Locator ID Separation for Mobility Management in the New Generation Network*

Ved P. Kafle and Masugi Inoue
National Institute of Information and Communications Technology (NICT)
Tokyo, Japan
{*kafle, inoue*}*@nict.go.jp*

Abstract

Given that the majority of communications devices are mobile terminals, efficient mobility support should be a key feature in the new generation network or future Internet. The current Internet does not have native mobility support. Although variants of Mobile IP protocols have been developed to address this problem, these protocols cause signaling overhead, create a single point of failure, and lack smooth handover capabilities and interoperability between IPv4 and IPv6. Recently, locator ID separation has been considered as a promising approach to better mobility support, while also improving security and routing scalability. In this paper, we present the mobility-related functions of the recently proposed locator ID separation-based network architectures. We also outline their limitations and list some possible extensions that will be needed if they are to be deployed in the new generation network.

1 Introduction

The Internet does not support mobility natively because IP addresses have an overloaded semantic of both host identifiers (IDs) and locators [1]. Namely, an IP address is used in network layer protocols as a locator to find the destination host in the network topology and forward packets toward their destination. The same IP address is also used in the transport and upper layer protocols as the host ID to identify the host or sessions associated with the host. These layers use IP addresses in session IDs by binding the socket application program interface (API) with the IP address. When the host moves from one subnet to another and connects through a new attachment point, it acquires a new IP address, while invalidating the previous IP address. This terminates the session identified by the previous IP address.

Recently, variants of Mobile IP protocols [13, 14] have been developed to resolve the mobility limitations of Internet architecture. However, these protocols cause signaling overhead, create a single point of failure, and lack smooth handover capabilities and interoperability between IPv4 and IPv6.

The introduction of the locator ID separation concept, also known as ID/locator split (i.e., using separate namespaces for host IDs and locators) approach to network architecture simplifies mobility support functions. The Internet Engineering Task Force (IETF) and other segments of the Internet community have recently been discussing this approach as a concept that could not only aid mobility but also contribute to multihoming, routing scalability, and security [6, 7, 10]. Related work in ID/locator split-based mobility architectures includes the Host Identity Protocol (HIP) [10, 11], Location Independent Network Architecture (LIN6) [12], and Locator/ID Separation Protocol (LISP) [7]. However, since the introduction of the locator ID separation approach will significantly change the Internet architecture, this approach is more suitable for the new generation network or future Internet, which would be based on a clean-slate design. Some future network projects, such as the AKARI Project [4] and the 4WARD Project [5]), are designing network architectures on the basis of this concept.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 1, number: 2/3, pp. 3-15
*This is an invited paper.

This paper presents a comparative study of the mobility functions available in related work. It identifies those functions that have not been included in architectures such as HIP and LISP, which have been progressing under the auspices of the IETF, but are covered in the AKARI Project [4]. The Heterogeneity Inclusion and Mobility Adaptation through Locator ID Separation (HIMALIS) architecture [3] of the new generation network is being developed as part of the AKARI Project. The HIMALIS architecture provides mobility functions for handover optimization and supporting heterogeneous network layer protocols. Its mobility functions are performed by the identity layer, a new layer inserted between the network and transport layers, which supports mobility across different network layer protocols.

This paper is organized as follows. Section 2 discusses related studies, the lessons learned from them, and their limitations. Section 3 describes the mobility functions of ID/locator split architectures, with a focus on the HIMALIS architecture. Section 4 lists additional issues such as security and interoperability with other functions (e.g., multihoming, routing) of the ID/locator split-based mobility architecture. Section 5 concludes the paper.

2 Related Work

2.1 Mobile IP Protocols

Recognizing the limitations of the original Internet architecture in supporting mobility, a number of Mobile IP protocols [13, 14] have recently been developed and standardized in the IETF. These protocols enable a mobile host to possess two types of IP addresses: a home address and a care-of address. The home address, which is configured from the home network IP address prefix, is the persistent address. The mobile host can continue to use the home address even when it moves to a foreign network. The mobile host gets a care-of address in the foreign network and registers the binding between the home address and the care-of address in the home agent located in the home network. The home address is anchored at the home agent. That is, data packets sent at the home address do reach the home agent when the mobile host is not located in the home network. The home agent forwards these packets to the mobile host's care-of address after encapsulating them with an additional IP header. As the packets arrive at the mobile host, the Mobile IP functions installed in Layer 3.5 de-capsulate the packets and forward them to the upper layer (i.e., transport layer).

Mobile IP protocols such as [13, 14] are host-based mobility management protocols. In other words, the protocol functions are implemented in mobile hosts that detect movements and carry out location update signaling with the home agents. There are additional protocols to optimize the handover operation, either by localizing mobility signaling messages or by creating local tunnels between access routers to reduce packet loss during handovers. Hierarchical Mobile IP [15] confines the flow of signaling messages within the visited network domain and Fast Mobile IP [16] establishes a tunnel between access routers to forward packets destined for the mobile host from the previous access router to the new access router during handovers. Similarly, certain network-based mobility management protocols have also been standardized. The network mobility (NEMO) [17] and Proxy Mobile IP [18] protocols fall in this category, where the mobility management functions are executed not by the individual host but by network nodes such as the mobile routers or access routers.

By observing the Mobile IP related protocols' development activities in the IETF, we have learned that the new generation network should have both host- and network-based mobility support functions. It should also possess functions for supporting network mobility and reducing handover delay as well as packet losses, while minimizing signaling traffic. For this purpose, we give an overview of locator ID separation-based mobility management protocols being developed in the IETF [7, 11] and the AKARI project [2, 3]. The mobility management scheme should also be independent of the network-layer protocols so that the same scheme can be applied to both IPv4 and IPv6 as well as to any future network

protocols.

2.2 ID/Locator Split-Based Mobility Protocols

HIP [10, 11], LINA [12], LISP [7], and HIMALIS [3] fall into the category of ID/locator split-based mobility protocols because they use different sets of values for host IDs and locators.

HIP [11] uses public keys (and their hash values) as host IDs and IP addresses as locators. A new layer, called the identity layer, inserted between the transport and network layers of the host protocol stack performs the host ID-to-locator mapping functions. HIP extends the Domain Name System (DNS) records to store host IDs as well. A host acquires its peer host's ID and locator by sending a domain name lookup request to a DNS server. While communicating with the peer host, both the source and destination hosts' IDs appear in the identity header and locators in the network header of data packets. Although HIP is a good step in developing a locator ID separation-based mobility scheme, it is still in its infancy and lacks several functions. It has no support for smooth handover. Its session initiation process is computationally heavy, making it inappropriate for small, resource-limited devices. It uses locators in some signaling messages, thus necessitating the re-establishment of session contexts in the event of switching locators. This requirement is counterproductive to fast handover.

LINA [12] is another ID/locator split-based mobility protocol. Here, IDs of 128-bit length are formed by concatenating location-independent prefixes (of 64 bits) and node IDs (of 64 bits), while locators are formed by concatenating location-dependent network prefixes and node IDs. The network layer of the host protocol stack is divided into two sublayers: the identification sublayer and the delivery sublayer. The former carries out the ID-to-locator mapping function and the latter forwards packets using destination locators present in the packet header. It uses mapping agents to resolve IDs into corresponding locators. It is a host-based mobility approach, i.e., there is no support for network-based mobility and smooth handover.

LISP [7] uses prefix aggregateable endpoint IDs (EIDs), which are also used as locators in the edge network. In the transit network, routing locators (RLOC) are used as locators. EIDs to RLOCs mapping takes place in the Ingress and Egress Tunneling Routers (ITR/ETR) located in the border between the edges and the transit network. LISP's main focus is to reduce the global Border Gateway Protocol (BGP) routing table size by using fewer RLOCs in the transit network. Since it also uses EIDs as local locators in edge networks, it does not provide host mobility support. To provide host-mobility, there is a proposal for having the host possess a lightweight version of the ITR/ETR functions [8]. However, it may not be effective for reducing the BGP routing table size, if a distinct RLOC is assigned to each host. Obviously, LISP lacks smooth handover functions.

Considering the limitations of related work, we recently proposed the HIMALIS architecture [3] for the new generation network. Figure 1 shows the architectural components and the protocol stack in the HIMALIS architecture. The end hosts as well the border routers or gateways have the identity layer inserted between the network and transport layers. The identity layer executes mobility functions when it receives mobility indications from the network layer. The mappings between hostnames, IDs and locators are stored in two different registries: Domain Name Registry (DNR) and Host Name Registry (HNR). That is, these registries are used to resolve hostnames to IDs and locators during a communication initialization phase. The border routers connecting edge networks to the global transit network also cache ID-to-locator mapping data in their ID tables. The border routers distribute ID-to-locator-mapping updates in the event of host mobility. This architecture supports a hybrid of host- and network-based mobility. The end nodes as well as network nodes, such as border routers, maintain host ID-to-locator mapping caches, participate in mobility signaling and use host IDs present in the identity header as the reference value to dynamically change locators present in the network layer header, while keeping the change hidden from the transport and application layers. Thus, the architecture is mobility friendly. In

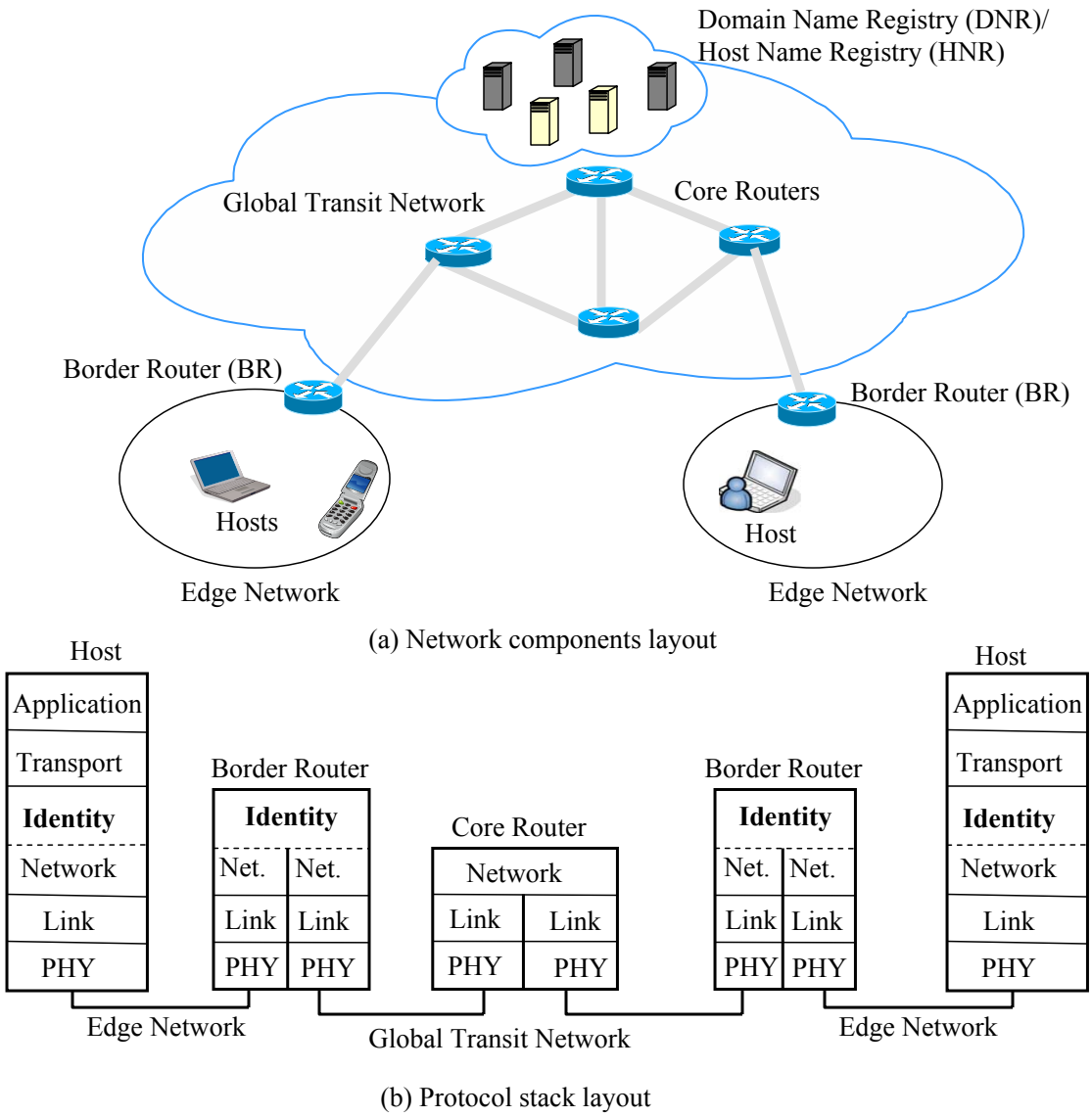

Figure 1: ID/locator split architecture components and protocol stack

fact, HIMALIS provides other support, such as for heterogeneous network layer protocols and resource constrained nodes. We refer the interested reader to [3] for additional descriptions of the architecture.

3 Mobility Related Functions in ID/Locator Split Architectures

In this section, we discuss the different types of mobility-related functions available in the ID/locator split architectures.

3.1 Name Resolution System

Mobility support requires the name resolution system to have functions not only for faster resolution of hostnames to locators but also for faster update of the records in the event of changing locators when

mobile hosts move. The Internet employs the DNS to resolve domain names into IP addresses and other resources. Internet applications resolve the domain name into an IP address during a communication initialization phase via a DNS record lookup process. Although DNS has been providing scalable and faster name resolution, it is not suitable for fast updating of the hosts' dynamic information, because of the existence of multiple cached copies in the global DNS server system. For efficient mobility support, in addition to DNS, a new mapping system is needed to store hosts' dynamic information, such as locators. In fact, the new mapping system would work as the fixed anchor point, where mobile hosts' reachability information is stored and updated. The rendezvous servers in HIP and host name registries in HIMALIS serve as the fixed anchor points.

In HIP [11], mobile hosts' domain names and their static rendezvous server's locators are registered with the DNS, while the mobile host's locator is stored in the rendezvous server. When a correspondent host wants to communicate with the mobile host, the correspondent host resolves the mobile host's fully qualified domain name (FQDN) into the host ID and locator by sending a name resolution query to a DNS server. The host locator received in the response is in fact the locator of the rendezvous server. Therefore, the first packet sent by the correspondent host to the mobile host's ID and locator goes to the rendezvous server, which searches its database for the mobile host's locator to relay the packet to the mobile host's current location. When the mobile host changes its locator due to mobility, it sends a location update request to the rendezvous server. Thus, the rendezvous servers are somewhat similar to the home agents in Mobile IP.

Similarly, in LISP [7], mapping servers [9] are used to store dynamic mapping between host IDs and locators. LISP mapping servers provide ID-to-locator mapping records to ITRs. Unlike HIP's rendezvous servers, LISP mapping servers do not receive and relay the first data packet.

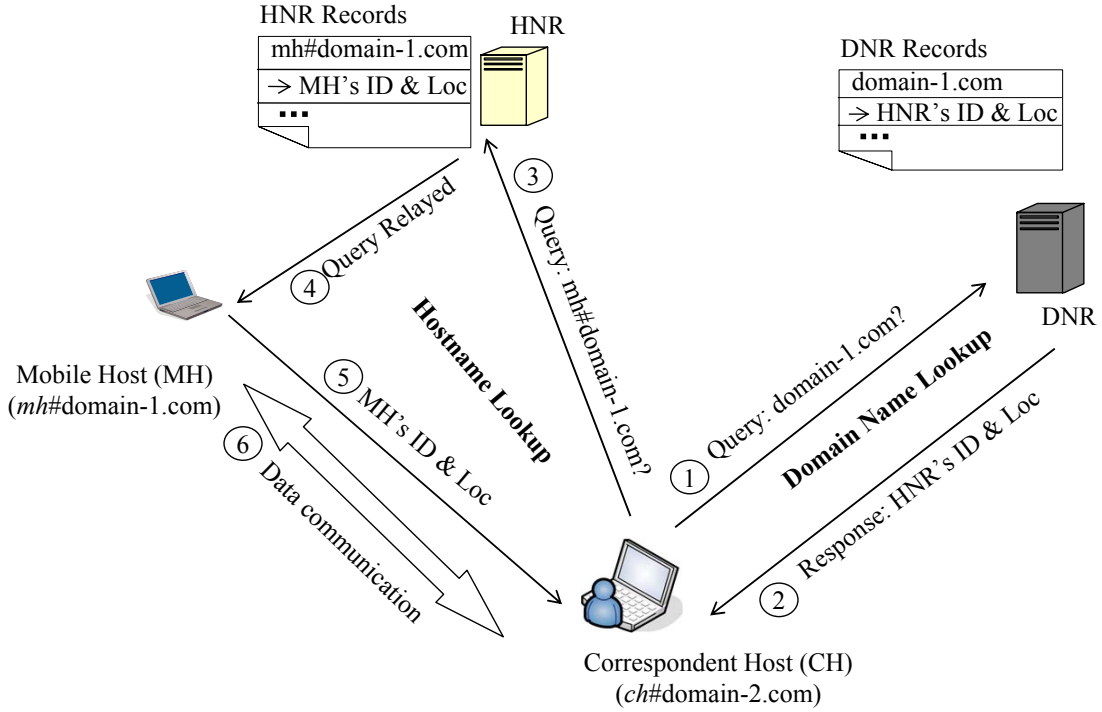

Figure 2: Hostname resolution process

In HIMALIS [3], the HNRs are the fixed anchor points that store the locators of mobile hosts, whereas the HNRs' locators are stored in the DNR. To make the hostname resolution process efficient, the for-

mat of the global hostname is changed slightly. In the current Internet, the domain name and hostname semantics are mixed together. In contrast, the HIMALIS architecture separates the global domain name and local hostname by using a hash "#" sign. That is, a global hostname is formed by concatenating its local hostname and global domain name with the # sign. For example, if a mobile host with a local hostname kafle-pc is administratively associated with a domain nict.go.jp, its global hostname would be kafle-pc#nict.go.jp. In the communication initialization phase, a correspondent host resolves the mobile hosts' hostname into the host ID and locator in two steps, as shown in Figure 2. Suppose the correspondent host (hostname: ch#domain-2.com) wants to communicate with the mobile host (hostname: mh#domain-1.com). The correspondent host first sends a domain name resolution request to a DNR and gets the HNR's ID and locator. It then sends a hostname resolution request to the HNR. The HNR searches its database for the record containing the mobile host's ID and locator.

The HNR may have two choices in sending the host ID and locator mapping record: (1) it may send the record directly to the correspondent host, or (2) it may relay the hostname resolution request to the mobile host. Figure 2 depicts the second choice, which may have the following advantages:

1. If the mobile host is multihomed to different networks and has several locators, it can select the most appropriate locator for the communication with the correspondent host. The network resource availability and intended service requirements (if the name resolution request also includes information about the type of communication service the correspondent host wants to have with the mobile host) can be used as decision parameters in the locator selection process.

2. HNR record update frequency of a multihomed host can be reduced by registering only a locator belonging to the network that has the widest coverage (e.g., a locator associated with a cellular network or an explicit signaling network such as that used in the MIRAI architecture [19]). The locators associated with other networks are not registered in the HNR. For example, a mobile host with both cellular and wireless LAN interfaces would require only registration of the locator associated with the cellular network.

3.2 Mobility Functions in Hosts and Network Nodes

Host-based mobility support requires the host protocol stack to possess functions to carry out the following tasks: detect movement, configure a new locator, carry out location update signaling, use the new locator in data packet headers, and hide the locator change from the upper layers. The mobility detection and new locator configuration tasks are usually performed by the network layer protocols. The remaining tasks are performed by the mobility specific functions located in Layer 4 (i.e., in the identity layer in HIP and HIMALIS) or in Layer 3.5 (in LINA and Mobile IP).

Since the inclusion of ID/locator split functions in the host protocol stack naturally enables hosts to detect movement and carry out mobility-related signaling, pure network-based mobility support (such as in Proxy Mobile IP, where hosts do not carry out any mobility related functions), is not required in ID/locator split architectures. Similarly, ID/locator mapping functions installed in border routers or gateways for making the core routing scalable or providing traffic engineering (as proposed in LISP and HIMALIS) are also helpful to handover optimization, mobility across heterogeneous network protocols, and route optimization.

3.3 Handover Optimization

Handover optimization functions aim at reducing one or more of the following three parameters: handover delay, packet loss during handover, and signaling traffic due to handover. Among the ID/locator split-based architectures, only HIMALIS possesses handover optimization functions. These functions

are distributed both in the end hosts and in the border routers, which exchange the mobile host's locator update signaling and forward packets from the previous border router to the new border router. By doing so, handover delay is reduced and packet losses are also avoided. The basic concept of handover optimization is similar to that used in Fast Mobile IP [16]. The steps of the handover process are shown in Figure 3.

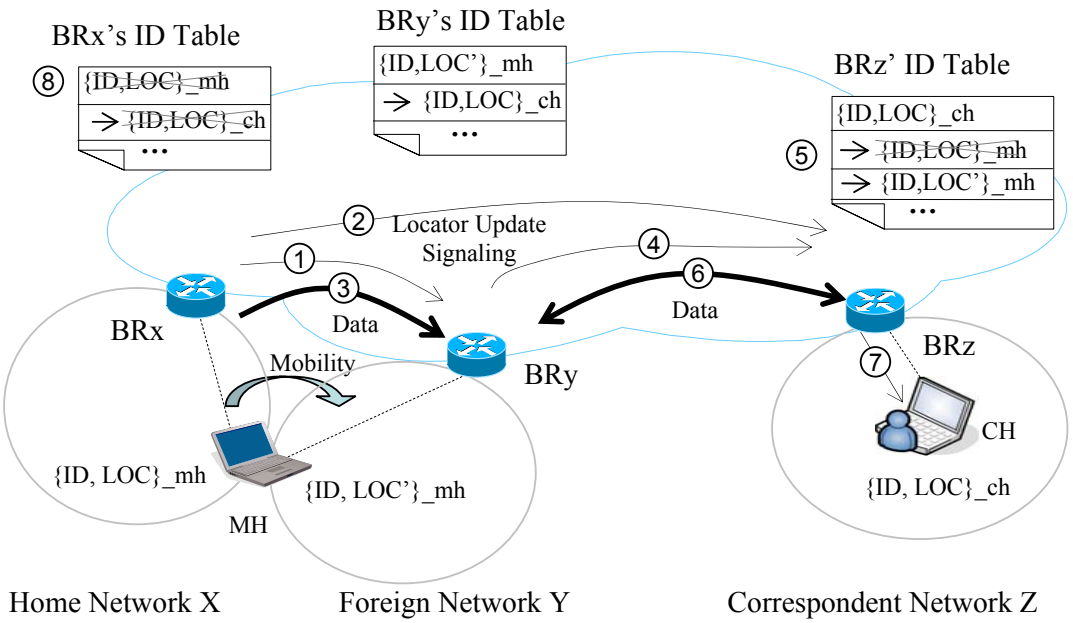

Figure 3: Handover process in a homogeneous network

Figure 3 also shows the ID and locator mapping caches maintained in the ID tables of border routers (BRs) when a mobile host (MH) located in its home network X is communicating with a correspondent host (CH) located in the correspondent network Z. Here, we consider mobility across homogeneous networks, namely the home network, foreign network, and correspondent network are using the same network layer protocol[1]. {ID, LOC}_mh and {ID, LOC}_ch represent the host ID and locator pairs of the mobile host and correspondent host, respectively. The MH moves to the foreign network Y while continuing a communication session with the CH. The handover can be of make-before-break or break-before-make type, depending on the access networks' configuration and MH's capability. That is, in the former type, the MH gets a new locator LOC'_mh from the foreign network Y while it is still connected to its home network. In this case, the MH informs the home border router BRx of the new locator by using the previous link. In the latter type of handover, by contrast, the MH is disconnected from its home network first and then connects to the foreign network. In this case, the MH cannot directly inform the home border router BRx of its new locator; rather, it provides the ID and locator of BRx to BRy, using the new link established in the foreign network. BRy then informs BRx of the MH's new locator as well as BRy's ID and locator. Using these values, BRx translates destination locators of the packets received for the MH during handovers and forwards them toward BRy.

The circled numbers in the figure indicate the following mobility steps. On receiving the MH's new locator, either directly from the MH or from BRy, BRx (1) transfers the CH's ID-to-locator mapping

[1]Mobility across heterogeneous networks is described in the next subsection.

record, i.e., {ID, LOC}_ch, to BRy and (2) sends a location update request containing the MH's host ID and new locator, i.e., {ID, LOC'}_mh, to BRz. The signaling messages are followed by the corresponding acknowledgments (not shown in the figure). (3) BRx translates the destination locator into the MH's new locator in the packets destined for the MH and forwards the packets to BRy. (4) On receiving the ID-to-locator mapping record of the MH's correspondent host, BRy also sends the MH's mapping update {ID, LOC'}_mh to BRz to confirm the mobility. (5) BRz updates the MH's ID-to-locator mapping in its ID table. (6) BRz translates the destination locator into the new locator in the packets destined for the MH and forwards them to BRy. That is, the MH and CH communicate via BRy and BRz. (7) BRz also relays the location update message to the CH, which starts using the new locator as the destination locator in the network header of the packets destined for the MH. On receiving the packets, BRz stops locator translation. By this time, the MH also has already sent a location update request to its HNR to update its record (not shown in the figure). Once the MH receives the location update acknowledgment from the HNR, it sends a message to BRx to delete its ID-to-locator mapping entry from the ID table. (8) BRx deletes the MH's ID-to-locator mapping entry. This completes the handover process.

Note that the location update signaling to the correspondent host is hidden from the mobile host while it is carried out by the border routers. This transparent signaling process is helpful for supporting mobility across heterogeneous networks, as discussed in the next subsection.

3.4 Mobility Across Heterogeneous Network Protocols

HIMALIS also supports mobility across heterogeneous network layer protocols if the mobile host has a dual protocol stack. For example, the mobile host can move from an IPv6 network to another IPv4 network.

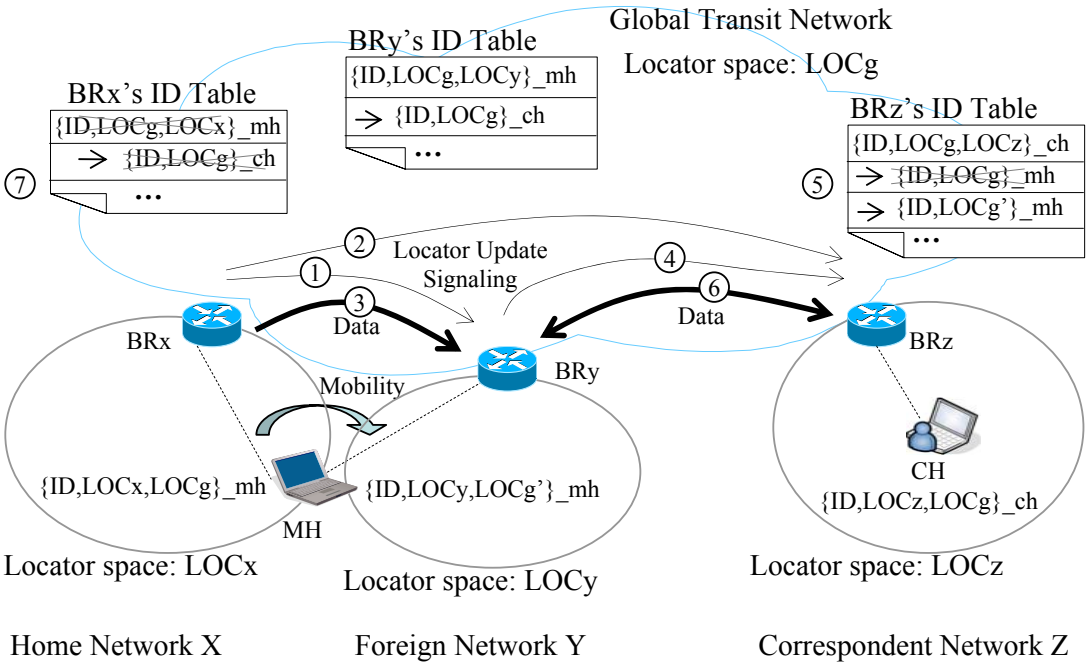

Figure 4: Handover process in heterogeneous networks

Figure 4 shows a network configuration where the edge networks and the global transit network use different types of network layer protocols and locator spaces. The home network, foreign network, and

correspondent network may also use different network layer protocols and locator spaces. LOCg indicates the locator space used in the global transit network. Similarly, LOCx, LOCy, and LOCz denote the local locator spaces used in the edge networks X, Y, and Z, respectively. LOCx_mh, and LOCy_mh are the locators of the mobile host configured from locator spaces LOCx and LOCy, respectively. Similarly, LOCz_ch is the correspondent host's locator configured from locator space LOCz. LOCg_mh and LOCg'_mh represent global locators of the mobile host when it is located in the home network and foreign network, respectively. Similarly, LOCg_ch represents the correspondent host's global locator. These global locators are in fact the locators of the upstream links of the border routers BRx, BRy, and BRz, respectively, configured from the global network locator space LOCg. These border routers also have locators LOCx_br, LOCy_br, and LOCz_br configured from the local locator spaces LOCx, LOCy, and LOCz, respectively. The border routers understand both the global and local network protocols and translate the local network protocols and locators into the global network protocol and locators, and vice versa.

In a heterogeneous networking environment, the border routers maintain the ID tables storing both the global and local locators of local hosts and the global locators of remote hosts with which the local hosts are communicating. That is, when the MH is located in the home network X, BRx's ID table stores {ID, LOCg, LOCx}_mh. And when the MH starts communication with the CH, the latter's ID and global locator, i.e., {ID, LOCg}_ch, are added to the MH's entry in BRx's ID table. The MH is also aware of its global locator (supplied by the border router BRx when the MH associates with it), although it does not know the protocol where the locator is used. The MH uses its global location in the locator update signaling message in the event of mobility (as described latter.)

The border router uses the ID table for translating network layer protocols when packets flow from the global network to the edge network, and vice versa. When packets destined for the MH from the CH arrive at BRx through the global transit network, they contain ID_mh and ID_ch as the destination and source IDs in the identity header, as well as LOCg_mh and LOCg_ch as the destination and source locators in the network header. BRx searches its ID table and finds LOCx_mh as the local locator of the MH, translates the network layer protocol, and uses LOCx_mh and LOCx_br (i.e., BRx's local locator) as the destination and source locators, respectively. Similarly, the packet originating from the MH contains ID_ch and ID_mh as the destination and source IDs in the identity header, as well as LOCx_br and LOCx_mh as the destination and source locators in the network header. When BRx receives the packet, it searches its ID table for the CH's ID-to-locator mapping, i.e., {ID, LOCg}_ch. It then translates the edge network protocol into the global network protocol while using LOCg_ch and LOCg_mh as the destination and source locators, respectively.

Figure 4 shows the handover procedure, the steps in which are similar to those discussed in the previous subsection. For the make-before-break type of handover, the MH informs BRx directly of its new global locator LOCg'_mh. With the break-before-make type of handover, however, the MH does this through the border router BRy of the foreign network. The circled numbers in the figure indicate the following steps: On receiving the MH's new locator, BRx (1) transfers the CH's ID-to-global locator mapping record, i.e., {ID, LOCg}_ch, to BRy and (2) sends a location update request containing the MH's host ID and new locator, i.e., {ID, LOCg'}_mh, to BRz. (3) BRx forwards the packets destined for the MH to BRy. (4) BRy also sends the MH's ID-to-locator mapping update, i.e., {ID, LOCg'}_mh, to BRz to confirm the mobility. (5) BRz updates the MH's ID-to-locator mapping in its ID table. (6) BRz translates the destination locator into the new locator in the packets destined for the MH and forwards them to BRy. By this time, the MH has already sent a location update request to its HNR to update its record (not shown in the figure). Once the MH receives the location update acknowledgment from the HNR, it sends a message to BRx to delete its ID-to-locator mapping entry from the ID table. (7) BRx deletes the MH's ID-to-locator mapping entry. This completes the handover process.

Since the signaling and packet redirecting functions are distributed in the border routers, the HI-

MALIS architecture supports a hybrid of both network-based mobility such as Proxy Mobile IPv6 [18] and Network Mobility (NEMO) [17], and host-based mobility such as Mobile IP [14] of the current Internet. We call this type of mobility Host Initiated Network Assisted (HINA) mobility. The pure network-based or pure host-based mobility management approaches are not suitable for heterogeneous networks for the following reasons: In host-based mobility management, movement detection and consequent signaling operations are handled by the mobile host. Since, in heterogeneous networks, the mobile host cannot communicate with correspondent host without getting protocol translation support from border routers, it is not capable to exchange signaling messages with the correspondent host or the HNR that are located outside the mobile host's edge network. Similarly, in pure network-based mobility, the mobile host is kept unaware of its movement by falsely presenting the new network's subnet prefixes. In heterogeneous networks, however, the mobile host should explicitly know about the network protocol change during the mobility. Therefore, the HINA hybrid mobility management is necessary for heterogeneous networks.

4 Additional Issues with ID/Locator Split-based Mobility

There are several issues related to the deployment of ID/locator split-based mobility functions. Among them, in this section, we discuss security, ID-to-locator mapping records optimization, and interoperability with other functions such as multihoming and scalable routing.

4.1 Security

ID/locator split-based mobility functions of the HIMALIS architecture raise severe security issues because they require securely maintaining dynamic mapping information between host IDs and locators at various points in the network. Since this architecture requires network nodes such as border routers to send location update signaling messages on behalf of mobile hosts, vulnerabilities could arise if proper security functions are not implemented in the border routers as well as in the hosts.

The security issues and their possible solutions are as follows:

1. Authentication of mobile hosts for network access: When a mobile host moves from one edge network to another, it has to authenticate itself in the new edge network before the edge network allows the mobile host to use its network resources. For this purpose, the mobile host may present some credential, e.g., a certificate received from a mutually trusted certificate agency, to the border router of the new network. On verifying the mobile host's credential, the border router creates an entry in its ID table for the visited mobile host's ID and locator and grants network resources (e.g., locators and bandwidth) to the mobile host.

2. Authentication between hosts: As with certain secured services in the present day Internet, the new generation network requires hosts to authenticate each other to access communication services provided by the peer host. HIP [11] contains a security mechanism for this purpose. It employs public key cryptography, certificates, and challenge-response type of security mechanisms to enable hosts to authenticate each other. HIMALIS can also use similar security mechanisms when strong security is needed. Since HIP-like security functions are computationally heavy for resource-limited devices, lightweight security functions need to be explored to ensure that the ID/locator split-based mobility architecture is widely deployable.

3. Authentication of border routers: In HIMALIS, not only end hosts but also network nodes such as border routers take part in mobility signaling on behalf of mobile hosts. This creates severe

security implications. A malicious entity can send location update messages to highjack communication sessions belonging to other hosts. Therefore, the border routers must be authenticated before any location update messages are accepted by other border routers or hosts. Border routers belonging to the same administrative domain can use a shared secret for this verification purpose. For border routers belonging to different administrative domains, we need to find an effective security mechanism.

4. Verification of signaling messages and data packets: We also need security mechanisms to verify that the location update signaling messages have come from the authenticated entity (host or router). Similarly, we should also be able to verify that data packets are from the authenticated host and that the integrity of the packet is intact.

4.2 Optimizing ID-to-Locator Mapping Records

The performance of the ID-locator split-based mobility architecture relies heavily on maintaining up-to-date ID-to-locator mapping records at different network locations. The two-step name resolution used in the HIMALIS architecture may increase the time needed to retrieve the host ID and locator related to a hostname. Consequently, optimization is necessary. For this purpose, the two-step resolution process can be converted into a one-step process by having the DNR forward the hostname resolution request to the HNR, instead of replying to the querying host with the HNR's ID and locator. This can reduce the time required for the DNR's response message to reach the querying host and the time needed to issue another hostname resolution request from the querying host. Similarly, in the event of mobility, we need to minimize the time required to update the host locator in the HNR record, to prevent the host from becoming unreachable.

4.3 Interoperability with Other Functions

Since ID/locator split-based network architecture is also helpful to other functions such as multihoming, routing, and traffic engineering, these functions should not be adversely affected by those implemented for mobility management. Therefore, when developing an ID/locator split concept-based new generation network, we should carry out research to optimize the whole system, rather than optimizing a specific task associated with a particular function. For example, having a function for traffic engineering can solve the problem of route optimization that may be caused by a mobility function. Similarly, having multihoming functions can facilitate mobility by utilizing multiple connections simultaneous during handovers. Thus, we can share many functions for multiple purposes, if we think of the whole system and its optimization together.

5 Conclusion

This paper presented an overview of the mobility functions of network architectures based on the ID/locator split approach. These functions include name resolution, handover optimization, and supporting mobility across heterogeneous network protocols. The locator ID separation approach simplifies mobility management at the cost of maintaining and distributing ID-to-locator mapping records and translating locators in border routers. These tasks raise many security issues. For this reason, future work should address the security issues and seek to reduce the cost of maintaining up-to-date ID-to-locator mapping records.

Acknowledgments

The authors would like to thank the researchers at the Network Architecture Group of the New Generation Network Research Center of NICT and the members of the AKARI Architecture Design Project for their valuable suggestions during the discussion on the research reported in this paper.

References

[1] J. Saltzer, "On the naming and binding of network destinations," RFC 1498, Aug. 1993.

[2] V. P. Kafle, H. Otsuki, and M. Inoue, "An ID/locator split architecture for future networks," IEEE Commun. Mag., Vol. 48, No. 2, pp. 138-144, Feb. 2010.

[3] V. P. Kafle and M. Inoue, "HIMALIS: Heterogeneity inclusion and mobility adaptation through locator ID separation in new generation networks," IEICE Trans. on Commun., Vol. E93-B, No. 3, pp. 478-489, March 2010.

[4] AKARI Architecture Design Project for New Generation Network, http://akari-project.nict.go.jp

[5] The FP7 4WARD Project, http://www.4ward-project.eu

[6] E. Nordmark and M. Bagnulo, "Shim6: Level 3 multihoming shim protocol for IPv6," RFC, June 2009.

[7] D. Farinacci, V. Fuller, D. Meyer and D. Lewis, "Locator/ID separation protocol (LISP)," Internet-Draft, draft-ietf-lisp-07, April 2010.

[8] D. Farinacci, V. Fuller, D. Lewis, and D. Meyer, "LISP mobile node," Internet-Draft, draft-meyer-lisp-mn-03, Aug. 2010.

[9] V. Fuller and D. Farinacci, "LISP map server," Internet-Draft, draft-ietf-lisp-ms-05, April 2010.

[10] R. Moskowitz and P. Nikander, "Host indentity protocol architecture," RFC 4423, May 2006.

[11] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, "Host identity protocol," RFC 5201, April 2008.

[12] M. Ishiyama, M. Kunishi, K. Uehara, H. Esaki, and F. Teraoka, "LINA: A new approach to mobility support in wide area networks," IEICE Trans. Commun. Vol. E84-B, No. 8, pp. 2076-2086, August 2001.

[13] C. Perkins, "IP mobility support for IPv4," RFC 3344, Aug. 2002.

[14] D. Johnson, C. Perkins, and J. Arkko, "Mobility support in IPv6," RFC 3775, June 2004.

[15] H. Soliman et al., "Hierarchical mobile IPv6 mobility management (HMIPv6)," RFC 4140, Aug. 2005.

[16] R. Koodli, "Fast handovers for mobile IPv6," RFC 4068, July 2005.

[17] V. Devarapalli et al., "Network mobility (NEMO) basic support protocol," RFC 3969, Jan. 2005.

[18] S. Gundavelli et al., "Proxy mobile IPv6," RFC 5213, Aug. 2008.

[19] G. Wu, M. Mizuno, and P. Havinga, "MIRAI architecture for heterogeneous network," IEEE Commun. Mag., Vol. 20, No. 2, pp. 126-134, Feb. 2002.

Ved P. Kafle received the B.E. degree in electronics and electrical communications from Punjab Engineering College (now PEC University of Technology), Chandigarh, India, in 1995. He received the M.S. degree in computer science and engineering from Seoul National University, South Korea, in 2003 and the Ph.D. in informatics from the Graduate University for Advanced Studies, Japan, in 2006. Since 2006, he has been working as a researcher at the National Institute of Information and Communications Technology (NICT), Japan. He is also a member of the AKARI Architecture Design Project for New Generation Networks. He is involved in designing new generation network architectures and protocols, considering emerging (as well as future) network environments and application requirements. In particular, he is currently investigating the research challenges of node identification and location architectures of the New Generation Network or future Internet. He has been awarded with the ITU Association of Japan Award in 2009 for his active contributions to the standardization of Next Generation Network architectures. He also received the best paper award (second prize) at the ITU-T

Kaleidoscope event on Innovations for Digital Inclusion, 2009. He is a member of the IEEE, Nepal Engineers' Association, and Nepal Engineering Council.

Masugi Inoue received the B.E. degree from Kyoto University in 1992 and the M.E. and D.E. degrees from the University of Tokyo in 1994 and 1997, respectively, all in electrical engineering. He is currently a Research Manager of the Network Architecture Group at NICT. He is leading studies on future mobile and sensor access networks, ID/locator-split architectures, and secure personal and group networking. He is also a member of the AKARI Architecture Design Project for New Generation Networks. He has been engaged in RD of ultrahigh-speed WLANs, wireless and mobile networks, ubiquitous computing, and future generation network architectures since he joined the Communications Research Laboratory (CRL), which was reorganized as NICT in 2004. He was a visiting researcher at Polytechnic University (now the Polytechnic Institute of NYU), Brooklyn, NY, in 2000. He is a member of the Technical Committees on Information Networks, Mobile Multimedia Communications, and Ubiquitous Sensor Networks of IEICE, a member of the New Generation Network Promotion Forum, Ubiquitous Networking Forum, and Next Generation IP Network Promotion Forum.