12-13-2016

Distributed All-IP Mobility Management Architecture Supported by the NDN Overlay

Zhiwei Yan
China Internet Network Information Center, China

Guanggang Geng
China Internet Network Information Center, China

Sherali Zeadally
University of Kentucky, szeadally@uky.edu

Yong-Jin Park
University of Malaysia Sabah, Malaysia

Repository Citation

Yan, Zhiwei; Geng, Guanggang; Zeadally, Sherali; and Park, Yong-Jin, "Distributed All-IP Mobility Management Architecture Supported by the NDN Overlay" (2016). *Information Science Faculty Publications*. 46.
https://uknowledge.uky.edu/slis_facpub/46

Digital Object Identifier (DOI)
https://doi.org/10.1109/ACCESS.2016.2639008

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 21, 2016; accepted December 2, 2016, date of publication December 13, 2016,
date of current version February 25, 2017.

Digital Object Identifier 10.1109/ACCESS.2016.2639008

Distributed All-IP Mobility Management Architecture Supported by the NDN Overlay

ZHIWEI YAN[1], GUANGGANG GENG[1], SHERALI ZEADALLY[2], AND YONG-JIN PARK[3]

[1]China Internet Network Information Center, NANEL, Beijing 100190, China
[2]College of Communication and Information, University of Kentucky, Lexington, KY 40506, USA
[3]University of Malaysia Sabah, Kota Kinabalu 88400, Malaysia

Corresponding author: G. Geng (gengguanggang@cnnic.cn)

This work was supported by a Grant from the National Natural Science Foundation of China under Grant 61303242. The work of Y.-J. Park was supported by JSPS KAKENHI under Grant 26330119.

ABSTRACT Two of the most promising candidate solutions for realizing the next-generation all-IP mobile networks are Mobile IPv6 (MIPv6), which is the host-based and global mobility supporting protocol, and Proxy MIPv6 (PMIPv6), which is the network-based and localized mobility supporting protocol. However, the unprecedented growth of mobile Internet traffic has resulted in the development of distributed mobility management (DMM) architecture by the Internet engineering task force DMM working group. The extension of the basic MIPv6 and PMIPv6 to support their distributed and scalable deployment in the future is one of the major goals of the DMM working group. We propose an all-IP-based mobility management architecture that leverages the concept of Named Data Networking (NDN), which is a distributed content management and addressing architecture. In the proposed solution, mobility support services are distributed among multiple anchor points at the edge of the network, thereby enabling a flat architecture that exploits name-based routing in NDN. Our approach overcomes some of the major limitations of centralized IP mobility management solutions, by extending existing routing protocol and mobility management architecture, to distribute the mobility management function of anchor points in the IP network and optimize the transmission path of mobile traffic.

INDEX TERMS Distributed mobility management (DMM), MIPv6, PMIPv6, named data networking (NDN).

I. INTRODUCTION

Mobility management provides wireless devices with uninterrupted Internet connectivity with the unprecedented growth of mobile computing and applications. Mobile IPv6 (MIPv6), proposed by Internet Engineering Task Force (IETF), allows a Mobile Node (MN) to be reachable, regardless of its current location [1]. When the MN moves to another subnet, the MN acquires an address in the new location and performs home registration with its Home Agent (HA) which enables it to keep its active communications. In order to minimize the signaling overheads of host-based mobility stack, the Network-based Local Mobility Management (NetLMM) functional architecture has been defined in RFC4831 [2]. In this architecture, the Proxy Mobile IPv6 (PMIPv6) [3] was developed. MIPv6 and PMIPv6 protocols are selected as the basic solutions for mobility services embedded in 3GPP [4] and WiMAX [5]. Moreover, MIPv6 and PMIPv6 have already been implemented by the major networking equipment vendors.

In the future mobile Internet, MIP/PMIP will be the basic protocols that support mobility management. However, how to effectively address the scalability issue caused by the increasing number of mobile terminals and volume of traffic generated will be vital to promote the all-IP based mobile Internet. According to the current protocol specifications, the centralized single-point entity, which is HA in MIPv6 and Local Mobility Anchor (LMA) in PMIPv6 respectively, is deployed to manage all the binding states and transmit the traffic for the MN. In this case, the key challenge is to guarantee the scalability of MIP/PMIP so as to distribute the HA/LMA function efficiently for large-scale networks. To address the architectural limitations of the centralized mobility management architecture, the IETF set up the Distributed Mobility Management (DMM) working group which is working on the distribution of mobile Internet traffic in an optimal way without relying on centrally deployed mobility anchors [6].

Although many studies [7]–[9] about the distributed extensions of the MIPv6 and PMIPv6 have been previously published in the literature, most of them optimize the MIPv6 and PMIPv6 based on their extensions and cannot satisfy important requirements of MIPv6 and PMIPv6 in the distributed mobile Internet. In this paper, we leverage Name Data Networking (NDN) to support the distributed extensions of both MIPv6 and PMIPv6 as a novel solution of DMM.

The remainder of this paper is organized as follows. First, we review the basic MIPv6/PMIPv6 and their distributed extensions. Second, we describe our proposed distributed mobility management scheme based on NDN followed by its performance evaluation. Finally, we make some concluding remarks.

II. RELATED WORK

A. HOST-BASED MOBILITY MANAGEMENT SCHEME: MIPv6

MIPv6 supports mobility for the MN by providing it with at least two addresses: a Home Address (HoA), which is a fixed address and is provided by the HA; a Care-of Address (CoA), which is obtained in the foreign access network and changes when the MN moves to a new subnet. The architecture of MIPv6 is shown in the left part of Figure 1.

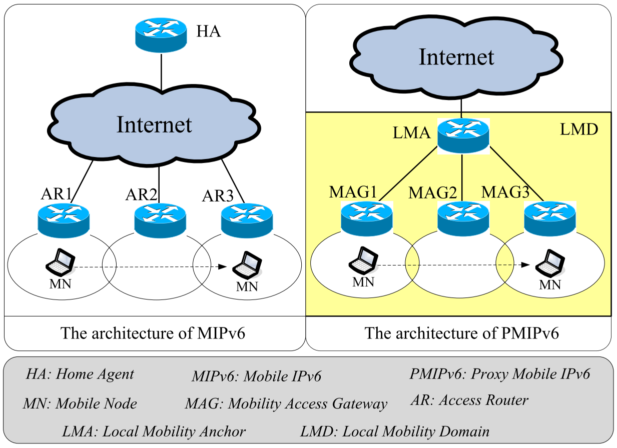
HA
Internet
AR1
AR2
AR3
MN
MN
The architecture of MIPv6
Internet
LMA
LMD
MAG1
MAG2
MAG3
MN
MN
The architecture of PMIPv6
HA: Home Agent
MIPv6: Mobile IPv6
PMIPv6: Proxy Mobile IPv6
MN: Mobile Node
MAG: Mobility Access Gateway
AR: Access Router
LMA: Local Mobility Anchor
LMD: Local Mobility Domain

FIGURE 1. **Architectures of MIPv6 and PMIPv6.**

When the MN stays in its home domain, the MN is able to receive packets destined to its HoA. These packets are forwarded through conventional IP routing mechanisms. When the MN crosses the boundary of its current serving network and attaches to another Access Router (AR), movement detection is performed in order to identify its new point of attachment and it acquires a new CoA. Once configured with a new CoA, the MN sends a Binding Update (BU) message to the HA to register its new location. When the MN is away from its home network, the HA acts as the MN's proxy entity. This means that any packets addressed to the MN will end up at the HA because the HA responds to all Neighbor Solicitation (NS) requests for the MN. Once the HA has intercepted a packet, it encapsulates this packet in a tunnel and forwards it to the MN's current CoA.

B. NETWORK-BASED MOBILITY MANAGEMENT SCHEME: PMIPv6

In contrast to MIPv6, PMIPv6 introduces two important entities, the LMA and the Mobility Access Gateway (MAG), which manage all mobility-related signaling operations so that the MN does not need to be involved in the signaling exchange. As the MN hands over and changes its point of attachment from one MAG to another MAG, the MN continues to use the same address which was obtained at its first MAG. Figure 1 (right side) shows the architecture of PMIPv6. When the MN performs a handover to a Local Mobility Domain (LMD), the MAG1 sends a Proxy Binding Update (PBU) message to the LMA to establish a bi-directional tunnel between the MAG1 and the LMA. It is worth noting that the tunnel is used for routing the packets to and from the MN. Upon receipt of the PBU sent by the MAG1, LMA recognizes that the MN is now under MAG1. The LMA manages the binding cache entry of the MN, the session and routing information. Then the MN receives a Router Advertisement (RA) message from MAG1 which includes the Home Network Prefix (HNP) allocated by LMA. The MN creates its address by using the prefix information. If the MN performs a handover from MAG1 to MAG2, MAG2 also sends a PBU message to the LMA and then a bi-directional tunnel between MAG2 and LMA is created for the MN and the tunnel between LMA and MAG1 is terminated. Since MAG2 also sends the same HNP to the MN, the MN does not observe any IP level mobility, i.e., its IP address remains unchanged. Thus, the MN can perform a handover in the LMD without participation in any mobility-related signaling operations.

C. LIMITATIONS OF CENTRALIZED MOBILITY MANAGEMENT SOLUTIONS

As described in the previous section, current mobility management solutions, such as MIPv6 and PMIPv6, rely on the existence of a central entity anchored in both the control and the data plane. That is, the HA and LMA are in charge of tracking the location of the MN and redirecting traffic toward the current location of the MN. While these solutions have been fully developed and explored during the past few years, there are also several limitations that have been identified [6], [9]:

- **Sub-optimal routing:** data traffic always traverses the central anchor, regardless of the current geographical position of the communication endpoints.
- **Scalability:** in current mobility architectures, network links and nodes have to be provisioned to manage all the traffic traversing the central anchors. This poses several scalability and network design problems as the number of MNs increases.
- **Reliability:** centralized anchoring points (i.e., HAs and LMAs) represent a potential single point of failure.

- **Low granularity:** current solutions define mobility support on a per MN basis. That is, the service is provided to the MN's communications as a whole.

D. DISTRIBUTED EXTENSIONS OF MIPv6 AND PMIPv6

To address some of the drawbacks and limitations of MIPv6 and PMIPv6, three main classes of solutions have been proposed for their DMM extensions: 1) client-based, 2) network-based, and 3) routing-based approaches.

Client-based mobility approaches aim at deploying multiple HAs at the edge of the access network in order to distribute the anchoring operations. The basic concept is that the MN no longer uses a single IP address anchored at a central HA, but it configures and uses an additional IP address at each visited access network. The MN uses the locally-anchored address to start new communications, while maintaining the reachability of those IP addresses used by ongoing and active communications. Session continuity is guaranteed by using bi-directional tunnels between the MN and each one of the HAs anchoring in-use addresses and does not require changes to the protocol behavior of the network entities [10], [11]. However, these client-based mobility schemes require protocol extensions and additional intelligence on the MN side because the MN has to manage multiple addresses simultaneously, select the right one to use for each communication, keep track of those addresses which need mobility support, and perform the required maintenance operations (i.e., binding signaling and tunneling). Additionally, non-locally-anchored traffic experiences sub-optimal routing.

For network-based approaches, two classes of solutions can be identified: 1) solutions with a fully distributed model, and 2) solutions with a partially distributed model. The distinction between fully and partially distributed approaches has to do with whether the control plane and the data plane are tightly coupled or not. In the fully distributed model, mobility anchors are moved to the edge of the access network and they manage both the control and the data plane. If we consider a partially distributed model, the data plane and the control plane are separated and only the data plane is distributed. Among the solutions that fall into the first category, [12] proposes implementing local routing at the MAG. In contrast, [13] introduces the logical entity of the central mobility database to maintain users' localization information and to allow the setup of on-demand tunneling when a specific service requires seamless mobility support. To achieve this goal, [14] proposes a solution that separates the data plane from control plane.

Finally, routing-based proposals, such as [15], follow a completely different approach. In this case, when the MN attaches to an AR, it obtains an IP address that is then internally advertised within the domain using an intra-domain protocol (e.g., Internal Border Gateway Protocol (IBGP)). In this way, the reachability of the MN is ensured while it roams around within the domain. This approach, however, has some limitations in terms of handover latency (limited by the intra-domain routing convergence) and scalability (i.e., caused by storms of routing updates).

Although the aforementioned solutions are still being standardized, there is a strong interest to address some of the current issues, especially when new services (e.g., distributed caching for multimedia content or Content Distribution Network (CDN)) representing renewed business revenues for the mobile network operators require a paradigm shift in the way mobility support is provided today.

III. PROPOSED ARCHITECTURE

A. NAMED DATA NETWORKING (NDN)

To effectively address some problems of the current Internet caused by the underlying location-based communication model and make it more suitable for future applications, the concept of Information-Centric Networking (ICN) [16], [17] was proposed and Named Data Networking (NDN) [18] has emerged as one of the most important representatives among various ICN proposals. In NDN, the communication is consumer-initiated. A consumer retrieves an individual content object by sending an Interest request that specifies the name of the desired content object. NDN changes the communication model in the IP network (as shown in Figure 2). Requests (Interest packets) for the content are forwarded toward a publisher location. A NDN router maintains a Pending Interest Table (PIT) for outstanding 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 Interests and maps them to network interface where corresponding requests have been received from. Data is then routed back on the reverse path using this state.

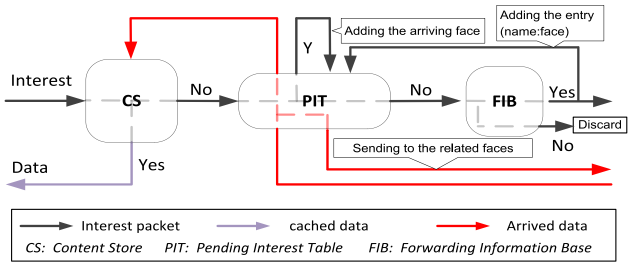

FIGURE 2. NDN communication model.

NDN supports on-path caching: contents received by a NDN router (in responses 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 cannot be consumed by the CS and has no matched entry in the PIT, the router sends it out according to the Forwarding Information Base (FIB), which is maintained as the routing table in the IP network.

NDN adopts the distributed routing algorithm to retrieve the named data, and pays no attention to its location. This new approach can always fetch the data from the most optimized location and is well suited for dynamic environments. Although NDN was specifically designed for the content-centric Internet, its large-scale deployment remains a challenge. But we can reap some of the NDN's benefits if we integrate it with current IP-based protocols where NDN is used as a single layer to manage the network states dynamically.

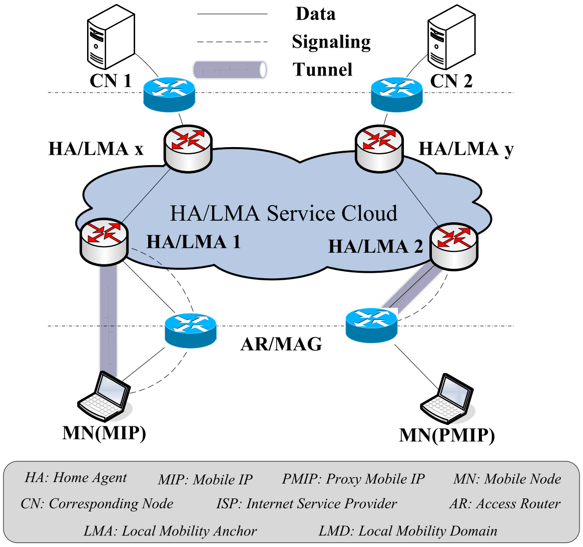

FIGURE 3. Distributed mobility management architecture.

B. ARCHITECTURE OF NDN-BASED DMM

Figure 3 shows that multiple HA/LMA entities are deployed in the core network.

These entities share a common name, which is stored in the Domain Name System (DNS) or policy store as basic information of the MIP/PMIP service. For example, the Name Authority Pointer (NAPTR) record [19] can be used to store this name if the DNS is used for the HA/LMA discovery [20], [21].

To achieve deployment flexibility, we develop mobility management protocols for both network-based as well as host-based cases and they are described in the following subsections.

C. HOST-BASED CASE

In MIPv6, the MN initiates the binding update and establishes the tunnel directly with the HA. In this host-based case, the mobility management is also handled by the MN itself as in the basic MIPv6.

1) BINDING UPDATE

When the MN receives the new RA message from the new access network, it configures a new CoA and initiates the binding update. The MN sends out the Interest message 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 (in this case we set the ISP as the domain boundary as an example). The nearest (or the best one based on the NDN routing policy) HA will finally receive the Interest packet. In order to make this work, the Interest message has to be marked to indicate that this Interest packet is used as a binding update message so that the HA can parse it accordingly. In this case, the mandatory information such as CoA and HoA has to be included.

Besides, all the HAs in the same HA service set (or HA Service Cloud) have to announce their existence by broadcasting an announcement message periodically as the content publisher does. Then the routers can maintain the FIB entry corresponding to the optimized HA according to their actual locations and current networking conditions (e.g., bandwidth, latency, and jitter).

Since our solution is integrated with 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 respond with a Data packet to acknowledge the location update.

2) STATE SYNCHRONIZATION

For the multiple HAs in the same HA service set, they should function as the same way in a distributed manner. They have to synchronize their binding states if a new binding is established or an old binding is refreshed. We also use the NDN's name-based routing scheme here because the scheme can support multicast. For example, when the HA receives the Interest packet from the MN and establishes the binding state, it will send a new Interest message with the content name as

/ISP/HomeAgent

In this case, the router will multicast this message to all the possible HA entities according to all the recorded FIB entries. In this Interest message, the HoA and CoA are also mandatory information. The more sophisticated scheme such as the ChronoSync [22] can be well used here for distributed state synchronization.

3) PACKET TRANSMISSION

When the MN sends a packet to the Corresponding Node (CN), it can be directly transmitted to the CN. The packet contains the HoA and the CN's address as the source and destination addresses, respectively.

For the packets sent from CN to the MN, the procedure is illustrated in Figure 4. All of the HAs have to announce the same IPv6 prefix containing the served HoA set to route the packets to the related MN. In this way, the packets sent from the CN to the MN will arrive at the nearest HA due to

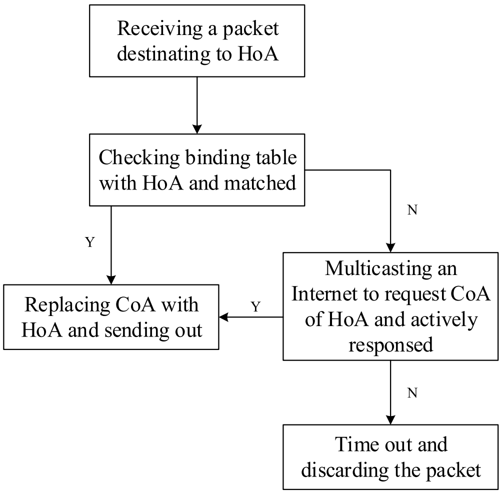
Receiving a packet destinating to HoA
Checking binding table with HoA and matched
N
Y
Multicasting an Internet to request CoA of HoA and actively responsed
Y
Replacing CoA with HoA and sending out
N
Time out and discarding the packet

FIGURE 4. Packet transmission procedure.

the routing protocol of the bypassed routers. Then the HA entity checks its binding table to validate the entry of the related HoA. If there is a positive match, the HA will replace the destination address with the related CoA and attach the HoA in the IPv6 routing header (e.g., Type 2 routing header). In this way, the packet will finally reach the MN. If there is no positive match, the HA multicasts an Interest message which contains the HoA of the MN. The other HAs will recognize that this Interest packet is used to fetch the corresponding CoA. Then, the first responding HA, which knows the CoA, will respond with a Data packet that contains the CoA.

If the HA cannot learn the CoA within a reasonable period, the packet will be discarded because the HA will recognize that the MN has not established the available binding.

4) TUNNELING-BASED SOLUTION

In the above procedure, the packet can be routed along the optimized path but the packet has to be reorganized to attach the routing header. In practice, this may be time-consuming. So we propose another approach based on tunneling.

When the HA receives the Interest message from the MN, it configures a tunnel with the CoA and the HA's address as the endpoints. The response Data packet contains the HA's address. In this way, the MN can also configure an IPv6 tunnel to transmit the HoA related traffic.

For the state synchronization, the HA that receives the Interest message will establish or refresh the tunnel with that HA by using the HoA as the index of the tunnel.

When the CN sends a packet to the MN, the nearest or optimum HA entity will receive the packet. The HA checks the binding state and tunnels the packet to the original serving HA. Then this HA which, maintains the tunnel with the MN, can de-capsulate the packet and finally tunnels it to the CoA.

D. NETWORK-BASED CASE

In PMIPv6, the MAG is in charge of the binding update for the MN. Then the tunnel is established between MAG and LMA. In this network-based case, the mobility management is also handled by the network entities as in basic PMIPv6.

1) BINDING UPDATE

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

/ISP/LocalMobilityAnchor

The routers will route this signaling message to the domain of the named ISP and then the routers in the ISP's domain will find the FIB to match the LocalMobilityAnchor label. Finally, the nearest (or the best) LMA will receive the Interest. For this approach to work, the Interest message needs to be extended to indicate that this Interest message is used as a proxy binding update message and then the LMA can parse it accordingly. The necessary information for PMIPv6 has to be added, including mandatory information such as the MN's identification and the address of MAG.

Besides, all the LMAs in the same LMA service set have to announce their existence as the content publisher does. Then the routers can maintain the FIB entry corresponding to the optimized LMA according to the actual location and network condition.

Since our proposed solution is integrated with 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 64 bits). Then the LMA which received the Interest packet will respond with a Data packet to acknowledge the location update. The Data packet contains the allocated HNP designated from the shared IPv6 prefix.

2) STATE SYNCHRONIZATION

All of the LMAs in the same LMA service set should operate in the same way. The LMAs have to synchronize their binding states if a new binding is established or an old binding is refreshed. We also use the NDN's name-based routing scheme. For example, when the LMA receives an Interest message from the MAG and establishes the binding state, it will send a new Interest message out with the content name as

/ISP/LocalMobilityAnchor

This Interest message will be multicasted and then the router sends this message to all the possible LMA entities according to all the recorded FIB entries. This Interest message contains the MN's identification, MN's HNP and the current serving MAG's address which are mandatory information. The ChronoSync can also be used here for state synchronization.

3) PACKET TRANSMISSION

When the MN sends a packet to the CN, it can be directly transmitted to the CN. The packet contains the HoA (configured with the HNP) and the CN' address as the source and destination addresses, respectively. All the LMAs have to announce the same IPv6 prefix containing the HNP set served in order to route the packets to the related MN. In this way, the packet sent from the CN to the MN will arrive at the nearest LMA by using the routing protocol of the bypassed routers. The LMA entity then checks its binding update table to find the entity of the related HNP. If there exists a positive match, the LMA replaces the destination address with the related MAG's address and attaches the original destination address in the IPv6 routing header (e.g., Type 2 routing header). In this way, the packet can finally reach the MN. If there is no positive match, the LMA multicasts an Interest message containing the source address of the MN. The other LMA will recognize that this Interest message is used to fetch the corresponding MAG's address. Then, the first responding LMA which knows the MAG's address responds with a Data packet that contains 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 recognize that the MN has not established the available binding.

4) TUNNELING-BASED SOLUTION

We also propose an alternative solution based on tunneling. When the LMA receives the Interest message from the MN, it will configure a tunnel with the MAG's address and LMA's address as the endpoints. The Data packet contains the LMA's address. In this way, the MAG can also configure an IPv6 tunnel to transmit the HNP's related traffic.

For state synchronization, when the LMA receives the Interest message, it establishes or refreshes the tunnel with that LMA and the HNP is used as the index of the tunnel.

When CN sends a packet to the MN, the nearest or optimum LMA entity will receive the packet. The LMA checks the binding state and tunnels the packet to the original serving LMA. Then this LMA which, maintains the tunnel with the MAG, can de-capsulate the packet and tunnel it to the MAG's address.

IV. PERFORMANCE EVALUATION

In this section, we analyze the handover performance of the proposed scheme in terms of handover latency. As the handover performance is very different for the distributed solutions under different assumptions and network topologies, here we only analyze the proposed solution and compare it with the basic schemes to enable a fair performance comparison.

A. NETWORK MODEL

We use the two-layer binary tree as our simulation network model. For MAG and LMA locations, we assume that the MAG is one-layer lower than the LMA. In this way, if the total number of LMAs deployed is N_1, the depth corresponding to a LMA is $n = \log_2(N_1)$ and the number of MAG is $2^{(n+1)}$. For example, if we assume that there are 16 LMAs, and then the hierarchy level (n) of LMA is 4 and the number of available MAGs is 32. Besides, the average number of hops (H) from a leaf node to the others (in a balanced binary tree with depth as n) can be computed as

$$H = \frac{(n-1) \times 2^{n+1} + 2}{2^n} \tag{1}$$

In the basic MIP/PMIP architecture, only one central point (HA/LMA) is deployed for the location management and packet transmission. We assume that the root point in the tree is the centralized HA/LMA. In contrast, in the distributed architecture, multiple HA/LMA entities can be deployed at the leaf points (one layer above the AR/MAG). We use this hierarchical model to differentiate the centralized HA/LMA function from the distributed HA/LMA function by taking into account the following two considerations:

- ∗ The HA/LMAs in the DMM are located between the AR/MAG and the centralized HA/LMA.
- ∗ The distance from AR/MAG to the HA/LMA in the centralized protocol is further than that distance in the distributed protocol.

B. SESSION AND MOBILITY MODELS

We assume that the residence time of the MN in a subnet is T^{res}_{sub} and it has exponential distribution with mean μ_r. The session arrival rate follows an exponential distribution with parameter μ_s. The ongoing sessions are all terminated when the MN turns off the wireless communication (as shown in Figure 5) and T is the total online time of the MN. Figure 5 shows that MN may be involved in two types of sessions during handover: one is the new session and the other one is previously established.

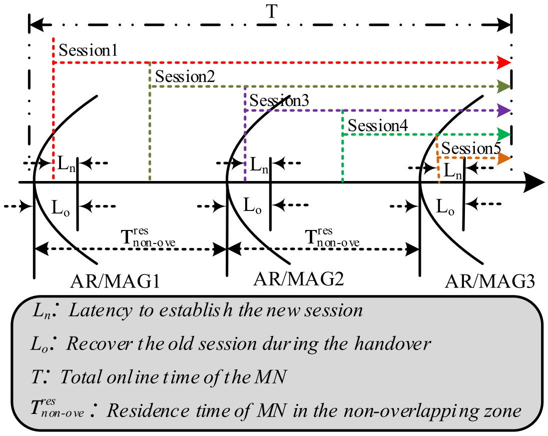
T
Session1
Session2
Session3
Session4
Session5
L_n
L_o
$T^{res}_{non\text{-}ove}$
AR/MAG1
AR/MAG2
AR/MAG3
L_n: Latency to establish the new session
L_o: Recover the old session during the handover
T: Total online time of the MN
$T^{res}_{non\text{-}ove}$: Residence time of MN in the non-overlapping zone

FIGURE 5. Session and mobility models.

If d_{sub} is the radius of a subnet and d_{ove} is the overlapping distance between neighboring subnets. The asymptotic density function that gives the probability of the MN to be at a certain point on a line segment $[0, d_{sub}]$ is given by

$$f_x(x) = -\frac{6}{d^3_{sub}}x^2 + \frac{6}{d^2_{sub}}x \tag{2}$$

where x is any point on the line segment which basically corresponds to the distance between the MN and the center of the subnet [23]. Thus, the probability of a MN being within that subnet is

$$\int_0^{d_{sub}} f_x(x)dx = 1 \tag{3}$$

The probability of the MN being in the overlapping zone is

$$\int_{x_{\min}}^{d_{sub}} f_x(x)dx = 1 + 2(\frac{x_{\min}}{d_{sub}})^3 - 3(\frac{x_{\min}}{d_{sub}})^2 \tag{4}$$

where $x_{\min} = d_{sub} - d_{ove}$.

If $T^{res}_{non-ove}$ is the residence time of MN in the non-overlapping zone (active communication duration), then

$$T^{res}_{non-ove} = T^{res}_{sub} \times (1 - \int_{x_{\min}}^{d_{sub}} f_x(x)dx) \tag{5}$$

We assume that the handover latency is much shorter than the inter-session time. L_n and L_o denote the latency to establish the new session and recover the old session during the handover, respectively. Then the average number of on-going sessions during the handover is

$$S_o = \frac{\sum_{k=1}^{T/\mu_r} \frac{k \times T^{res}_{non-ove}}{\mu_s}}{T/\mu_r} \tag{6}$$

The new pending sessions during the handover is

$$S_n = L_o/\mu_s \tag{7}$$

The new sessions can be accurately served only when the new location is updated among the HA/LMAs.

C. AVERAGE BLANK TIME

The *average blank time* is the duration that the MN is out of communication during handover, and is computed as follows:

$$T_B = \frac{S_n \times L_n + S_o \times L_o}{S_n + S_o} \tag{8}$$

For the basic MIPv6, the handover latency is

$$L_o = L_{l2} + L_{MD} + L_{AC} + 2 \times [\delta a + (n+1)a] \tag{9}$$

where L_{l2}, L_{MD} and L_{AC} denotes the L2 handover latency, mobility discovery latency and new CoA configuration latency in MIPv6 respectively. a is the one-hop wired link transmission latency and δ is the coefficient of the one-hop wireless link transmission latency compared with the wired case.

For the basic PMIPv6, the handover latency is

$$L_o = L_{l2} + 2 \times (n+1)a \tag{10}$$

For our proposed scheme in the host-based case

$$L_o = L_{l2} + L_{MD} + L_{AC} + [\delta a + (H+1)a] \tag{11}$$

For our proposed scheme in the network-based case

$$L_o = L_{l2} + (H+1)a \tag{12}$$

For the four cases (i.e., basic MIPv6-based scheme, basic PMIPv6-based scheme, proposed host-based scheme and proposed network-based scheme), the new sessions arriving during the handover can only be accurately served when the new location is updated. Considering the random distribution of the session arrival rate, the average latency to use the new available binding is $L_n = L_o/2$.

V. NUMERICAL RESULTS

The parameters used in the performance analysis are listed in Table 1 [24]–[26].

TABLE 1. Parameter settings.

Parameter	Value	Parameter	Value
T	1000s	d_{sub}	120m
μ_r	100s	d_{ove}	50m
μ_s	300s	L_{l2}	$10/\lambda_p^2$
n	16	δ , a	5, 0.1ms
L_{MD}	0.2s	L_{AC}	1s

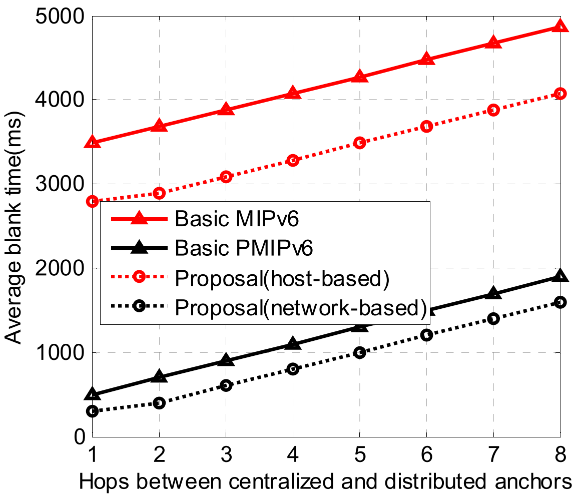

FIGURE 6. Average blank time as the function of distance between centralized and distributed anchors.

Figure 6 shows the variation of average blank time (in milliseconds) as the number of hops between the centralized and distributed anchors is varied.

The distance between the centralized and distributed anchors corresponds to the distance between the AR/MAG and the HA/LMA in the basic mobility management protocol and our proposal, respectively. In the basic MIPv6 and PMIPv6, one anchor point is deployed in order to manage the location of the MN in the administration region and redirect the packets of the MN to its actual position. However, we distribute the function of anchor point in our proposal and in this way the AR/MAG can access the anchor point through a shorter path. The basic PMIPv6 approach improves the performance compared with the MIPv6 approach because of the network based operation, but our proposed approach can optimize the PMIPv6 performance further.

Figure 7 shows the average blank time as a function of one-hop wired link transmission latency.

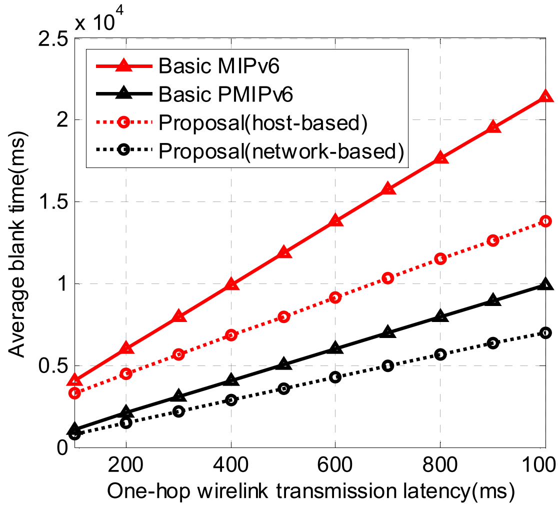

FIGURE 7. Average blank time as a function of one-hop wired-link latency.

Figure 7 shows that the handover latency increases as the one-hop wired link transmission latency increases. However, for wired link latency increases, our proposed approach for both host-based and network-based is more efficient because fewer links are involved in the signaling message exchange. In contrast to MIPv6, the optimized value in the case of PMIPv6 is lower because PMIPv6 is network-based and it avoids the wireless-link transmission latency and address configuration latency.

Although our proposed scheme, like other DMM solutions, can efficiently improve the performance of the mobility management and guarantee the availability of mobility service, DMM will incur additional signaling costs because of state synchronization among the location management entities. Then there is a trade-off between the packet transmission cost and signaling cost for the centralized and distributed mobility management solutions. This issue is analyzed in [27] for DMM.

VI. CONCLUSION

The challenges facing mobile network architectures in the application and service-centric future are indeed tremendous as data demands of mobile users continue to stress the existing network. We argue that a flexible approach to network architectures can go a long way towards addressing these challenges. However, a ''flexible network'' technology must be an evolution of existing networks. Otherwise, network operators will lose huge investments in current network infrastructures to deploy a brand new network – a proposition that is not practical and economically viable.

We promote that DMM offers a promising solution as a remedy of the TCP/IP protocols. This paper proposes a novel but back-compatible all-IP DMM architecture by leveraging an NDN overlay. Accordingly, the name-based routing solution in NDN enables the DMM requirements to distribute the anchor point and optimize the packet transmission path in the mobile computing environment.

ACKNOWLEDGMENT

The authors thank the anonymous reviewers for their valuable comments which helped them improve the quality of this paper.

REFERENCES

[1] C. Perkins, D. Johnson, and J. Arkko, *Mobility Support in IPv6*, document IETF RFC 6275, Jul. 2011.
[2] J. Kempf, *Goals for Network-Based Localized Mobility Management (NETLMM)*, document IETF RFC 4831, Apr. 2007.
[3] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, *Proxy Mobile IPv6*, document IETF RFC5213, Aug. 2008.
[4] *Architecture Enhancements for Non-3GPP Accesses*, document 3GPP TS 23.402, May 2007.
[5] S. H. Ahmed, S. H. Bouk, and D. Kim, "Target RSU selection with low scanning latency in WiMAX-enabled vehicular networks," *Mobile Netw. Appl.*, vol. 20, no. 2, pp. 239–250, Apr. 2015.
[6] H. Chan, Ed., *Requirements for Distributed Mobility Management*, document IETF RFC 7333, Aug. 2014.
[7] A. Yegin, D. Moses, K. Kweon, J. Lee, J. Park, and S. Jeon, "On demand mobility management," IETF draft, draft-ietf-dmm-ondemand-mobility-09, Tech. Rep., Nov. 2016.
[8] S. Gundavelli and S. Jeon, "DMM deployment models and architectural considerations," IETF draft, draft-ietf-dmm-deployment-models-00, Tech. Rep., Aug. 2016.
[9] D. Liu, J. C. Zuniga, P. Seite, H. Chan, and C. J. Bernardos, *Distributed Mobility Management: Current Practices and Gap Analysis*, document RFC 7429, Jan. 2015.
[10] B. Sarikaya, "Distributed mobile IPv6," IETF draft, draft-sarikaya-dmm-dmipv6-00, Tech. Rep., Feb. 2012.
[11] F. Giust, A. de la Oliva, and C. J. Bernardos, "Flat access and mobility architecture: An IPv6 distributed client mobility management solution," in *Proc. 3rd IEEE Int. Workshop Mobility Manage. Netw. Future World (Mobiworld)*, Apr. 2011, pp. 361–366.
[12] J. Korhonen, T. Savolainen, and S. Gundavelli, "Local prefix lifetime management for proxy mobile IPv6," IETF draft, draft-korhonen-dmm-local-prefix-01, Tech. Rep., Jul. 2013.
[13] C. J. Bernardos, A. de la Oliva, F. Giust, T. Melia, and R. Costa, "A PMIPv6-based solution for distributed mobility management," IETF draft, draft-bernardos-dmm-pmip-07, Tech. Rep., Mar. 2012.
[14] S. Matsushima, L. Bertz, M. Liebsch, S. Gundavelli, and D. Moses, "Protocol for forwarding policy configuration (FPC) in DMM," IETF draft, draft-ietf-dmm-fpc-cpdp-05, Tech. Rep., Oct. 2016.
[15] P. McCann, "Authentication and mobility management in a flat architecture," IETF draft, draft-mccann-dmm-flatarch-00, Tech. Rep., Mar. 2012.
[16] A. Feldmann, "Internet clean-slate design: what and why?" *SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 3, pp. 59–64, Jul. 2007.
[17] S. H. Ahmed and D. Kim, "Named data networking-based smart home," *ICT Exp.*, vol. 2, no. 3, pp. 130–134, Sep. 2016.
[18] V. Jacobson, "Networking named content," in *Proc. ACM CoNEXT*, Rome, Italy, Dec. 2009, pp. 1–12.
[19] M. Mealling and R. Daniel, *The Naming Authority Pointer (NAPTR) DNS Resource Record*, document IETF RFC 2915, Sep. 2000.
[20] G. Giaretta, J. Kempf, and V. Devarapalli, *Mobile IPv6 Bootstrapping in Split Scenario*, document IETF RFC 5026, Oct. 2007.
[21] J. Korhonen and V. Devarapalli, *Local Mobility Anchor (LMA) Discovery for Proxy Mobile IPv6*, document IETF RFC 6097, Feb. 2011.
[22] Z. Zhu and A. Afanasyev, "Let's ChronoSync: Decentralized dataset state synchronization in named data networking," in *Proc. IEEE ICNP*, Göttingen, Germany, Oct. 2013, pp. 1–10.
[23] A. A. S. Reaz, M. Atiquzzaman, and S. Fu, "Performance of DNS as location manager for wireless systems in IP networks," in *Proc. IEEE Globecom*, St. Louis, MO, USA, Nov./Dec. 2005, pp. 1–5.

[24] S. H. Bouk, S. H. Ahmed, and D. Kim, ''Vehicular content centric network (VCCN): A survey and research challenges,'' in *Proc. ACM Symp. Appl. Comput. (ACM SAC)*, Salamanca, Spain, Apr. 2015, pp. 695–700.

[25] T.-L. Sheu and B.-C. Kuo, ''An analytical model of two-tier handoff mechanisms for a hierarchical NEMO system,'' *Wireless Netw.*, vol. 14, no. 6, pp. 795–802, Dec. 2008.

[26] J.-H. Lee, Z. Yan, and I. You, ''Enhancing QoS of mobile devices by a new handover process in PMIPv6 networks,'' *Wireless Pers. Commun.*, vol. 61, no. 4, pp. 591–602, Dec. 2011.

[27] S. Wie and J. Jang, ''Distributed mobility management strategy with pointer forwarding technique,'' *J. Inf. Commun. Converg. Eng.*, vol. 13, no. 4, pp. 248–256, Dec. 2015.

ZHIWEI YAN received the Ph.D. degree from National Engineering Laboratory for Next Generation Internet Interconnection Devices, Beijing Jiaotong University. He joined Chinese Academy of Sciences in 2011 and is currently an Associate Professor of China Internet Network Information Center. Since 2013, he has been an Invited Researcher with Waseda University. His research interests include mobility management, network security, and next generation Internet.

GUANGGANG GENG received the Ph.D. degree from the State Key Laboratory of Management and Control for Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing, China. He was with Computer Network Information Center, Chinese Academy of Sciences, in 2008. He is currently an Associate Professor with the China Internet Network Information Center. His current research interests include machine learning, adversarial information retrieval on the Web, and Web search.

SHERALI ZEADALLY received the bachelor's degree from the University of Cambridge, England, U.K., and the Ph.D. degree in computer science from the University of Buckingham, England. He is currently an Associate Professor with the University of Kentucky, USA. He is a fellow of the British Computer Society and the Institution of Engineering Technology, England.

YONG-JIN PARK spent more than 30 years in research and education with Hanyang University, Seoul, and he became a Professor Emeritus in 2010. . He joined Waseda University in 2010. He is currently a professor of University of Malaysia Sabah. He was the President of the Korea Institute of Information Scientists and Engineers in 2003, the Director of Secretariat of Asia Pacific Advanced Network from 1999 to 2003, and the President of the Open Systems Interconnection Association from 1991 to 1992. He visited the Department of Computer Science, University of Illinois, Urbana–Champaign, as a Visiting Associate Professor, from 1983 to 1984. He also visited the Computing Laboratory, University of Kent, Canterbury, U.K., from 1990 to 1991, as a Research Fellow. He was the IEEE Region 10 Director and a member of the IEEE Board of Directors from 2009 to 2010. He is currently a member of the IEEE MGA Nominations & Appointments Committee, the IEEE Region 10 Advisory Committee, and the IEEE Japan Council Executive Committee. He is an IEICE Fellow.