated with IP link handovers. In particular, FMIPv6 is expected to fulfill the requirements on jitter, delay and packet loss raised by real-time applications.

Requirement #2 Both FMIPv6 and HMIPv6 require extra signaling compared with Mobile IPv6. As a whole the mobile node performs signaling message exchanges at each handover that are RtSolPr/PrRtAdv, FBU/FBA, LBU/LBA and BU/BA. However, as mentioned in Section 3.2, the use of HMIPv6 reduces the signaling overhead since no route optimization signaling is done for intra-MAP handovers. In addition, na ve combinations of FMIPv6 and HMIPv6 often result in redundant signaling. There is much work in the academic literature and the IETF on more refined ways of combining signaling from the two protocols to avoid redundant signaling.

Requirement #3 HMIPv6 may preserve location privacy, depending on the dimension of the geographic area covered by the MAP. As discussed in Section 3.2, the mobile node still maintains a local care-of address that can be exploited by worms or other malware.

Requirement #4 As mentioned for Requirement #2, the combination of HMIPv6 and FMIPv6 generates a lot of signaling overhead in the network. Concerning payload data, in addition to the over-the-air MIPv6 tunnel, a further level of tunneling is established between mobile node and MAP. Notice that this tunnel is in place even for route optimized traffic. Moreover, if FMIPv6 is directly applied to HMIPv6 networks, there is a third temporary handover-related tunnel between the mobile node and previous access router. Again, there is much work in the academic literature and IETF on ways to reduce the extra tunnel overhead on handover by combining HMIP and FMIP tunneling.

Requirement #5 The signaling overhead in the network is not reduced by HMIPv6, as mentioned in Section 3.2. Instead, FMIPv6 generates extra signaling overhead between the previous access router and new access router for HI/HAck exchange. For payload data, the same considerations as for Requirement #4 are applicable.

Requirement #6 FMIPv6 requires the mobile node and the previous access router to share a security association in order to secure the FBU/FBA exchange. In addition, HMIPv6 requires that the mobile node and MAP share an IPsec security association in order to secure LBU/LBA exchange. The only well understood approach to set up an IPsec security association using of certificates, but this may raise deployment issues. Thus, the combination of FMIPv6 and HMIPv6 doubles the amount of host to network security protocol required, since security for both FMIP and HMIP must be deployed.

Requirement #7 HMIPv6 and FMIPv6 support multiple wireless technologies, so this requirement is fufilled.

Requirement #8 The host must support both HMIPv6 and FMIPv6 protocols, so this requirement is not fulfilled.

Requirement #9 Currently there is no IPv4 version of HMIPv6. There is an IPv4 version of FMIP but it is not clear how it could be used together with FMIPv6 in order to handle fast handovers across any wired network.

3.4 Micromobility Protocols

Researchers have defined some protocols that are often characterized as micromobility protocols. Two typical protocols in this category are Cellular-IP [21] and HAWAII [22]. Researchers defined these protocols before local mobility optimizations for Mobile IP such as FMIP and HMIP were developed, in order to reduce handover latency.

Cellular IP and HAWAII have a few things in common. Both are compatible with Mobile IP and are intended to provide a higher level of handover performance in local networks than was previously available with Mobile IP without such extensions as HMIP and FMIP. Both use host routes installed in a number of routers within a restricted routing domain. Both define specific messaging to update those routes along the forwarding path and specify how the messaging is to be used to update the routing tables and forwarding tables along the path between the mobile and a micromobility domain boundary router at which point Mobile IP is to used to handle scalable global mobility. Unlike the FMIP and HMIP protocols, however, these protocols do not require the host to obtain a new care of address on each access router as it moves; but rather, the host maintains the same care of address across the micromobility domain. From outside the micromobility domain, the care of address is routed using traditional longest prefix matching IP routing to the domain's boundary router, so the care of address conceptually is within the micromobiity domain boundary router's subnet. Within the micromobility domain, the care of address is routed to the correct access router using host routes.

Cellular IP and HAWAII differ in a few aspects. Cellular IP seems to be restricted, based on the nature of the protocol, to tree-based network topologies. HAWAII claims to be applicable in both tree-based and more complete network topologies. HAWAII documents more functionality in the realm of reliability and QoS interworking. Both protocols involve the mobile node itself in mobility operations, although this is also true of the Mobile IP based optimizations, so both protocols raise the same security

concerns with respect to authorizing address update as the Mobile IP based optimizations. HAWAII provides some analysis of network deployment scenarios including scale, density, and efficiency, but some of these assumptions seem very conservative compared to realistic cellular type deployments.

Micromobility protocols have some potential drawbacks from a deployment and scalability standpoint. Both protocols involve every routing element between the mobile device and the micromobility domain boundary router in all packet forwarding decisions specific to care of addresses for mobile nodes. Scalability is limited because each care of address corresponding to a mobile node generates a routing table entry, and perhaps multiple forwarding table entries, in every router along the path. Since mobile nodes can have multiple global care of addresses in IPv6, this can result in a large expansion in router state throughout the micromobility routing domain. Although the extent of the scalability for micromobility protocols is still

not clearly understood from a research standpoint, it seems certain that they will be less scalable than the Mobile IP optimization enhancements, and will require more specialized gear in the wired network.

The following is a gap analysis of the micromobility protocols against the requirements in Section 2.0:

Requirement #1 The micromobility protocols reduce handover latency by quickly fixing up routes between the boundary router and the access router. While some additional latency may be expected during host route propagation, it is typically much less than experienced with standard Mobile IP.

Requirement #2 The micromobility protocols require signaling from the host to the access router to initiate the host route propagation, but that is a considerable reduction over the amount of signaling required to configure to a new IP link.

Requirement #3 No care-of address changes are exposed to correspondent nodes or the mobile node itself while the mobile node is moving in the micromobility-managed network. Because there is no local care-of address, there is no threat from malware that exposes the location by sending the care-of address to an adversary.

Requirement #4 The only additional over-the-air signaling is involved in propagating host routes from the mobile node to the network upon movement. Since this signaling would be required for movement detection in any case, it is expected to be minimal. Mobile node traffic experiences no overhead.

Requirement #5 Host route propagation is required throughout the wired network. The volume of signaling could be more or less depending on the speed of mobile node movement and the size of the wired network.

Requirement #6 The mobile node only requires a security association of some type with the access router. Because the signaling is causing routes to the mobile node's care-of address to change, the signaling must prove authorization to hold the address.

Requirement #7 The micromobility protocols support multiple wireless technologies, so this requirement is satisfied.

Requirement #8 The host must support some way of signaling the access router on link handover, but this is required for movement detection anyway. The nature of the signaling for the micromobility protocols may require host software changes, however.

Requirement #9 Most of the work on the micromobility protocols was done in IPv4, but little difference could be expected for IPv6.

4.0 Security Considerations

Sections 2.3 and 2.6 discuss security considerations for edge mobility. Ideally, a single authentication and authorization of the host for entry into a serving network should be sufficient to authorize the host for

receiving edge mobility service as well as normal IP routing to and from the Internet. In the other direction, authentication and authorization of the access routers through RFC 3971 [9] should be sufficient for the host to trust the routing infrastructure, including for edge mobility. This limits the serving network's exposure to the host and the host's exposure to the serving network to two points: the NAS (which, in a wireless network is typically built into the wireless access points) and the access routers. Any additional network elements required to implement edge mobility are not directly accessible to the host.

Sections 2.3 and 2.6 also discuss how involving the host in localized mobility management can increase the probability of DoS attacks or expose location privacy information. Global mobility protocols such as Mobile IPv6 that require host to network signaling have the same vulnerability, however, the difference with localized mobility management is that the number of network entities involved and their management is expected to be minimal. In addition, while it would certainly be preferable if global IP mobility could be designed in a way to eliminate any global mobility anchor, the nature of IP routing seems to preclude such an option. Any doubts about the dangers spyware, viruses, and other malware could pose to a design that didn't seek to mitigate such threats can be assuaged by checking the volume of spam that comes through zombies and other compromised hosts.

5.0 Recommendation

In view of the gap analysis in Section 3.0, none of the existing solutions provide complete coverage of the requirements. FMIPv6 provides a complete solution to Requirement 3.1 but to no other requirement. FMIP, HMIP and micromobility protocols require that the MN is modified to support the additional functionality. But as analyzed above, the functionality provided by each protocol is does not fully support the set of requirements discussed in Section 2.0.

We therefore recommend that a new, network based localized mobility management protocol be developed that minimizes or eliminates host involvement. Such a localized mobility management protocol can be treated

as
part of the network infrastructure. This kind of architecture is required
to
address the gaps with existing protocols described in Section 3.0. The new
localized mobility management protocol can be paired with a link layer
specific IP link handover optimization protocol, such as are provided by
wireless LAN switches, or an IP link handover optimization protocol, such
as
FMIPv6, to eliminate handover related packet latency. The protocol should
minimize the number of specialized routers in the localized mobility
management domain to reduce the amount of state update needed upon
movement
and to allow standardized network equipment to be used where mobility
support is not required.

With the edge mobility approach, a mobile node has a single IP address
that
does not change when the mobile node moves from one access router to
another, because the mobility anchor and access routers take care of
changing the routing. An edge mobility approach does not require a
separate
security association with a network element, reducing the amount of
overhead
required to get a connection up on the network. In an edge mobility
approach,
hosts only have link local addresses for access routers, so it is much
more

difficult to mount off-link DoS attacks, and on-link attacks are easier to trace and stop. With the edge mobility approach, no authentication and authorization is necessary beyond that necessary for initial network access and whatever additional authentication and authorization is required by the wireless link layer upon movement between access points.

6.0 Author Information

James Kempf
DoCoMo USA Labs
181 Metro Drive, Suite 300
San Jose, CA 95110
USA
Phone: +1 408 451 4711
Email: kempf@docomolabs-usa.com

Kent Leung
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
USA
EMail: kleung@cisco.com

Phil Roberts
Motorola Labs
Schaumberg, IL
USA
Email: phil.roberts@motorola.com

Katsutoshi Nishida
NTT DoCoMo Inc.
3-5 Hikarino-oka, Yokosuka-shi
Kanagawa,
Japan
Phone: +81 46 840 3545
Email: nishidak@nttdocomo.co.jp

Gerardo Giaretta
Telecom Italia Lab
via G. Reiss Romoli, 274
10148 Torino
Italy
Phone: +39 011 2286904
Email: gerardo.giaretta@tilab.com

Marco Liebsch
NEC Network Laboratories
Kurfuersten-Anlage 36
69115 Heidelberg
Germany
Phone: +49 6221-90511-46
Email: marco.liebsch@ccrle.nec.de

7.0 Informative References

[1] Kempf, J., Leung, K., Roberts, P., Nishda, K., Giaretta, G., Liebsch, M., and Gwon, Y., "Problem Statement for IP Local Mobility," Internet Draft, work in progress.

[2] Manner, J., and Kojo, M., " Mobility Related Terminology", RFC 3753, June, 2004.

[3] Carpenter, B., "Architectural Principles of the Internet," RFC 1958, June, 1996.

[4] Johnson, D., Perkins, C., and Arkko, J., ôMobility Support in IPv6,ö RFC 3775.

[5] Moskowitz, R., Nikander, P., Jokela, P., and Henderson, T., "Host Identity Protocol", Internet Draft, work in progress.

[6] Choi, J, and Daley, G., " Goals of Detecting Network Attachment in IPv6", Internet Draft, work in progress.

[7] IEEE, "Port-based Access Control", IEEE LAN/MAN Standard 802.1x, June, 2001.

[8] Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., and Yegin, A., "Protocol for Carrying Authentication for Network Access (PANA)", Internet Draft, work in progress.

[9] Arkko, J., Kempf, J., Zill, B., and Nikander, P., "SEcure Neighbor Discovery (SEND)", RFC 3971, March, 2005.

[10] Moore, N., "Optimistic Neighbor Discovery", Internet Draft, Work in Progress.

[11] Ackerman, L., Kempf, J., and Miki, T., "Wireless Location Privacy: Law and Policy in the US, EU, and Japan", ISOC Member Briefing #15, http://www.isoc.org/briefings/015/index.shtml

[12] Haddad, W., Nordmark, E., Dupont, F., Bagnulo, M., Park, S.D., and Patil, B., " Privacy for Mobile and Multi-homed Nodes: MoMiPriv Problem Statement", Internet Draft, work in progress.

[13] Kivinen, T., and Tschopfening, H., " Design of the MOBIKE Protocol", Internet Draft, work in progress.

[14] Koodli, R., " IP Address Location Privacy and IP Mobility", Internet Draft, work in progress.

[15] Koodli, R., Devarapalli, V., Flinck, H., and Perkins, C., " Solutions for IP Address Location Privacy in the presence of IP Mobility", Internet Draft, work in progress.

[16] Bao, F., Deng, R., Kempf, J., Qui, Y., and Zhou, J., " Protocol for Protecting Movement of Mobile Nodes in Mobile IPv6", Internet Draft, work in progress.

[17] Wakikawa, R., Devarapalli, V., and Williams, C., " IPv4 Care-of Address Registration", Internet Draft, work in progress.

[18] Koodli, R., editor, ôFast Handovers for Mobile IPv6,ö Internet Draft, a

work in progress.
[19] Soliman, H., editor, ôHierarchical Mobile IPv6 Mobility Management,ö Internet Draft, a work in progress.

[20] Kempf, J., and Koodli, R., " Bootstrapping a Symmetric IPv6 Handover Key from SEND", Internet Draft, work in progress.
[21] Campbell, A., Gomez, J., Kim, S., Valko, A., and Wan, C., "Design, Implementation and Evaluation of Cellular IP", IEEE Personal Communications, June/July 2000.
[22] Ramjee, R., La Porta, T., Thuel, S., and Varadhan, K., "HAWAII: A domain-based approach for supporting mobility in wide-area wireless networks", in Proceedings of the International Conference on Networking Protocols (ICNP), 1999.

8.0 IPR Statements

9.0 Disclaimer of Validity

10.0 Copyright Notice