A New Decentralized Mobility Management Service Architecture for IPv6-based Networks

Deguang Le, Jun Lei[*] and Xiaoming Fu[†]
Computer Networks Group, University of Goettingen, Germany.
{le,lei,fu}@cs.uni-goettingen.de

ABSTRACT

In Mobile IPv6, the home network – through a designated home agent – is responsible for distributing all traffic from/to the mobile node in the default bidirectional tunneling mode, when the mobile node is connected to a foreign network. This approach not only lacks sufficient scalability and efficiency of delivery, but also poses a heavy burden on the home network and the global Internet. In this paper we propose a new decentralized mobility management service (DMMS) architecture to address this issue. The idea is to employ a local mobility agent in each access network, which handles node mobility based on local movement information, so that the ongoing communication can be maintained efficiently and scalable without relying on centralized traffic distributing entities.

Categories and Subject Descriptors

C.2.1 [**Network Architecture and Design**]: Distributed networks, network communications, network topology, wireless communication; C.2.2 [**Network Protocols**]: Protocol architecture; C.2.6 [**Internetworking**]: Standards

General Terms

Design, Performance, Security

Keywords

Internet Mobility, Multihoming, SHIM6, Mobile IPv6

1. INTRODUCTION

The rapid diffusion of portable terminals is generating an increasing demand for a global mobility service. The users expect to stay always best connected and enjoy a wide variety of voice, data and multimedia services independently of their geographical location, with performance significantly better than today. It is getting widely accepted that a key technology to achieve these objectives will be the next generation Internet protocol (IPv6) [8], which will support the foreseen growth in the number of mobile users without breaking the end-to-end transparency of the Internet. Besides, The Internet Engineering Task Force (IETF) is developing the Mobile IPv6 (MIPv6) [16] protocol for network layer mobility support in IPv6.

However, several drawbacks exist when using MIPv6 in a mobile computing environment. The most important one identified to date is the centralized strategy for mobility management: as MIPv6 defines a centralized home network for each mobile node, both mobility control messages and data traffic of the mobile node must be managed through the use of a corresponding home address and a home agent in the home network. This centralized mobility architecture not only lacks the flexibility of development, limiting the transfer efficiency (e.g. the high transport latency), but also poses the heavy burden on the home agent, resulting in the instability of network systems (e.g. the home agent/network single-point-of-failure). To solve this deficiency of MIPv6, we propose a new Decentralized Mobility Management Service (DMMS) architecture for IPv6-based networks. This architecture is based on exploiting the SHIM6 protocol to support the handover for mobile nodes. We extend the SHIM6 protocol for mobility management by introducing a new entity, so-called Mobility Agent (MA). The MA is not limited at a specific network, but can be distributed in any local access network. Therefore, wherever the mobile node moves, it can enjoy the mobility service through this local mobility agent that performs the mobility control on behalf of the mobile node.

Our proposal has the advantages of requiring no centralized home registration process and no need of maintaining dedicated home addresses. Besides, due to the decentralized feature, the DMMS architecture has improved stability and efficiency of mobility management. Moreover, such a decentralized scheme is more flexible from the deployment point of view.

This paper is organized below. Following this introduction, Section 2 presents the related work including existing Internet mobility solutions: MIPv6 and Proxy MIPv6 (PMIPv6), and a new network layer protocol SHIM6. In Section 3 we propose an novel alternative Internet mobility solution which integrates the SHIM6 multihoming tech-

[*] J. Lei and D. Le contributed equivalently to this work.

[†] Correspondence to: X. Fu, Institute for Informatics, Lotzestr. 16-18, 37083 Göttingen, Germany, Tel/fax: +49 551 39 144 11/03, Email: fu@cs.uni-goettingen.de.

WMuNeP'07, October 22, 2007, Chania, Crete Island, Greece.

nique is proposed. In addition, we provide details on how the SHIM6 multihoming technique is used for the mobility management in our proposed architecture. Section 4 details the extensions to the MA to be facilitated with SHIM6 for mobility routing in DMMS. In Section 5, we study selected security issues involved in the proposed architecture. Section 6 evaluates the proposal by analyzing and comparing it with MIPv6 and PMIPv6. Finally, we concludes this paper and outlines future work in section 7.

2. RELATED WORK

This section provides a brief overview of the basic MIPv6 [16], Proxy MIPv6 [13] and SHIM6 [20], which are relevant for understanding of our proposed scheme.

2.1 Mobile IPv6

Given the importance of mobility support on the future Internet, in the past several years, many researches on mobility support have been performed, coming up with a number of protocol proposals and schemes [17]. Among them, Mobile IPv6 (MIPv6) [16], developed by the IETF, is the best-known network layer mobility management solution. Its basic principle is to introduce a so-called Care of Address (CoA) as a mobile node's location indicator, which allows the mobile node to keep its ongoing connections while moving from one network to another, without changing its identifier (i.e. the home address).

In MIPv6, when a Mobile Node (MN) moves to a foreign network, it acquires a CoA through either stateful or stateless address auto-configuration. After obtaining a new CoA, the mobile node registers to the Correspondent Node (CN) as well as the Home Agent (HA) with Binding Update messages (BUs). The HA and CN record this binding in their binding cache. After this, packets can be routed with the relay of HA (i.e. the Bidirectional Tunneling, BT), or directly between the MN and CN (i.e. the Route Optimization, RO). In case that the CN wants to communicate to the mobile node for the first time, the first packet is tunneled through the HA. The HA intercepts any packets addressed to the mobile node's home address and tunnels them to the mobile node's CoA using IP-in-IP encapsulation. Figure 1 shows the MIPv6 architecture and its operations.

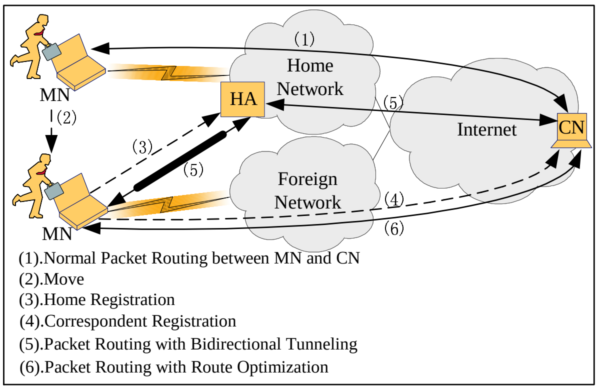
(1)
Home Network
MN
HA
(2)
(3)
(5)
(5)
Internet
CN
Foreign Network
(4)
(6)
MN
(1).Normal Packet Routing between MN and CN
(2).Move
(3).Home Registration
(4).Correspondent Registration
(5).Packet Routing with Bidirectional Tunneling
(6).Packet Routing with Route Optimization

Figure 1: MIPv6 architecture and its operations

The above proposed protocol for Internet mobility management has the features: (1) MIPv6 defines a constant identifier (i.e. the home address) for the transport layer protocols; (2) MIPv6 employs a centralized entity for packet transfer and location information store (i.e. the HA). These features of centralized mobility management, however, introduce the scalability and performance issues that they might raise when the vast majority of Internet nodes will become mobile. The problems of complexity and difficulty supporting incremental deployment of MIPv6 introduce the requirements of a highly efficient treatment of traffic generated on the move, so it deserves to investigate and design a new architecture for the Internet mobility management to plan in advance its long-term evolution in the Internet community. This is certainly a very innovative and challenging area.

To tackle these problems and develop an incremental mobility management scheme from the deployment point of view, we will propose a novel mobility management scheme in this paper.

2.2 Proxy Mobile IPv6

Proxy Mobile IPv6 (PMIPv6) [13] is one of network-based mobility management protocols which can avoid tunneling overhead over the air as well as hosts' involvement in mobility management. PMIPv6 focuses on extending MIPv6 to achieve mobility due to two main reasons. The first reason is that MIPv6 is a very mature mobility protocol for IPv6. There have been many implementations and interoperability events where MIPv6 has been extensively tested. The design of PMIPv6 has considered to re-use these mature mechanisms as much as possible to solve the real deployment problem. Second, PMIPv6 allows re-using the MIPv6-aware home agents (i.e. local mobility anchor) to provide mobility to hosts without requiring any additional mobility management protocol.

Figure 2 gives a brief overview of the PMIPv6 architecture. In the PMIPv6 domain, a new entity – Mobile Access Gateway (MAG) – is introduced. It mainly has the following three functional roles: (1) detecting the mobile node's movement and initiating the signaling with the mobile node's Local Mobility Anchor (LMA) for updating the route to the mobile node's home address; (2) setting up the data path for enabling the mobile node to use its home address for communication from the access link; (3) emulation of the mobile node's home link on the access link.

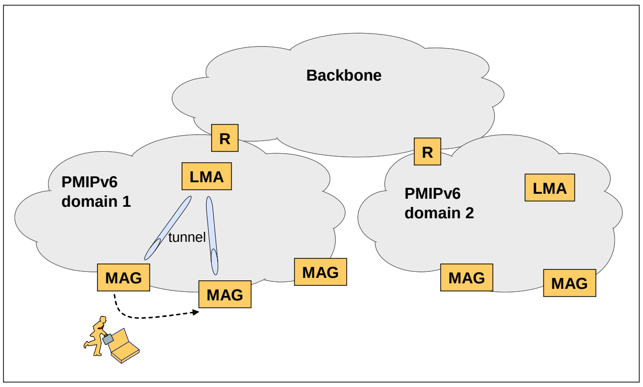

Figure 2: PMIPv6 architecture and its operations

Besides, the Local Mobility Anchor (LMA) is the entity that maintains the binding between the prefix assigned to a mobile node and the local Proxy-CoA. That is, the LMA has the functional capabilities of a home agent as defined in MIPv6 base specification [16] and with the additional required capabilities for supporting PMIPv6 as defined in the specification [13]. From the perspective of the LMA, the MAG is the special entity that sends MIPv6 signaling message on behalf of a mobile node, using its own identity.

Each time the mobile node moves from one MAG to another MAG, it needs to update the current location of the mobile node. For updating this location to the LMA, the MAG sends a Proxy Binding Update (PBU) message to the LMA. Upon receiving the PBU request, the LMA sends a Proxy Binding Acknowledgment (PBA) message to the MAG. Once receiving the PBA message, the MAG will set up a tunnel to the LMA and add a default route over the tunnel to the LMA. After that, the LMA forwards any packet sent by any corresponding node to the mobile node through the current MAG. Therefore, PMIPv6 can also be regarded as one of the centralized mobility management protocols.

2.3 SHIM6

Since we exploit the SHIM6 protocol for mobility management at the network level in our proposal, we will briefly present the SHIM6 protocol as follows.

SHIM6 [20] is a network layer approach for providing the split of locator/identifier of the IP address, so that multihoming can be provided for IPv6 with transport-layer survivability. A SHIM6 node uses a constant IP address (e.g. its initial locator) as the Upper Layer Identifier (ULID) for a Upper Layer Protocol (ULP) connection. Besides, it allows using multiple IP addresses as locators (L) for routing packets. To do so, SHIM6 establishes a context for each ULP connection by using four signalling messages: I1, R1, I2 and R2 (so-called SHIM6 context). This context maintains the state for the mapping between a ULID and a set of locators for each node. Therefore, when the ULID pair of a ULP connection is no longer used as the locator pair, the SHIM6 module can translate the ULID pair into the currently active locator pair. This functionality is indicated in Figure 3.

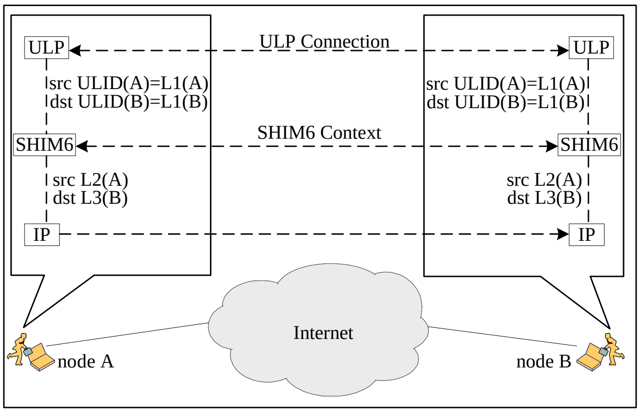

Figure 3: SHIM6 ULID mapping with changed locators

In Figure 3, ULID(A) and ULID(B) represent the identifiers of communicating nodes, i.e., node A and node B respectively, which are used to identify the ULP connection. L1(A) and L2(A) represent the locators in the locator set of node A. These locators are assigned to the multihomed node A by its transit providers. Similarly, L1(B) and L3(B) represent the locators in the locator set of node B. From this figure, we can see that above the SHIM6 protocol, the ULP selects the initial locator pair (e.g. L1(A) and L1(B) in this example) being the ULID pair (e.g. ULID(A) and ULID(B)) [4], which avoids introducing a new identifier name space as well as the modification of ULP. The SHIM6 context provides the binding of a node identifier with a set of locators. When a ULP packet is passed from the ULP to IP through SHIM6, the identifier pair of ULP (e.g. L1(A) and L1(B)) are mapped to a current active pair of locators (e.g. L2(A) and L3(B)). Then, the ULP packet is added with a Payload Extension header for associating with the established SHIM6 context. The reverse mapping is applied to incoming packets, where the incoming locator pair is stripped off the packet, and then the packet header is rewritten with the mapped node ULID pair. Packets are then passed to the ULP. The feature of locator/identifier splitting mechanism of SHIM6 makes SHIM6 a useful component for Internet mobility management.

SHIM6 is used to create the SHIM6 context between end-systems. In order to enable legacy IPv6 nodes, Bagnulo [6] proposes an extension to the SHIM6 architecture to support SHIM6 proxy on behalf of non-SHIM6 capable end-systems, so that the non-SHIM6 capable end-systems can gain the benefits of SHIM6 multihoming.

3. A NEW DECENTRALIZED MOBILITY MANAGEMENT SERVICE ARCHITECTURE FOR IPV6-BASED NETWORKS

In this section, we propose a new decentralized mobility management service (DMMS) architecture by introducing a new entity (i.e. the MA) for mobility management in the local access network. The key idea behind our proposal is to deploy a mobility management entity, so-called Mobility Agent (MA) within each access network. These MAs are allowed to be deployed and operated in a distributed fashion. Upon the distributed cooperation among the mobility agents, wherever the mobile node moves, DMMS can achieve the mobility service through the local MA.

3.1 Decentralized Mobility Architecture

As described in the introductory section, we are considering decentralized architecture that achieves the mobility service from the distributed MAs in the local access networks. The resulting configuration is illustrated in Figure 4.

From this figure, we can see that the proposed architecture has the following components:

3.1.1 Decentralized IP Address

In our proposal, the mobile node within an access network is allocated with a single IP address. It contains the following characteristics: (1) this address is globally unique and routable; (2) this address is dynamically allocated to the mobile node; (3) this address is dependent of the current location of the access network to which the mobile node attaches. So, we call it as a decentralized IP address. Each time the mobile node acquires the decentralized IP address, it will be updated to the Dynamic DNS (D-DNS) server [25], so that the mobile node can establish a new communication with other nodes using the new decentralized IP address as the routing locator as well as the transport connection identifier at the initial stage.

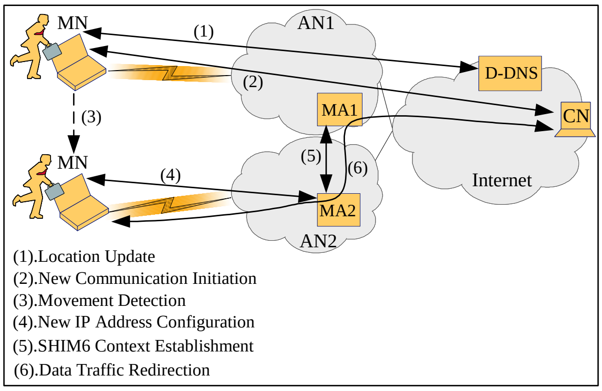
MN
(1)
AN1
D-DNS
(2)
MA1
CN
(3)
MN
(5)
(6)
Internet
(4)
MA2
AN2
(1).Location Update
(2).New Communication Initiation
(3).Movement Detection
(4).New IP Address Configuration
(5).SHIM6 Context Establishment
(6).Data Traffic Redirection

Figure 4: DMMS: Decentralized Mobility Management Service Architecture

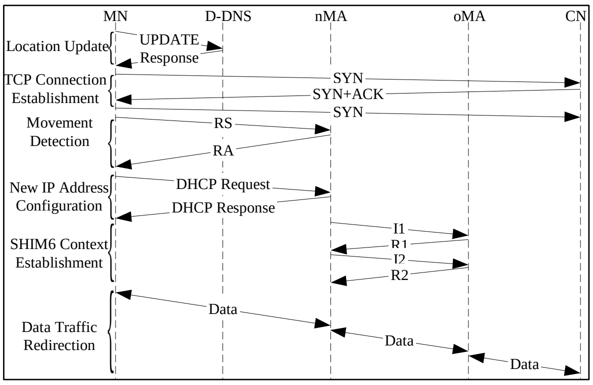

Figure 5: Detailed messages and data flows

3.1.2 Dynamic DNS component

As described above, the mobile node within a local access network is configured with a temporary IP address dynamically. In order to allow other nodes to initiate communications with the mobile node using this IP address, it is necessary to publish this IP address in the DNS dynamically (D-DNS) [25]. Because most applications ubiquitously resolve the Fully Qualified Domain Name (FQDN) to an IP address at the beginning of the communication, D-DNS can be considered for the location management in the mobile environment where the mobile node acts as a server and other nodes actively originate communications with the mobile node. To implement a dynamic DNS, it is necessary to set the maximum caching time of the domain to an unusually short period (e.g. TTL = 0). This prevents other nodes in the Internet from retaining the old address of the mobile node in their DNS cache, so that they will typically contact the name server of the domain for each new connection.

3.1.3 Mobility Agent Component

Once that a mobile node, which has moved into a new local access network, sends a packet containing an external IP address as source address, the packet is intercepted by the new Mobility Agent (MA). At this moment, the new MA (nMA) establishes a SHIM6 context with the old MA (oMA) of the old network. Once that the SHIM6 context has been established, the packets are translated and locators associated to the established context are included in the address fields of the packet. These functions are performed by the MA component.

3.2 Operation Details

The detailed messages and data flow in our proposed architecture are illustrated in Figure 5.

From this figure, we can see the proposed decentralized mobility management scheme is achieved by the following six steps.

3.2.1 Location Update

In the proposed DMMS architecture, each IP address associated with a mobile node (e.g. the MN) is decentralized. Whenever a mobile node attaches to a network, it should perform updating D-DNS in order to keep the mobile node reachable. For this purpose, the MN dynamically registers and updates its FQDN-to-IP entry along with the new IP address to D-DNS servers by sending UPDATE messages (see (1) in Figure 4). In contrast to MIPv6 or PMIPv6, in which the current location information of mobile node is stored in a specific entity (the HA or the LMA), our proposal allows the location information of mobile node to be stored in a type of DNS server. Since DNS is a mature and ubiquitously deployed standard over the Internet, the method in our proposal has the advantage of avoiding an additional entity for location manager without any change in the Internet infrastructure.

3.2.2 New Communication Initiation

When a mobile node (e.g. the MN) attaches to some Access Network (e.g. the AN1) and is assigned an IP address (e.g. the A1) from this network at the beginning, then for the initial connection, the MN uses the A1 as the connection identifier as well as the working locator, and the packet flow passes through the AN1 (see (2) in figure 4). Datagram between the MN and its peer (e.g. the CN) are transmitted through the standard IP routing. Compared with MIPv6, in which each new communication must be initiated through the middle entity (i.e. the HA), our approach allows the CN initiates new communication with the MN through its current location directly. The real benefit of this method in our proposal is that new communication are route optimized.

3.2.3 Movement Detection

When a mobile node moves, it must detect its current location. In IPv6 networks, a mobile node can determine its current location by listening to the router advertisements [23] and comparing the network prefix of the source address within this advertisement with the network prefix of its locator. If the network prefix of the source address within the router advertisement equals the network prefix of the locator of mobile node, the location of mobile node does not change. Otherwise, the mobile node is moving into another network (see (3) in figure 4). Like MIPv6 or PMIPv6, we use the facilities of the inherent IPv6 neighbor discovery mechanism [23] for the movement detection, which is considered well enough for the reason of simplicity. It is, however, expected to incorporate make-before-break technique [21] for fast movement detection.

3.2.4 New IP Address Configuration

When a mobile node attaches to a new access network, it will have to acquire a new IP address. To obtain the new IP address, the mobile node can use either stateful or stateless address auto-configuration methods. In the first case, the mobile node obtains the new IP address from a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [9] server. In the latter case, by using the neighbor discovery protocol [23], a mobile node is able to find the network prefix at any point of attachment that it might select and then adds a unique interface identifier to form a new IP address for that point of attachment [22] (see (4) in figure 4). In MIPv6, many researchers have developed a lot of methods for easing CoA configuration [14, 18]. These techniques can also be exploited for optimizing the new IP address configuration in our proposal.

3.2.5 SHIM6 Context Establishment

Once the local MA (e.g. MA2) is aware that a new mobile node associated an IP address does not belong to the local address space. It will initiate the 4-way handshake to create a SHIM6 context (see (5) in figure 4). In the context, the Upper Layer IDentifier (ULID) pair will be the old IP address of mobile node and the IP address of CN, and the active locator pair will be the IP addresses of MA. Once that the SHIM6 context is established, it is used to process the packets. Compared with MIPv6, which requires registering the current location information (i.e. the CoA) with a constant IP address (i.e. the home address), the SHIM6 context in our proposal allows using the current locator as transport connection identifier. This enables the mobility management function to be distributed and performed at the local access network rather than a centralized network (e.g the home network in MIPv6). Therefore, our method is more flexible from the deployment point of view and has the perceived improvement of reliability of network system over MIPv6.

3.2.6 Data Traffic Redirection

Finally, after SHIM6 context establishment, the ongoing connections established in previous network can transfer datagram continuously. This task can be accomplished by forwarding datagram between oMA and nMA with the help of SHIM6 context. Compared with MIPv6, which employ IP tunnel for data traffic redirection, our approach gains more transport efficiency in terms of the data overhead. In the next sections, we will clarify this advantage through analyzing the detailed procedures.

4. MOBILITY ROUTING IN DMMS

In mobile environments, how to direct data traffic of transport connection between communicating nodes correctly when the communicating node moves away from its current location is a big challenge. This functionality is called as mobile routing. For this purpose, we will describe extensions to the MA to support SHIM6 protocol that will allow continuous data traffic transmission through datagram forwarding between MAs in this section. Figure 4 illustrates the mobility routing mechanisms in DMMS.

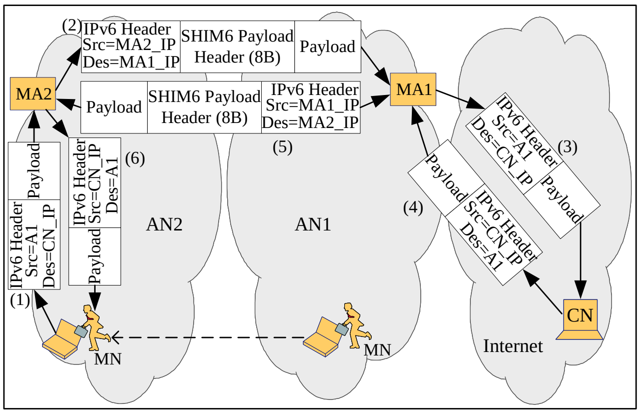

Figure 6: Mobile packet routing in DMMS

From this figure, we can see that in the direction from mobile node (e.g. the MN) to the communicating peer (e.g. the CN), packets sent by the mobile node are delivered to the MA2 via standard IP routing since the MA2 is the mobile node's default router (see (1) in Figure 6). When a packet containing an old IP address (e.g. the A1) as a source address arrives, the MA2 uses the established SHIM6 context to process the packet. To do so, the MA2 sets the IPv6 header's source address to its IP address (e.g. the MA2_IP), the destination address field to the MA1's IP address (e.g the MA1_IP), and adds the context tag to the Payload Extension header (see (2) in Figure 6). When the MA1 receives the packet from the MA2, it parses the extension headers in the order of the normal IPv6 packet processing. If a SHIM6 Payload Extension header is found, it will extract the context tag from the Payload Extension header, and uses this to find a SHIM6 context. With the context in hand, the receiver can now replace the IP address fields with the ULIDs kept in the context. Finally, the Payload Extension header is removed from the packet, yielding the original IP datagram, which is then forwarded to the final destination (e.g. the CN) via standard IP routing (see (3) in Figure 6). This way, the mobile node not only keeps mobility transparent to its upper software, but also passes the packet through any router implementing ingress filtering [11].

In the opposite direction, when sending packets to the mobile node, the CN sends datagram to the mobile node's old IP address (e.g. the A1) via standard IP routing (see (4) in Figure 6). When packets arrive at the old network, the MA1 is able to attract and intercept datagram that are destined to the old IP address of any of its registered mobile nodes. Then, the packets will be forwarded to the MA2 through the established context. To do so, the MA1 specifies its IP address as the source address, the MA2's IP address as the destination address in the IPv6 header, and adding the SHIM6 context tag to the Payload Extension header (see (5) in Figure 6). When the MA2 receives packets, it processes this Payload Extension header and finally delivers packets to the mobile node as if the mobile node was at the old network (see (6) in Figure 6).

In our routing mechanism, an additional IPv6 extension header (i.e. SHIM6 Payload Extension header) is introduced in the data packet. This introduce data overhead. In MIPv6, it has the same problem since it employ tunnel for this purpose. However, compared with MIPv6, the data overhead in our scheme is much little since the SHIM6 Payload Extension header only occupies 8 Bytes while each tunnel header needs 40 Bytes. Moreover, this forwarded packet in our scheme will only traverse a small portion of the Internet, without adding much overhead in overall network.

5. SECURITY CONSIDERATIONS

Several security issues are considered in our proposal. Each time the mobile node moves to a new access network, the new mobility agent has to establish a SHIM6 context with the previous mobility agent. Therefore, the design of rerouting through the MA requires well-defined trust (and business) relationships between two neighboring access networks. For example, they may belong to the same Internet Service Provider (ISP) or otherwise they should have a Service Level Agreement (SLA) between the involved adjacent ISPs. Besides, the MA employs four-way exchanges as suggested in HIP [19] for secure SHIM6 context establishment. The four-way exchanges and use of Nonce of SHIM6 help to make the communication between the new MA and old MA against DoS attacks.

For authenticity, the MA needs to ensure that the routed packet comes from an authentically identified, trusted source. In SHIM6, two techniques (i.e. the CGA [3] and the HBA [5]) are proposed to verify the source. Among them, the HBA is the extension of CGA for providing a cost efficient alternative to public key cryptography based approach without requiring the usage of public key cryptography. However, the HBA assumes the IP addresses of a node are predefined and known in advance, which is not suitable to the mobility case, where the IP addresses of the mobile node are dynamical and are not known a prior. Therefore, we propose using the CGA technique [3] for doing this validation, so that redirection attacks are prevented. In addition, it verifies that the ULID is indeed present at that locator. This verification is performed by doing a return-routability test as part of the probe sub-protocol [1].

As described in our proposal, the mobility control messages in the MA carry the context tag assigned to the particular context. This implies that an attacker needs to discover the context tag before being able to spoof any MA control message. Such a discovery probably requires to be along the path in order to sniff the context tag value. The result is that through this technique, the MA is protected against off-path attackers. In addition, by using the IP address of MA as the source address in the IPv6 header, the packet will be able to safely pass through any router implementing ingress filtering [15].

We further consider the access control mechanisms in the access networks. In MIPv6, the access control is completely relying on the home agent. From the deployment point of view, it might be reasonable since all MIPv6-enabled services will be later charged by the mobile node's home network via the home agent. Differently, in our proposal the first MA to which the mobile node attaches will answer for the Authentication, Authorization and Accounting (AAA) on behalf of the HA. In fact, service related information will be fetched from the HA only once (most likely before access control). Such a mechanism has several benefits. First, it gives incentive to access networks to provide services to mobile nodes. Secondly, it can largely avoid remote services which not only cause long service delay but also consume more network resource. Thirdly, it reduces the possibilities of attacks along the long path.

For the security consideration on D-DNS, any threat [2] to the DNS infrastructure can be against by developing the DNS Security Extensions (DNSSEC) protocol standard [12]. Furthermore, the dynamic UPDATE messages are based on authenticated requests [26] and transactions are used to provide authorization by Secret Key Transaction Authentication for DNS (TSIG) [24] or by DNS Request and Transaction Signatures (SIG(0)) [10]. Only authorized sources are allowed to make changes to the corresponding contents that include the mappings between the IP addresses and domain names.

It is not even possible for us to cover all the security issues in our proposal since security is a challenging issue in any mobility management scheme. Certainly, there are still some known security concerns (e.g. address privacy) with our proposal, and some security related extensions are not yet addressed. For examples, bootstrapping and general stateful packet firewall traversal are open research issues which need to be addressed in the future.

6. PERFORMANCE ANALYSIS

Our proposed scheme has several advantages over MIPv6 [16] and PMIPv6 [13], in terms of its stability and efficiency. First, MIPv6 may suffer from single node failures (e.g. the HA failure) since all traffic from an arbitrary node must traverse through the HA. Differently, our proposal does not rely on any specific entity to perform the mobility management. In case a MA in a particular access network fails, it will only have some impacts on already established connections through this MA. But all the upcoming connections can still be established because other nodes (e.g. newly coming CN) can obtain a new IP address of the mobile node from the dynamic DNS server. The mobile node can achieve the mobility by connecting the new MA at the current access network. Second, our scheme is more efficient since it causes less handover latency than MIPv6 and PMIPv6. In the following subsections, we will identify its efficiency based on a mathematical model.

6.1 Considered Scenario

We firstly introduce a hierarchical topology used for analytical study. Figure 7 depicts the considered scenario. We assume that a mobile node is initially located at the AR and then moves from the AR to a new AR (nAR). The mobile node receives the data packets sent from the Corresponding Node (CN). The analysis will study the cases of MIPv6, PMIPv6 and our proposed DMMS. When PMIPv6 is considered, the mobile access gateway (MAG) will be performed at the access router. Similarly, when considering our DMMS scheme the function of the MA will be performed at access routers. Note that the MIPv6 with route optimization is not considered in the following analysis since it has some extra requirements (e.g. the correspondence node supporting MIPv6). For fairness, our scheme assumes the correspondence node is not SHIM6-enabled.

6.2 Assumptions and Parameters

In order to compute the handover latency we have to consider the latency introduced by both the wireless and the wired part. The handover latency will be analyzed considering the mobile node initiated handover case. We assume that the processing delay are negligible compared to access to the channel and transmission delays. For the wireless part we suppose the same value for the uplink and downlink case. With respect to the parameters, we have the following

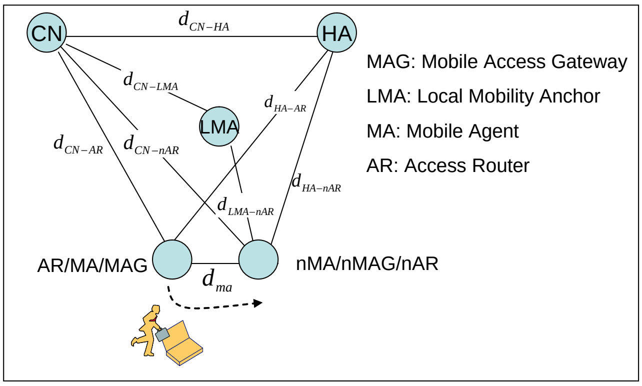

Figure 7: Considered scenario for performance analysis

assumptions.

- d_i only denotes the transmission delay between any two entities. For example, d_{CN-AR} is referred to as the time required by forwarding packets from the CN to the AR.
- It is assumed that the AR and nAR locate at the same access network according to the measurement study in [7] that most of the user's mobility is local. If d_{ma} is the latency of forwarding packets between two neighboring access routers, d_{ma} can be regarded as a quite small value when it is compared with d_{HA-nAR} or d_{CN-AR}.
- The following inequality is satisfied: $d_{ma} < d_{LMA-nAR} < d_{HA-nAR}$. Since the term LMA and HA are interchangeable and depend on the context in which the protocol is used. When the protocol specified in PMIPv6 is used for local mobility management of a host, i.e. within the scope of an access network or administrative domain, the term LMA is used or applicable. When the protocol is used for global mobility management of a host, the entity is essentially a HA.
- The processing latency of local trigger in a mobile node's protocol stack is ignored. Thus, the period used to receive a moment hint with link-layer support is zero.

6.3 Handover Latency Study

Considering MIPv6, in our proposed scenario described in Figure 7, the latency will be 1) the time required to send the BU and receive the BA through the wireless medium, plus 2) the time required by the BU to reach the HA who forwards the packet to the MN, plus 3) the time required by the BA to reach the current nAR, plus 4) the time required by the forwarded packet to arrive at the current nAR and plus 5) the delay caused by the wireless part to send the packet to the mobile node.

Thus, the handover latency performing a handover from the AR to the nAR in MIPv6 can be computed through the following formula:

$$d_w + d_w + d_{HA-nAR} + d_{HA-nAR} + d_{HA-nAR} + d_w \qquad (1)$$

where d_w denotes the delay introduced by the wireless part.

Considering the case of PMIPv6, the latency is 1) the time required to send the PBU from nMAG to LMA, plus 2) the time required by the PBA from LMA to nMAG, plus 3) the time required by the packet from LMA to nMAG, plus 4) the delay caused by the wireless part to send the packet to the mobile node.

Thus, the handover latency performing a handover from the MAG to the nMAG in PMIPv6 can be computed through the following formula:

$$d_{LMA-nAR} + d_{LMA-nAR} + d_{LMA-nAR} + d_w \qquad (2)$$

Considering the proposed decentralized scheme, the latency will be 1) the time required to send the SHIM6 context $I1$ to the MA, plus 2) the time required to receive the SHIM6 context $R1$ from MA, plus 3) the time required by the $I2$ sent to the MA, plus 4) $R2$ received from the MA to the nMA, plus 5) the time required by the forwarded packet to arrive at the current nMA and plus 6) the delay caused by the wireless part to send the packet to the mobile node.

Thus, the handover latency performing a handover from the MA to the nMA in DMMS can be computed through the following formula:

$$d_{ma} + d_{ma} + d_{ma} + d_{ma} + d_{ma} + d_w \qquad (3)$$

where d_{ma} is the latency of forwarding packets between two neighboring access routers.

6.3.1 Handover Latency Results

To summarize the above analysis, the handover latencies introduced by MIPv6, PMIPv6 and DMMS are represented in Table 1.

Table 1: Handover Latency

Protocol	Handover Latency
MIPv6	$3d_w + 3d_{HA-nAR}$
PMIPv6	$d_w + 3d_{LMA-nAR}$
DMMS	$d_w + 5d_{ma}$

6.3.2 Comparison

First, we compare the handover latency introduced by PMIPv6 with that of the basic MIPv6. Then, the latency caused by PMIPv6-aware handover will be compared with that of our proposed scheme.

Based on the assumption that $d_{LMA-nAR}$ is smaller than d_{HA-nAR}, it is very easy to get the following result: $D_{MIPv6} > D_{PMIPv6}$. It is quite reasonable since PMIPv6 can avoid tunneling overhead over the air.

When we compare the equation D_{PMIPv6} and D_{DMMS}, the difference between them is $3d_{LMA-nAR} - 5d_{ma}$. Note that LMA may be located far from the current AR (e.g. the nAR) but the AR is very near from nAR. Without the loss of generality, we can assume that $d_{LMA-nAR} >= 2d_{ma}$. Therefore, the handover latency caused by PMIPv6 is somehow larger than that of our scheme, namely, $D_{PMIPv6} > D_{DMMS}$.

The above analyses indicate that DMMS outperforms MIPv6 and PMIPv6 in terms of handover efficiency, in addition to the benefit of having smaller overhead and less impacts to the global Internet in DMMS as discussed in Section 4.

7. CONCLUSIONS AND FUTURE WORK

Observing from the fact that the centralized mobility management in MIPv6 introduces a number of adverse effects, we propose a new decentralized mobility management scheme. Meanwhile, we extend the SHIM6 protocol for mobility management by deploying a MA in local access networks. Our scheme has many advantages over MIPv6 such as improved stability and efficiency of mobility management. Besides, our scheme first assumes that the correspondence node is not SHIM6-enabled. If the correspondence node supports SHIM6, the performance of DMMS can be further improved.

Since our work is in the primitive stage, there are many challenges to be overcome in the future. Firstly, one next work item will be to make further performance evaluation of this proposal through network simulations. Secondly, fast handover techniques and hierarchical architecture have been developed in the community and being considered useful, how to incorporate these techniques into our proposal for further performance improvement is a meaningful work in the future. Finally, our approach requires data traffic forwarding through the old network even if the mobile node has move into a new network, which increases the transport latency. Therefore it is necessary to optimize the packet routing especially if a corresponding node is mobility-aware. For example, in some cases it may be possible that the data traffic can be transmitted directly between the mobile node and the correspondent node bypassing the old network not matter where the mobile node is connected to. However, this requires additional analysis, as it introduces new potential security threats and some other implications.

Acknowledgements

This work has been partially supported by the EC FP6 IST research project *ENABLE – Enabling Efficient and Operational Mobility in Large Heterogenenous IP Networks* (contract number 027002).

8. REFERENCES

[1] J. Arkko and I. van Beijnum. Failure Detection and Locator Pair Exploration Protocol for IPv6 Multihoming. draft-ietf-shim6-failure-detection-09 (work in progress), July 2007.

[2] D. Atkins and R. Austein. Threat Analysis of the Domain Name System (DNS). RFC3833, 2004.

[3] T. Aura. Cryptographically Generated Addresses (CGA). RFC 3972, Mar. 2005.

[4] M. Bagnulo. Updating RFC 3484 for Multihoming Support. draft-bagnulo-rfc3484-update-00 (work in progress), June 2006.

[5] M. Bagnulo. Hash Based Addresses (HBA). draft-ietf-shim6-hba-03 (work in progress), June 2007.

[6] M. Bagnulo. Proxy Shim6 (P-Shim6). draft-bagnulo-pshim6-01 (work in progress), Mar. 2007.

[7] C. Castelluccia. HMIPv6: A Hierarchical Mobile IPv6 Proposal. Mobile Computing and Communication Review (MC2R), Apr. 2000.

[8] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460, Dec. 1998.

[9] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). RFC 3315, 2003.

[10] D. Eastlake. DNS Request and Transaction Signatures (SIG(0)s). RFC 2931, 2000.

[11] P. Ferguson and D. Senie. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. RFC 2827, May 2000.

[12] A. Friedlander, A. Mankin, W. D. Maughan, and S. D. Crocker. DNSSEC: A Protocol Toward Securing the Internet Infrastructure. *Communications of the ACM*, 50(6):44 – 50, 2007.

[13] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil. Proxy Mobile IPv6. draft-ietf-netlmm-proxymip6-00 (work in progress), Apr. 2007.

[14] A. Gwon and A. Yegin. Enhanced Forwarding from the Previous Care-of Address (EFWD) for Fast Handovers in Mobile IPv6. In *Proceedings of Wireless Communications and Networking Conference (WCNC'04)*, pages 861 – 866. IEEE, 2004.

[15] C. Huitema and M. Bagnulo. Ingress filtering compatibility for IPv6 multihomed sites. draft-bagnulo-shim6-ingress-filtering-00 (work in progress), 2006.

[16] D. Johnson, C. Perkins, and J. Arkko. Mobility Support in IPv6. RFC 3775, June 2004.

[17] D. Le, X. Fu, and D. Hogrefe. A Review of Mobility Support Paradigms for the Internet. *IEEE Communications Surveys and Tutorials*, 8(1):2 – 15, 2006.

[18] N. Moore. Optimistic Duplicate Address Detection (DAD) for IPv6. RFC 4429, 2006.

[19] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson. Host Identity Protocol. draft-ietf-hip-base-08 (work in progress), June 2007.

[20] E. Nordmark and M. Bagnulo. Level 3 Multihoming Shim Protocol. draft-ietf-shim6-proto-08 (work in progress), May 2007.

[21] K. Ramachandran, S. Rangarajan, and J. C. Lin. Make-Before-Break MAC Layer Handoff in 802.11 Wireless Networks. Proceedings of International Conference on Communications (ICC'06), 2006.

[22] S. Thomson and T. Narten. IPv6 Stateless Address Autoconfiguration. RFC 2462, 1998.

[23] T.Narten, E.Nordmark, and W.Simpson. Neighbor Discovery for IP Version 6 (IPv6). RFC 2461, 1998.

[24] P. Vixie, O. Gudmundsson, D. Eastlake, and B. Wellington. Secret Key Transaction Authentication for DNS (TSIG). RFC 2845, May 2000.

[25] P. Vixie, S. Thomson, Y. Rekhter, and J. Bound. Dynamic Updates in the Domain Name System (DNS UPDATE). RFC 2136, 1997.

[26] B. Wellington. Secure Domain Name System (DNS) Dynamic Update. RFC 3007, 2000.