A Novel DMM Architecture Based on NDN

Zhiwei Yan[1,2(✉)], Jong-Hyouk Lee[3], Guanggang Geng[1,2], Xiaodong Lee[1,2], and Yong-Jin Park[4]

[1] China Internet Network Information Center, Beijing, China
{yan, gengguanggang, xl}@cnnic.cn
[2] National Engineering Laboratory for Naming and Addressing, Beijing 100190, People's Republic of China
[3] Department of Computer Software Engineering, Sangmyung University, Seoul 110-743, Republic of Korea
jonghyouk@smu.ac.kr
[4] Department of Communications and Computer Engineering, School of Fundamental Science, Waseda University, Tokyo 169-8555, Japan
yjp@ieee.org

Abstract. The unprecedented expansion of mobile Internet traffic has resulted in the development of distributed mobility management architecture. In this paper, based on Named Data Networking (NDN), traditional mobility support services are distributed among multiple anchor points in the IPv6 core network, to overcome some of the major limitations of centralized IP mobility management solutions.

Keywords: MIPv6 · PMIPv6 · DMM · NDN

1 Introduction

Mobility management which provides wireless devices with connectivity service to Internet becomes major marketable goods as mobile computing is frequent and popularized. The Mobile IPv6 (MIPv6) proposed by IETF allows Mobile Nodes (MNs) to be reachable, regardless of its current location [1]. When the MN moves to other subnet, it acquires address in the new location and performs home registration with its Home Agent (HA), which enables the MN to keep its active communications. In order to cut down the signaling overhead by network-based mobility management manner and avoid the host-based mobility stack in the MN, the Network-based Local Mobility Management (NetLMM) functional architecture is defined in RFC 4831 [2]. According to this architecture, the Proxy Mobile IPv6 (PMIPv6) [3] was developed. Being different from MIPv6, PMIPv6 introduces two important entities, Local Mobility Anchor (LMA) and Mobility Access Gateway (MAG), which manage all mobility related signaling so that the MN is freed from the mobility management task.

In the future mobile Internet, MIP/PMIP will be the basic protocols to support the mobility management. However, how to effectively address the scalability issue caused by the large-scale mobile terminals and traffic is vital to promote the all-IP based mobile Internet. According to the current protocol specifications, the single serving

J.-H. Lee and S. Pack (Eds.): QShine 2016, LNICST 199, pp. 485–491, 2017.
DOI: 10.1007/978-3-319-60717-7_49

point (HA or LMA) is deployed to manage all the binding states and transmit the traffic for the MN. Then the key point to guarantee the scalability of MIP/PMIP is to distribute the HA/LMA function to multiple equal entities. In order to address architectural limitations of the centralized mobility management, the IETF has established the Distributed Mobility Management (DMM) working group aiming at distributing mobile Internet traffic in an optimal way while not relying on centrally deployed mobility anchors [4]. Although there are many studies about the distributed extensions of the MIPv6 and PMIPv6, most of them remedy or optimize the MIPv6 and PMIPv6 based on the extensions of the basic protocols and cannot satisfy the farsighted requirements of MIPv6 and PMIPv6 in the distributed mobile Internet. In this paper, we use the idea of Name Data Networking (NDN) to support the distributed extensions of both MIPv6 and PMIPv6.

2 Proposed Architecture

2.1 Why Can NDN Help?

In order to effectively solve the problems of the current Internet caused by the location-based communication model and make the Internet more suitable for the future applications, the concept of Information-Centric Networking (ICN) [5] was proposed and the Named Data Networking (NDN) [6] is one of the most important representatives among the ICN proposals. In NDN, the communication is consumer- initiated and a consumer retrieves an individual content object by sending an Interest packet which specifies the name of the desired content object. The NDN changes the communication model in the TCP/IP network and it is shown in Fig. 1.

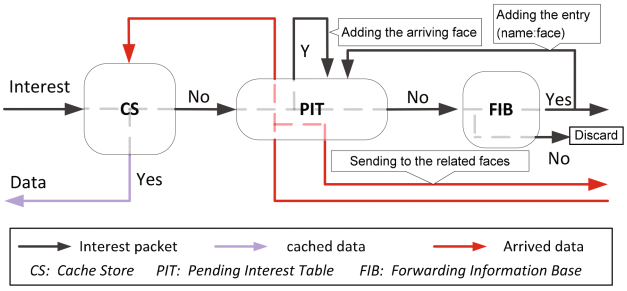

Fig. 1. NDN communication model

Requests (Interest packets) for some content are forwarded toward a publisher location. A NDN router maintains a Pending Interest Table (PIT) for forwarded requests, which enables request aggregation; that is, a NDN router would normally not forward a second request for a specific content when it has recently sent a request for

that particular content. The PIT maintains state for all Interest packets and maps them to the network interfaces from which the corresponding requests have been received. Data packet is then routed back on the reverse path using this state. NDN supports in-network caching: contents received by a NDN router (in response to requests) can be cached in the Content Store (CS) so that subsequent received requests for the same object can be answered from that cache. If the Interest packet cannot be consumed by the CS and has no match entry in the PIT, the router will send it out according to the Forwarding Information Base (FIB), which is maintained as the IP routing table.

NDN adopts the distributed routing algorithm to retrieve the named data, and pays no attention to its location. This kind of scheme can always fetch the data from the most optimized location and be suited in the dynamic environment. Although NDN is well designed for the content-centric Internet, its large deployment will be a long way. Then we can make use of its advantages if it can be overlapped with the IP protocols. In which, the NDN is used as a signaling layer to manage the binding states dynamically to support the distributed MIPv6 and PMIPv6.

2.2 Basic Architecture

Multiple HA/LMA entities are deployed in the core network as shown in Fig. 2.

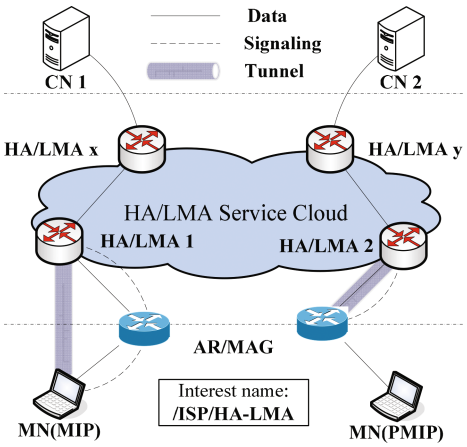

Fig. 2. Distributed mobility management architecture

They share a common name, which is stored in the Domain Name System (DNS) or policy store as basic information of the MIP/PMIP service [7, 8]. For the deployment flexibility, we also design the mobility management protocols with both network-based manner and host-based manner, which are described in the following subsections.

2.3 Host-Based Case

(A) Binding Update

When the MN receives the new Router Advertisement (RA) message from the new access network, it will configure a new Care-of Address (CoA) and initiate the binding update. MN sends out the Interest packet with the name as

/ISP/HomeAgent

The routers will route this signaling message to the domain of the identified Internet Service Provider (ISP) and then the routers in the ISP's domain will find the FIB to match the *HomeAgent* label. Then the nearest (or the best) HA will receive the Interest packet finally. In order to make this work, the Interest packet has to be extended to identify that this packet is used as a binding update message and then the HA can parse it accordingly. Of course, the necessary information in MIPv6 has to be included, for example, CoA and Home address (HoA) are the mandatory information.
Besides, all the HAs in the same HA service set (or cloud) have to announce their existence as the NDN content publisher does. Then the routers can maintain the FIB entry corresponding to the optimized HA according to the actual location and network condition. Because our solution is overlapped on the IP protocol, the HA also has an available IPv6 address to transmit IP traffic to and from the MN. Then the HA which received the Interest packet will response with a Data packet to acknowledge the location update.

(B) State Synchronization

For the multiple HAs in the same HA service set, they should function equally in a distributed manner. In this way, they have to synchronize the binding state if the new binding is established or the old binding is refreshed. We also use the NDN routing scheme herein because the name-based routing can support the multicast in nature. For example, when the HA received the Interest packet from the MN and established the binding state, it will send a new Interest packet out with the content name as

/ISP/HomeAgent

In this Interest packet, the multicast routing requirement should be flagged. Then the router will send this message to all the possible HA entities according to all the recorded FIB entries. In this Interest packet, the HoA and CoA are also mandatory information. More sophisticated scheme such as the ChronoSync [9] can be well used here for the state synchronization.

(C) Packet Transmission

For the packet sent from MN to the Corresponding Node (CN), it can be directly transmitted to the CN with the HoA and CN's address as the source and destination addresses, respectively. All the HAs have to announce the same IPv6 prefix containing the served HoA set to attract the packets for the related MN. In this way, the packet sent from CN to the MN will arrive at the nearest HA due to the routing protocol of the bypassed routers. Then the HA entity will check its binding update table to locate the

entry of the related HoA. If there is positive match, the HA will replace the destination address with the related CoA and attach the HoA for example in the Type 2 routing header [1]. In this way, the packet can arrive at the MN finally. If there is no positive match, the HA will send an Interest packet with the flagged multicast requirement, which contains the HoA of the MN. The other HAs will recognize that this Interest is used to fetch the corresponded CoA. And then the first HA who knows the CoA will response with a Data packet including the CoA. If the HA cannot learn the CoA within a reasonable period, the packet will be discarded because it will conclude that the MN has not established the available binding.

2.4 Network-Based Case

(A) Binding Update

When the MN attaches to the new access network, the MAG will trigger the location update. It sends out the Interest packet with the name as

/ISP/LocalMobilityAnchor

The routers will route this signaling message to the domain of the identified ISP and then the routers in the ISP's domain will find the FIB to match the *LocalMobilityAnchor* label. Then the nearest (or the best) LMA will receive the Interest finally. In order to make this work, the Interest packet has to be extended to identify that this Interest is used as a proxy binding update message and then the LMA can parse it accordingly. Of course, the necessary information in PMIPv6 has to be included, for example, MN's identification and the address of MAG are the mandatory information.

Besides, all the LMAs in the same LMA service set (or cloud) have to announce their existence as the NDN content publisher does. Then the routers can maintain the FIB entry corresponding to the optimized LMA according to the actual location and network condition. Because our solution is overlapped on the IP protocol, the LMA also has an available IPv6 address to transmit IP traffic to and from the MN. Besides, the LMAs have to maintain a common IPv6 prefix (which is shorter than 64bits). Then the LMA which received the Interest packet will response with a Data packet to acknowledge the location update. In the Data packet, the allocated Home Network Prefix (HNP) is contained.

(B) State Synchronization

For the multiple LMAs in the same LMA service set, they should function equally in a distributed manner. In this way, they have to synchronize the binding state if the new binding is established or the old binding is refreshed. We also use the NDN routing scheme herein because the name-based routing can support the multicast in nature. For example, when the LMA received the Interest from the MAG and established the binding state, it will send a new Interest packet out with the content name as

/ISP/LocalMobilityAnchor

In this Interest packet, the multicast routing requirement should be flagged. Then the router will send this message to all the possible LMA entities according to all the recorded FIB entries. In this Interest packet, the MN's HNP and the current serving MAG's address are also mandatory information. More sophisticated scheme such as the ChronoSync [9] can be well used here for the state synchronization.

(C) Packet Transmission

For the packet sent from MN to the CN, it can be directly transmitted to the CN with the HoA (configured by the HNP) and CN' address as the source and destination addresses, respectively. All the LMAs have to announce same IPv6 prefix containing the served HNP set to attract the packets to the related MN. In this way, the packet sent from CN to the MN will arrive at the nearest LMA due to the routing protocol of the bypassed routers. Then the LMA entity will check its binding update table to locate the entity of the related HNP. If there is positive match, the LMA will replace the destination address with the related MAG's address and attach the original destination address for example in the Type 2 routing header [1]. In this way, the packet can arrive at the MN finally. If there is no positive match, the LMA will send an Interest packet with the flagged multicast requirement, which contains the source address of the MN. Then the other LMA will recognize that this Interest is used to fetch the corresponded MAG's address. And then the first LMA who knows the MAG's address will response with a Data packet including the MAG's address. If the LMA cannot learn the MAG's address within a reasonable period, the packet will be discarded because it will conclude that the MN has not established the available binding.

2.5 Conclusions

This paper proposes the DMM architecture in all-IP mobile network with the NDN-based control plane. Accordingly, the name-based routing solution in NDN facilitates the DMM requirements to distribute the anchor point and optimize the packet transmission path in the mobile environments. As our future work, the performance of the proposed architecture will be studied and evaluated.

Acknowledgments. This paper was supported by the National Natural Science Foundation of China under Grant No. 61303242. The work of Yong-Jin Park was supported by the JSPS KAKENHI under Grant No. 26330119.

References

1. Perkins, C., Johnson, D., Arkko, J.: Mobility support in IPv6. IETF RFC 6275, July 2011
2. Kempf, J.: Goals for network-based localized mobility management (netlmm). IETF RFC 4831, April 2007
3. Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., Patil, B.: Proxy mobile IPv6. IETF RFC 5213, August 2008

4. Chan, H. (ed.): Requirements of distributed mobility management. IETF RFC 7333, August 2014
5. Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., Ohlman, B.: A Survey of information-centric networking (Draft). In: Proceedings of Dagstuhl Seminar, February 2011
6. Jacobson, V., et al.: Networking named content. In: Proceedings of ACM CoNEXT, Rome, Italy, December 2009
7. Giaretta, G., Kempf, J., Devarapalli, V.: Mobile IPv6 bootstrapping in split scenario. IETF RFC5026, October 2007
8. Korhonen, J., Devarapalli, V.: Local mobility anchor (LMA) discovery for proxy mobile IPv6. IETF RFC 6097, February 2011
9. Zhu, Z., Afanasyev, A.: Let's ChronoSync: decentralized dataset state synchronization in named data networking. In: Proceedings of IEEE ICNP, Göttingen, Germany, October 2013