International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 13 (2015) pp 33583-33586

An IP mobility management framework based on handover type differentiation and distributed location management

Sangyup Han[1], Myungchul Kim[1], Kyounghee Lee[2]*, Kwihoon Kim[3], Hyunjae Kim[3] and Woongshik You[3]
[1]Department of Computer Science, KAIST, Daejeon, Korea
[2]Department of Computer Engineering, Pai Chai University, Daejeon, Korea
[3]Future Research Creative Laboratory, ETRI, Daejeon, Korea
[1]{ilu8318,mck}@kaist.ac.kr, [2]leekhe@pcu.ac.kr, [3]{kwihooi,khjgo,wsyou}@etri.re.kr
*Corresponding Author

Abstract- Nowadays, mobile network operators provide heterogeneous access networks, such as LTE and Wi-Fi, and users frequently change their connections among various access networks by considering cost, bandwidth, and coverage. However, the current mobile networks do not provide a solution for 'wide-area' IP mobility due to difficulty and risks from large-scale network upgrade and access-technology heterogeneity. In this paper, we propose an enhanced IP mobility management framework for evolving mobile communication environment represented as 5G network. The proposed framework separates a mobile node's handover control from its location management performed with a distributed manner like Domain Name System (DNS), thereby achieving the localized and fast control procedure for IP handovers. In addition, the proposed framework differentiates control schemes for IP handovers according to their types (i.e., forward-forward and forward-backward) to increase control efficiency.

Keywords- IP Mobility, 5G Network, Handover Types, Distributed Location Management, Localized Handover Control

1 Introduction

Mobile communication technology in cellular networks has evolved by the 3rd Generation Partnership Project (3GPP). In terms of mobility service, the 3GPP networks have advanced on the basis of cellular network architecture by partially accommodating other popular access technology, such as Wi-Fi. On the other hand, Internet has worked up to the current successful state based on the standards of Internet Engineering Task Force (IETF) which started from interworking issues among fixed networks. They mainly deal with mobility issue at IP layer or higher. Thus we have two different core network architectures for cellular network and Internet. This becomes one of the main reasons that seamless IP mobility service over heterogeneous networks has not been widely deployed yet.

On observing IP mobility technology for a couple of decades, we may see the existing approaches did not prove their sufficient scalability and efficiency to be easily deployed in the operator networks. Two most popular IP mobility support protocols, Mobile IP (MIP) [1] and Proxy MIPv6 (PMIPv6) [2], also have limitations of inefficient routing path, traffic concentration on a specific node, or high complexity on managing tremendous location information and controlling frequent handovers of millions of mobile nodes (MNs).

In this paper, we propose an enhanced IP mobility management framework focusing on simplicity and scalability required for evolving communication environment (e.g., 5G networks). The proposed framework employs Uniform Resource Identifier (URI) for host identification while the existing approaches generally use IP address for the same purpose. This enables a lot of MNs' location information to be well distributed into a system like widely-used Domain Name System (DNS). In the proposed framework, the handover control can be localized and accelerated so as to support realtime services by being separated from location management. Additionally, the proposed framework differentiates control schemes for IP handovers according to their types (i.e., forward-forward and forward-backward). This could further increase control efficiency to deal with frequent handover situations.

The rest of this paper is organized as follows. In Section 2, we discuss some related approaches. In Section 3 and 4, we derive some design considerations and propose our IP mobility management framework. Finally, we conclude the paper in Section 5.

2 Related Work

There are a few works that propose an IP mobility solution, which can be categorized into host-based and network-based approaches. As the host-based approaches, MIPv4 [1] and MIPv6 [4-6] are proposed. They require an MN to actively send a control message to Home Agent (HA), Foreign Agent (FA), or even Correspondent Node (CN). Although the MN can maintain its IP address while roaming, a lot of implementation details in MN are required, which are also complex. In addition, MIP and MIPv6 cause the well-known triangular routing problem: the packets that are transmitted by CN traverse the inefficient routing path that crosses over HA and FA.

For the network-based approach, PMIPv6 [2, 7-9] is proposed without requiring the modification to end-hosts. In

a PMIPv6 network, there exists a proxy, called Mobile Access Gateway (MAG), which performs handover operations on behalf of MNs. An anchoring point, called Local Mobility Anchor (LMA) transmits data packets to the MAGs where MNs are associated with. Although PMIPv6 is a most popular IP mobility protocol, it does not sufficiently prove its scalability in wide-area heterogeneous networks with a large number of users. Currently, PMIPv6 is partially used in the Long-Term Evolution (LTE) networks to establish IP tunneling between fixed and mobile networks rather than pure IP mobility.

Another network-based approach, called Locator/ID Separation Protocol (LISP) [3, 10], is proposed to separate host and location identifications. LISP adopts two namespaces and uses different IP addressing system for them: Endpoint Identifiers (EIDs) and Routing Locators (RLOCs) used to identify an end-host and a routing device, respectively. However, those approaches do not focus on IP mobility and require additional protocol to handle mobility issue.

3 Design Considerations for IP Mobility Support

In this section, we derive some design considerations for supporting IP mobility, which will be the basic principles of our proposed framework. First, the system for the host identification should be differentiated from the system for the location identification. In this paper, the Uniform Resource Indicator (URI) addressing system and the IP addressing system are used for the host identification and location identification, respectively. On the other hand, the persistent location identification (i.e., Home Address (HoA) in MIP/MIPv6) and the temporal location identification (i.e., Care of Address (CoA) in MIP/MIPv6) should be unified in order to reduce the overhead of managing the binding information and to simplify the control procedure of IP mobility.

Second, the binding information should efficiently be distributed over the networks, thereby reducing congestion on a specific node and increasing the agility of control procedure. The hierarchical structure of DNS can be used to do so. In addition, the control plane of IP mobility framework should logically and physically be separated from the transport plane of IP mobility framework, which simplifies the control functions of network devices.

Third, a new IP mobility framework should support the Forward and Backward (FB) type handover as simple and efficient as possible. As shown in Figure 1, we derive two types of handover by analyzing users' handover patterns and network environments. The FB type handover is defined as that the MN changes the connection to a new access network (i.e., Wi-Fi domain A) and returns back to the previous access network (i.e., cellular domain A). On the other hand, the Forward and Forward (FF) type handover is defined as that after performing a forward handover the MN performs a forward handover again to other access networks (i.e., cellular domain B). Note that most of the vertical handover scenarios where the MN using cellular networks moves into houses, offices, or hot-spot areas virtually correspond to the FB type handover. Therefore, it is important to support the FB type handover as simplified and efficient as possible.

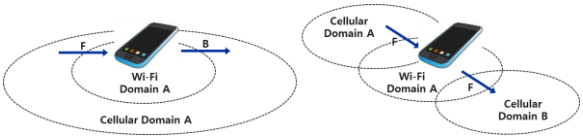

Figure 1. Two types of handover: FB type (Left) and FF type (Right)

4 Proposed Mobility Management Framework

The proposed IP mobility framework, as shown in Figure 2, operates between the service stratum and the transport stratum. Thus, it transmits data or control messages to the networks through the transport stratum and provides the service stratum with seamless IP mobility. The proposed framework consists of four major functions: Mobility Information Management Function (MIMF), Handover Support Function (HSF), Handover Monitoring Function (HMF), and Mobile Equipment Function (MEF). MIMF and HSF can be deployed in a local or global domain. HMF and MEF must be deployed in an access network and an MN, respectively. The behavior of each function is detailed as follows.

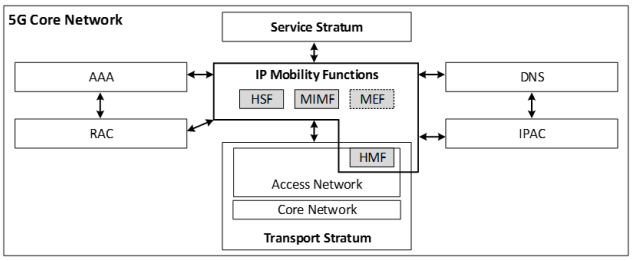

Figure 2. The proposed IP mobility management framework

MIMF manages the binding information that couples the host identification and the location identification of an MN. MIMF is connected with DNS and provides a naming service for the MNs that subscribe IP mobility service. Thus, when any node requests a host identification, MIMF responds with the corresponding location identification. In addition, MIMF updates the location identification when it receives the control message from HSF, which notifies MIMF of the MN's IP address change.

HSF sends, receives, and processes the control messages when a handover occurs. In addition, HSF is connected with the Authentication, Authorization and Accounting (AAA) and authorizes the subscribed MNs. In addition, in order to deliver data packets to the MNs, a HSF creates IP tunnels with the other HSFs that are located in adjacent networks. Thus when a handover occurs, a HSF can forward data packets to the other HSFs through the tunnels.

HMF detects a L2 connection or handover event and notifies HSF of the event. HMF assigns a new location identification (i.e., IP address) that is generated by IP Address Configuration (IPAC (i.e., DHCP)) to the newly associated MNs.

MEF is installed on an MN and manages ongoing sessions. In order to maintain the ongoing sessions irrespective of IP address changes of the MN, MEF stores the MN's IP address when a session is made. Therefore, even if

the MN is allocated to a new IP address, MEF can change the source IP address of uplink data packets to the original IP address and can maintain the ongoing sessions.

4.1 URI-based Host Identification

The proposed framework uses the URI as the host identification, as shown in Figure 3. We assume that the network operators or administrators assign a host identification beforehand to the MNs that need IP mobility service.

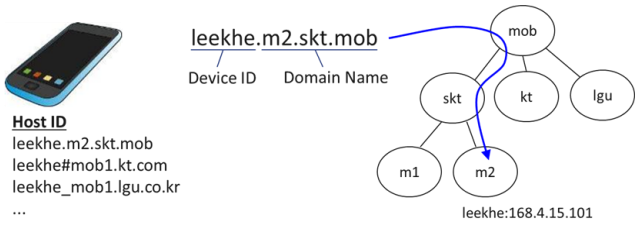

Fig 3. URI-based host identification

The advantages of using a way of URI are an intuitive and convenient way to be used in application services, a distributed manner of managing the binding information of host and location identifications, and an approach compatible with DNS. As a result, the MNs' location information and the handover control management can be distributed all over the network.

4.2 Simple and Fast Handover Support

The proposed framework adopts different approaches to the FB and FF type handovers. In case of the FB type handover, as shown in Figure 4, when the MN handovers from the network A to the network B, the downlink packets that contain the old IP address arrive at the network A first. Afterwards, the HSF in the network A forwards the data packets to the HSF in the network B through the pre-configured IP tunnel. Finally, the HSF in the network B forwards the data packets to the MN.

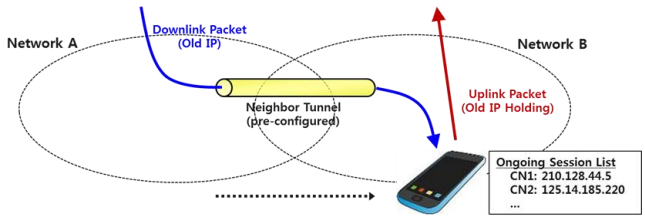

Fig 4. FB type handover control

On the other hand, when the MN transmits data packets (uplink packets), the MEF on the MN changes the source IP address of data packets to the old IP address in order to maintain the ongoing sessions, which is called IP holding scheme in this paper. The IP holding scheme manages an ongoing session list and is comparable with the IP spoofing technique. However, it is different in that it requires the MEF to be authenticated and only authenticated MEF can change the IP address. By employing the IP holding scheme, a part of packet transmissions (i.e., uplink transmission) can be processed in the MN thereby reducing the processing overhead at the networks.

In order to support the FF type handover, which is not suitable to set up an IP tunnel towards different access networks, we adopt an approach similar to the route optimization in MIP. As shown in Figure 5, after the MN performs a FF type handover, the MEF on the MN first sends the IP Change Notification message to the MEF on the CN. Afterwards, the MEF on the CN updates the MN's IP address in its routing cache with one newly notified by the MN. On the other hand, the MEF on the MN just has to use the new IP address without the IP holding scheme.

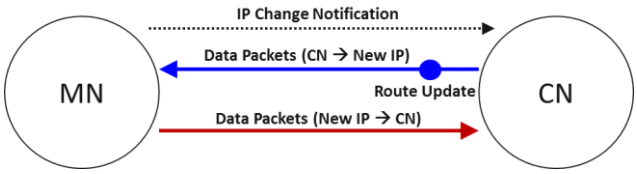

Fig 5. Route optimization for FF type handover control

4.3 State Transition Diagram of MN

Figure 6 shows the state transition diagram of MN. When an MN first attaches to the network, it should be authenticated for both network access and IP mobility service. Afterwards, the MN receives a new IP address, and its host identification and location identification are registered in the MIMF. Thereafter, the MN shifts to the *Stable* state, which enables the MN to perform a handover.

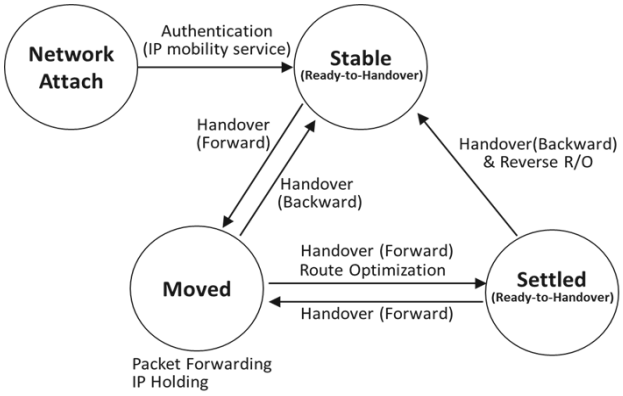

Fig 6. The state transition diagram of MN

If the MN performs a handover in the *Stable* state, the MN shifts to the *Moved* state. In the *Moved* state, an IP tunnel is established to forward downlink packets, and the IP holding scheme is used to transmit uplink packets. In the *Moved* state, the MN can shift to the *Stable* state or the Settled state whether or not the MN performs a backward handover (return to the original network) or a forward handover (moving to a new network), respectively.

If the MN returns to the *Stable* state, the handover information and control functions regarding the MN are initialized. On the other hand, if the MN shifts to the *Settled* state, the route optimization approach in the FF type handover is used. In the *Settled* state, if the MN performs a backward handover, the MN shifts to the *Stable* state, and the

route optimization approach is performed again. At this time, the MEF on the CN changes the old IP address of the MN to the new IP address, based on the routing cache. Therefore, this specific route optimization is called reverse route optimization. In addition, the handover information and control functions are also initialized.

4.4 Control Message Flows

Figure 7 shows the message flow of MN's IP handover scenario. When the MN in Figure 7 performs a handover from the access network of HSF1 to the access network of HSF2, the MN should be authenticated whether or not it is a valid subscriber to the IP mobility service, and the MN's binding information at the MIMF is updated (these procedures are not shown.).

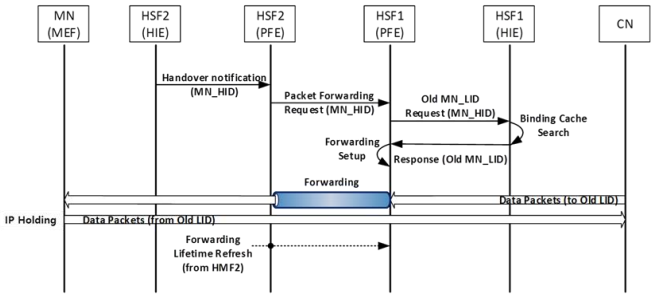

Fig 7. Message flow for handover control

While these procedures are operating, the Handover Initiation Entity (HIE) in HSF2 sends a handover notification message to the Packet Forwarding Entity (PFE) in HSF2 and notifies the PFE of that the MN's state is transited to the Moved state. Afterwards, in order to create a data tunnel, the PFE of HSF2 sends a packet forwarding request message to the PFE of HSF1. Afterwards, the PFE of HSF1 requests the MN's old location identification to the HIE of HSF1 and sets up a data tunnel with the PFE of HSF2.

Thereafter, the data packets that contain the MN's old location identification as the destination IP address arrive first at the PFE of HSF1 and are forwarded to the PFE of HSF2 and finally to the MN's MEF. On the other hand, the MN's uplink traffic is directly delivered to the CN through the IP holding scheme.

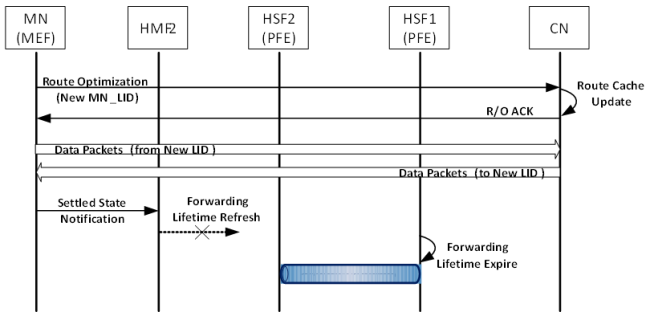

Fig 8. Message flow for reverse route optimization

Figure 8 shows the message flow of reverse route optimization procedure. The MN firstly sends a route optimization request message that embeds the MN's new location identification to the CN. Then, the CN finds out the MN's information from the route cache and updates the MN's location identification. After the CN replies with a route optimization acknowledgement message, the data traffic transmitted by the MN is directly delivered to the CN without using the IP holding scheme. In addition, the data traffic transmitted by the CN is directly delivered to the MN by the updated route cache. Thereafter, the MN is transited to the Settled state and notifies the HMF2 so that it does not transmit a lifetime refresh message to the PFE of HSF2, thereby removing the IP tunnel.

5 Conclusion

In this paper, we have proposed an IP mobility support framework focusing on simplicity and scalability required for evolving communication environment. We derive the design considerations for a new framework, which can be summarized as URI-based host identification and control differentiation with handover types. With the URI-based host identification, the proposed framework provides a distributed and hierarchical structure reducing the control overhead at a specific node. Different control schemes according to handover types further increase control efficiency to deal with frequent handover situations. As further work, we plan to experiment with a large scale simulation for the proposed framework.

References

[1] C. Perkins, "IP Mobility Support for IPv4", RFC 5944, IETF, (2010).
[2] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6", RFC 5213, IETF, (2008).
[3] D. Farinacci, V. Fuller, D. Meyer, and D. Lewis, "The Locator/ID Separation Protocol (LISP)", RFC 6830, IETF, (2013).
[4] C. Perkins, D. Johnson, and J. Arkko, "Mobility Support in IPv6", RFC 6275, IETF, (2011).
[5] L. Deguang and C. Jinyi, "Tunnelling-Based Route Optimization for Mobile IPv6", International Conference on Wireless Communications, Networking and Information Security (WCNIS), IEEE, (2010).
[6] B. Christian "Network Mobility Route Optimization with Certificate-based Authentication", First International Conference on Ubiquitous and Future Networks (ICUFN), IEEE, (2009).
[7] H. Chan, "Proxy mobile ip with distributed mobility anchors", GLOBECOM Workshop, IEEE, (2010).
[8] S. Koh et al., "Use of proxy mobile ipv6 for distributed mobility control", Internet-Draft draft-sjkoh-mext-pmip-dmc-03, IETF, (2011).
[9] C. Bernardos and J. Zuniga, "Pmipv6-based distributed anchoring", Internet-Draft draft-bernardos-dmm-distributed-anchoring-00, IETF, (2012).
[10] D. Farinacci, V. Fuller, D. Meyer, and D. Lewis, "The Locator/ID Separation Protocol (LISP)" IETF, (2013).

Received: Month xx, 20xx