A Dynamic Authentication, Authorization, and Accounting (AAA) Resolution for Hierarchical Mobile IPv6 Network

Jinsuk Baek,[†] *and Eunjung Lee*[††]*,*

[†]Department of Computer Science, Winston-Salem State University, Winston-Salem, NC, USA
[††]PSF Technologies, Inc, Winston-Salem, NC, USA

Summary
In order to provide seamless service in the mobile wireless networks, we need to minimize the disruption time including AAA cost needed to process a handoff of an ongoing session. There are several schemes focusing on this issue. However, they require a lot of signaling message exchanges, resulting in exposures of confidential information of the mobile nodes in the network. Moreover, to the best of our knowledge, no studies have been conducted in the area of AAA resolution protocol for HMIPv6 networks, the next generation platform for mobile networks. In this paper, we propose an efficient scheme called Dynamic AAA that eliminates these disadvantages. The proposed scheme can be applied to the HMIPv6 network for a fast AAA resolution. Simulation results show our scheme can significantly reduce the message overhead while maintaining almost the same handoff delay as other schemes.

Key words:
AAA, MIPv4, MIPv6, HMIPv6 .

Introduction

Access speed in mobile communications has become a daunting task in our every day life due to the widespread use of portable computers and handheld devices such as PDAs and cellular phones [6]. While roaming between different IP networks, mobile users access the Internet to retrieve e-mails, the latest weather report or communicate via video conferencing [2]. Recently, a growing number of mobile applications require mobile users to transmit multimedia data in wireless environments.

In order to transmit this time-sensitive real-time multimedia data in mobile wireless environments, seamless handoff by reducing the disruption time should be provided.

This disruption time for the handoff process can be broadly divided into three parts. The first part is the connection initiation where a mobile node (MN) initiates a new connection with its new foreign network whenever it moves into the foreign network. MN refers to every device which is capable of physically moving from one network link to another. The second part is the registration of the MN. When each MN moves into the foreign network, it should register with the foreign network giving its home network information.

Before accepting the MN, the foreign network should perform a security check such as authentication, authorization, and accounting (AAA) of the MN. Hence, each MN should identify itself by interacting with the AAA server of its home network (*h*AAA). We call this the AAA resolution and it is known to be a time consuming process.

In order to facilitate a mobile device to roam between different wireless or wired access networks, Mobile IP protocols have been introduced by the Internet engineering Task Force (IETF). In a Mobile IPv4 (MIPv4) protocol [7]–[8], the registration can be performed in specialized routers called Foreign Agents (FAs) and Home Agents (HAs). On the other hand, Mobile IPv6 (MIPv6) [3] does not require dedicated routers to act as FAs.

Both protocols allow a MN to maintain a permanent IP address, called home address, while visiting different networks. While the MN is away from its home network, the HA redirects packets to the MN. Whenever a MN changes its point of attachment, they require the MN to update its HA and all correspondent nodes (CNs) communicating with the MN, of its new location. Even if the MN roams between subnets of the same domain, the MN has to send a Binding Update (BU) to its HA which usually resides far away from the MN.

To reduce this signaling overhead caused by the handover process, the concept of Mobility Anchor Point (MAP) is introduced by Hierarchical MIPv6 (HMIPv6) [10]. A MAP serves as a local HA in a foreign network. Whenever a MN moves to a new subnet within the same domain, it sends a BU to the MAP rather than to the HA. This reduces the signaling overhead tremendously, since generally the MAP is much closer to the MN than the HA is. Within large scale network infrastructures, usually several MAPs coexist to improve robustness and enable traffic sharing.

To reduce the AAA resolution cost, *Shadow Registration* [5] and its variants [1, 3, 6] were proposed. The key idea in Shadow Registration is to establish a Security Association (SA) in the neighboring foreign networks *a priori* anticipating a possible handoff when the MN registers to the given network. Thus, when a MN hands off to a neighboring foreign network, the AAA resolution is processed locally within that network without going all the way to the MN's AAA server in the home network. This scheme is found to be efficient but we need to point out that it generates a lot of messages to establish SA between the MN and the AAA servers in all of neighboring foreign networks. Also, establishing a SA to all neighboring domains is not desirable from the security point of view. We have proposed a different approach called Dynamic Shadow Registration [6] that can be applied to both Mobile IP and SIP protocols and some success has been achieved. Unfortunately, neither approach can be straightforwardly applied to the HMIPv6 network having a different architecture. To the best of our knowledge, no studies have been conducted in the area of AAA resolution protocol for HMIPv6 networks, which is a next generation platform for mobile networks. In this paper, we propose an efficient scheme called Dynamic AAA (DAAA) that can be applied to the HMIPv6 network for a fast AAA resolution.

Under our scheme, for the MAP crossing of the MN, the AAA server in the current MAP domain (*m*AAA) predicts the candidate neighboring *m*AAAs for the given MN. After that, it forwards the selected candidate *m*AAAs list to the AAA server of the MN's home network (*h*AAA). The *h*AAA will then multicast the AAA information to the candidate *m*AAAs of the MN. Also, for the subnet crossing of the MN, each AAA server in the subnet domain (*s*AAA) predicts the candidate neighboring *s*AAAs for the given MN. Then, the AAA server in the current subnet forwards the candidate *s*AAAs list to the AAA server of the MAP domain (*m*AAA). As a result, the *h*AAA allows one or more *m*AAAs or *s*AAAs to have security information of the given MN before the MN actually enters the next subnet or MAP domain. The performance of the proposed scheme highly depends on how accurately the AAA servers predict the next AAA servers for the given MN. In order to achieve more accurate prediction, we also propose a new sector based prediction scheme. This scheme allows each subnet or MAP domain to divide its domain into several sectors and requires each domain to maintain a reference table for recording the mobility of its MNs based on the sectors.

The proposed scheme provides two advantages compared to the previous shadow registration scheme when applied to the HMIPv6 network. First, it reduces message overhead, because *h*AAA or *m*AAA sends a message for establishing security association only to a limited number of *m*AAAs or *s*AAAs, which are likely to be an actual AAA servers for a given MN. Second, the MN can be managed in a more secure manner since we prevent other neighboring AAA servers from keeping the credential information of the MN. Both features do not introduce any additional time overhead, since the local AAA servers do not need to contact *h*AAA or *m*AAA of the MN whenever the MN sends a registration request. In addition, the dynamism allows us to maintain the reference table and the number of sectors in a network domain as small as possible.

The remainder of the paper is organized as follows. Section 2 describes the basic AAA procedures for MIPv4 and MIPv6. Also, we review the existing mobility management schemes. In Section 3, we define a sector-based mobility prediction scheme used in our DAAA scheme, introduce our new DAAA scheme in more detail, and show how it can be possibly applied in Mobile IP. In Section 4, we show the performance of the proposed scheme by computer simulation. Finally, our concluding remarks are presented in Section 5.

2. Related Work

Mobile IP allows MN to attach to the Internet through arbitrary access networks within the topology. These access networks have to be managed in a secure manner to ensure that attackers or unauthorized users do not access their networks. MNs should be authenticated based on the authentication process; a decision is made whether these MNs are authorized to gain access. Furthermore, some form of accounting is needed in order to charge mobile users. These processes can be done with Authentication, Authorization and Accounting (AAA) protocol. In this section, we describe the basic AAA resolution procedures in MIPv4 and MIPv6 networks.

2.1 AAA Procedure for MIPv4

To make continuous network coverage for MNs possible, these MNs should stay connected to the network regardless of their location. This requirement creates a conflict between two mobility supports. First, a MN should change its IP address in order to allow correct packet routing. At the same time, it cannot change its IP address without breaking all its existing connections. Mobile IP solves these mobility problems by using two IP addresses: *permanent home address* assigned at the home network and *temporary care-of address* (CoA) representing the current location of the MN. Whenever a MN obtains the new IP address from a foreign network, the binding between the two addresses should be maintained transparently. There are two specialized routers, known as mobility agents, that maintain this mobility binding, namely the home agent (HA) in the home network and the foreign agent (FA) in the visited network.

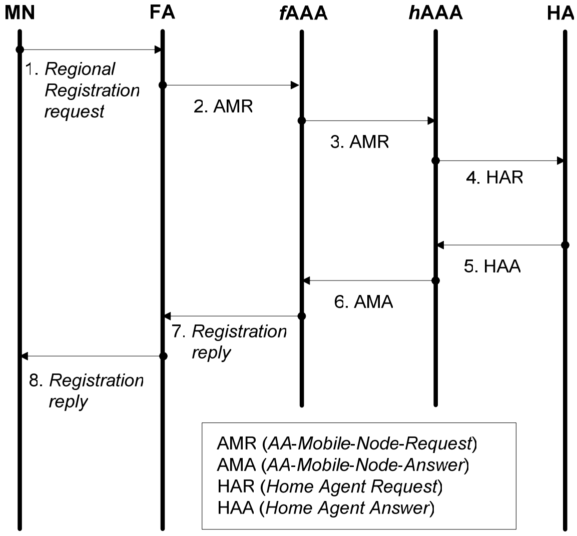


Fig. 1 AAA procedure for MIPv4

The HA resides in the MN’s home network. It is responsible for mapping the *permanent home address* of a MN on its *temporary care-of address*. To store mapping information, the HA maintains a mobility binding table. A FA resides in a network different from the MN’s home network. It maintains a visitor list, containing an entry for each visiting MN. The visitor list holds information about a MN’s home address, the IP address of its home agent, its MAC address and lifetime. Usually, a MN’s *care-of address* matches the IP address of the FA. To enable CN-to-MN communication, the CN must address all packets to the MN’s home address. The HA intercepts these incoming packets. After looking up the MN’s *care-of-address* in its mobility-binding table, the packets are then encapsulated to the MN’s FA. When the MN’s FA receives them, it relays the packets to the MN. To enable MN-to-CN communication, the MN forwards outgoing packets to its FA. The FA in turn, forwards the packets to the designated CN.

As seen in Fig. 1, in order to provide AAA resolution, MIPv4 can involve AAA servers in both foreign network (*f*AAA) and home network (*h*AAA) requiring the following sequence of actions when the MN starts initial registration at a FA:

1. The MN sends the *Registration Request* message to the FA.
2. The FA then modifies the message into the *AA-Mobile-Node Request* (AMR) message and sends it to the *f*AAA.
3. When the *f*AAA receives the AMR message, it forwards the message to the *h*AAA of the MN.
4. The *h*AAA should now contact HA to get a certification of the MN. In order to do this, it generates a *Home Agent Request* (HAR) message and sends it to the HA.
5. The HA processes this message and then responds with a *Home Agent Answer* (HAA) message.
6. After receiving a positive answer, the *h*AAA generates and sends an *AA-Mobile-Node-Answer* (AMA) message to the *f*AAA.
7. This AMA message is possibly modified to a *Registration Reply* and forwarded to the FA.
8. Finally, the FA returns the *Registration Reply* message to the MN.

To reduce the time required to process inter-domain handoff, the *Shadow Registrations* [5] was proposed. This scheme can be applied in the MIPv4. Under this scheme, the current *f*AAA of the MN makes a list of all neighboring *f*AAAs and sends the list to the *h*AAA of the MN with the AMR message. The *h*AAA of the MN will broadcast the security credentials of the MN to the all of the neighboring *f*AAAs. Therefore, it establishes a registration status in the neighboring administrative domains *a priori* before the actual handoff occurs. As a result, it can reduce the handoff processing time because the security credentials of the MN are already available at the next *f*AAA when the MN handoff to that domain. When the Shadow Registration scheme is applied to the MIPv4 network, the step 3 and step 6 are changed as follows.

3. When the *f*AAA receives the AMR message, it adds the information about its neighboring *f*AAAs to this message. After that, it forwards the message to the *h*AAA of the MN.

6. After receiving a positive answer, the *h*AAA generates and sends an *AA-Mobile-Node-Answer* (AMA) message to all of the neighboring *f*AAAs. Hence, there can be as many AMA messages as the number of the neighboring *f*AAAs.

2.2 AAA Procedure for MIPv6

MIPv6 has been proposed to overcome the lack of available IP addresses and eliminate several other disadvantages of MIPv4. MIPv6 does not require special routers to act as FAs. Enhanced features like neighbor discovery and address auto-configuration enable the MN to function in any IPv6 network environment. On the other hand, MIPv6 is extensible to support unforeseen future needs by introducing extension headers. Further improvements are built in support for route optimization and a lowering of routing bandwidth overhead. AAA procedures for MIPv6 can be performed based on the DIAMETER extension for MIPv6 protocol.

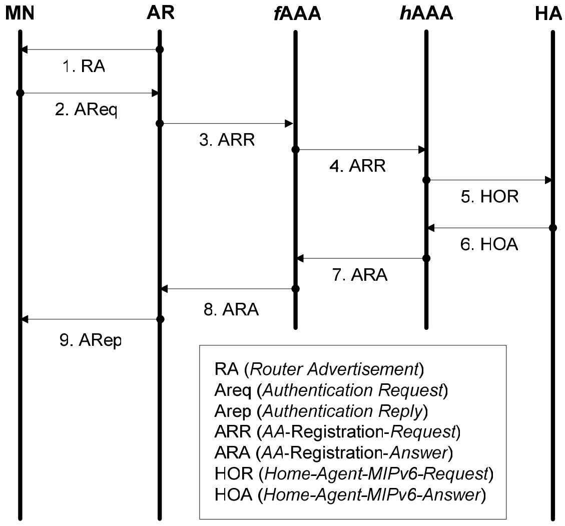

MN
AR
*f*AAA
*h*AAA
HA
1. RA
2. AReq
3. ARR
4. ARR
5. HOR
6. HOA
7. ARA
8. ARA
9. ARep
RA (*Router Advertisement*)
Areq (*Authentication Request*)
Arep (*Authentication Reply*)
ARR (*AA*-Registration-*Request*)
ARA (*AA*-Registration-*Answer*)
HOR (*Home-Agent-MIPv6-Request*)
HOA (*Home-Agent-MIPv6-Answer*)

Fig. 2 AAA procedure for MIPv6

As seen in Fig. 2, the DIAMETER extension for MIPv6 requires the following sequence of actions when the MN starts registration at a subnet domain:

1. When a MN enters a new administrative domain, it listens to a Router Advertisement (RA) messages from the AR in that domain.
2. The MN sends an *Authentication Request* (AReq) message to the AR based on the security key shared with its *h*AAA.
3. When the AR receives an AReq message, it creates an *AA-Registration-Request Command* (ARR) message and sends it to the *f*AAA.
4. The *f*AAA relays it to the *h*AAA of the MN.
5. Upon receiving the ARR message from the *f*AAA, the *h*AAA should now contact HA to get a certification of the MN. In order to do this, it generates a *Home-Agent-MIPv6-Request Command* (HOR) message and sends it to the MN's HA.
6. The HA processes this message and creates a key to establish a SA with the MN. After that, it responds with a *Home-Agent_MIPv6-Answer Command* (HOA) message.
7. After receiving a positive answer, the *h*AAA generates and sends *AA-Registration-Answer Command* (ARA) message that has an authentication result and sends it to the *f*AAA.
8. The *f*AAA stores the authentication result locally and forward the ARA message to the AR.
9. The AR possibly modifies the ARA message into the *Authentication Reply* (ARep) message and forwards it to the MN. Based on this message, the MN now knows the authentication result from the *h*AAA and the established key for the SA.

3. Proposed Scheme

3.1 Hierarchical Mobile IPv6

We start this section by summarizing the standard Hierarchical Mobile IPv6 protocol. A major disadvantage of MIPv6 is its high handoff latency. Every time a MN moves into a new Access Network a sequence of signaling takes place. The MN configures its new IP address and updates its HA and CN by sending BU messages. HMIPv6 establishes the concept of MAP to reduce the signaling overhead during the handoff procedure. A MAP exempts the MN from transmitting expensive BUs to its HA and CNs, when its movement is limited to the same administrative domain.

The MAP acts as a local HA within the visited domain. It is located on any level in a hierarchical network of routers, including the AR. Whenever a MN moves to a new subnet within the domain of its associated MAP, it sends a BU to the MAP rather than to the HA. As the HA is typically further away than the local MAP, the handover process is sped up dramatically.

Two new IP addresses are established to employ HMIPv6: A Regional Care-of Address (RCoA) and a Local Care-of Address (LCoA). The RCoA is an address on the MAP's subnet. The LCoA is the on-link address configured on a MN's interface based on the prefix advertised by its default router. When a MN enters a new administrative domain it is informed about the presence of MAPs by collecting Router Advertisement messages of the AR. Once the MN has selected the best fitting one, it sends to the chosen MAP, a local BU containing its RCoA and LCoA. When the MAP accepts the binding request, it will create a Binding by storing the IP addresses in its binding cache and answer with a Binding Acknowledgement (BA). After the MN receives the BA of its MAP it sends a BU to its HA, containing its RCoA. Following a successful registration, a bi-directional tunnel between the HA and the MAP is established. All packets sent by the MN will be tunneled to the MAP. All packets addressed to the MN are intercepted by the HA and forwarded to the MN's RCoA. The MAP will intercept the packets and tunnel them to the MN by using the corresponding LCoA.

The main advantage of HMIPv6 is the fact that a MN does not have to send a BU to its HA when it moves to another subnet within the MAP's domain. As the MN will still be bound to the same MAP, its RCoA is unmodified and its LCoA is changed. Therefore the MN has to send a BU to its MAP. There is no need to update its HA, as the HA is only aware of the MN's RCoA. HMIPv6 also supports route optimization by delivering packets between CN and MN on the shortest possible path.

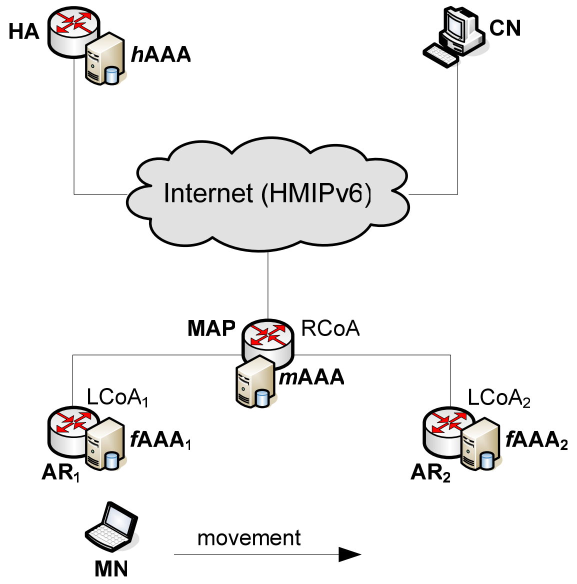


Fig. 3 AAA Architecture for HMIPv6

In HMIPv6 network, the MAP can be utilized to perform access control on MNs and interact with AAA protocol. For example, the AAA server in the MAP domain (*m*AAA) can speed up a handoff process by having the MN's security credentials which will allow it to verify whether a newly entered MN is allowed access to the network.

The *m*AAA also interacts with *h*AAA in performing the AAA process for newly entered MN. The most straightforward scenario would be as follows: A *m*AAA of the MAP domain can store the MN's security credentials after the MN is allowed network access. During the subnet domain handoff, the *m*AAA could pass the MN's security credentials to the *f*AAA located in the new AR's domain to avoid performing the AAA process involving the *h*AAA and CN of the MN whenever the MN moves to a different subnet. Fig. 3 shows an example of the network architecture for AAA services in HMIPv6 network.

3.2 Sector-Based Mobility Prediction

Our Dynamic AAA (DAAA) scheme establishes the security association between the MN and the *m*AAAs for MAP domain handoff and between the MN and the *f*AAAs for subnet domain handoff before the actual handoff occurs. In order to achieve this, the *h*AAA should transmit messages to the neighboring *m*AAAs or *f*AAAs of the MN. Unlike the Shadow Registration scheme, the DAAA scheme requires the *h*AAA to send the messages only to the selected candidate neighboring *m*AAAs or *f*AAAs that are likely to be actual *m*AAAs or *f*AAAs of the MN rather than to all neighboring *m*AAAs or *f*AAAs.

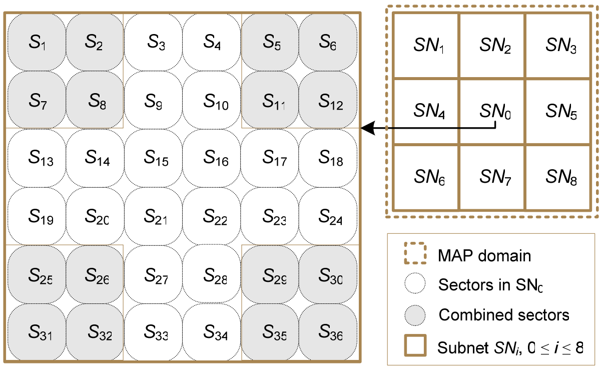


Fig. 4 Subnet Structure with Sectors

For our scheme to be efficient, the current *m*AAA needs to predict the candidate *m*AAAs for a given MN in a MAP domain level. The current AR also needs to predict the candidate *f*AAAs for a given MN in a subnet domain level. In order to predict the candidate *f*AAAs, we propose a new sector-based prediction scheme. Even though this scheme describes how the current AR of the MN can predict the candidate *f*AAAs for the MN, it can be inherently applied in predicting the candidate *m*AAAs in a MAP domain level, which exists on upper level. Under our scheme, the candidate *f*AAAs selection is not static. Instead, it dynamically selects the candidate *f*AAAs for a given MN based on the reference table. As we will see, the *f*AAA maintains the reference table for the network and divides the network into multiple sectors. The reference table contains the mobility information for each sector. Our scheme makes the following assumptions:

- Each subnet network *i* (SN$_i$) has *SN(i)* neighboring subnets.
- Each SN$_i$ is divided into $N_S(i)$ sectors.
- There are $N(i)$ MNs in one subnet (SN$_i$).
- There is a *f*AAA for one subnet. Hence, the *f*AAA is responsible for predicting and selecting one or more candidate *f*AAAs for its $N(i)$ MNs.
- The *f*AAA assigns a sector ID to each of the sectors in its network such that S_j for j = 1, 2, ….., $N_S(i)$.
- The *f*AAA also assigns a SN ID to its neighboring SNs such that SN_i for i = 1, 2, ….., $SN(i)$.

As seen in Fig. 4, each *f*AAA arbitrarily divides its network into $N_S(i)$ (>1) equal size sectors at the initial phase. The sectors are dynamically resized depending on the handoff probability in each sector.

Table 1 shows an example of the reference table. In this table, the first row implies that (1) the MN is now located in SN_0, (2) it was previously in SN_8 before handoff, (3) it was previously in S_7 of the SN_0, (4) it is currently in S_1 of the SN_0, and (5) the probability the MN moves to a certain sector in SN_1 is P_1.

Table 1: Example of the reference table for SN_0

From	Old_sector	Current_sector	To	Probability
SN_8	S_7	S_1	SN_1	P_1
SN_8	S_7	S_1	SN_2	P_2
SN_8	S_7	S_2	SN_2	P_3
SN_8	S_7	S_2	SN_1	P_4
SN_8	S_8	S_1	SN_1	P_5
SN_8	S_8	S_1	SN_2	P_6
SN_8	S_8	S_2	SN_1	P_7
SN_8	S_8	S_2	SN_2	P_8
…	…	…	…	…

After that, the *f*AAA observes the movement of the MNs in its network. Based on this observation, it creates and maintains the reference table containing all of the combinations of the movement history whenever its MNs handoffs. The reference table is comprised of five fields that are as follows.

- From: It is an ID of the SN from where the MN originally came.
- Old sector: It is a previous sector number of the MN when the MN handoffs in the current sector.
- Current sector: It is a current sector number when the MN handoffs.
- To: It is an ID of the SN to where the MN handoffs.
- Probability: It is a probability that the MN handoffs in the current sector with a combination of (Old sector, Current sector, and To).

Given the network structure shown in Fig 4, Table 1 shows an example of the reference table maintained in each of the *f*AAA. In this example, during some amount of time, the *f*AAA has collected some mobility history of its MNs in each sector. The sectors can then be broadly divided into two regions. One is no handoff region and the other is handoff region. Our scheme requires each subnet to eliminate some entries in a no handoff region where no handoff occurs. We can determine these entries by checking their probability field. If any handoff has not occurred in those regions, its value should be equal to 0.

Owing to this dynamic management, our scheme maintains the table size as small as possible. Also, the *f*AAA will combine some sectors showing the same handoff tendency into one single sector. As a result, the *f*AAA will maintain relatively small number of sectors in its reference table.

Based on this table, each *f*AAA selects one or more candidate *f*AAAs in a given sector. The number of candidate *f*AAAs depends on the mobility tendency. That is, the *f*AAA selects the candidate *f*AAAs for each MN by considering a probability threshold *T*.

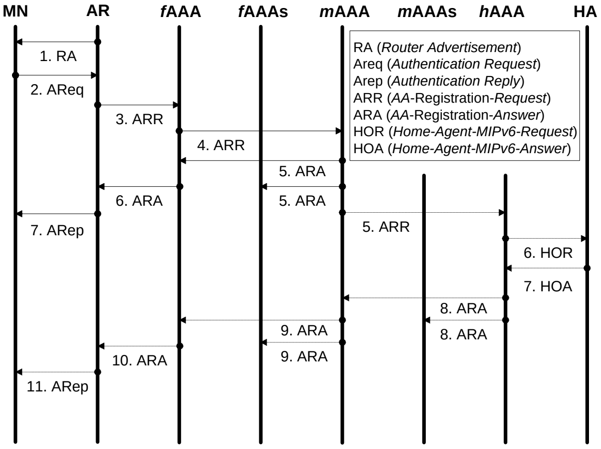

MN
AR
*f*AAA
*f*AAAs
*m*AAA
*m*AAAs
*h*AAA
HA
RA (*Router Advertisement*)
Areq (*Authentication Request*)
Arep (*Authentication Reply*)
ARR (*AA*-Registration-*Request*)
ARA (*AA*-Registration-*Answer*)
HOR (*Home-Agent-MIPv6-Request*)
HOA (*Home-Agent-MIPv6-Answer*)
1. RA
2. AReq
3. ARR
4. ARR
5. ARA
6. ARA
5. ARA
7. ARep
5. ARR
6. HOR
7. HOA
8. ARA
9. ARA
8. ARA
10. ARA
9. ARA
11. ARep

Fig. 5 AAA procedure for HMIPv6

Our simulation allows us to manually set up the threshold. After defining the probability threshold, the *f*AAA will select one or more SNs until the sum of the probabilities is greater than or equal to the threshold. We also need to mention that this selection is based on the highest probability first mechanism. To apply this to our DAAA scheme, we require the *f*AAA to transmit an ARR message to the *h*AAA of the MN when the MN enters the corresponding sector. These messages include information about the selected candidate *f*AAAs of the MN.

3.3 Dynamic AAA Resolution for HMIPv6

In this section, we show how our Dynamic AAA (DAAA) scheme can be applied for HMIPv6 to reduce disruption time in the inter-domain handoff. The procedure is depicted in Fig. 5. It requires the following sequence of actions when the MN starts registration at an AR:

1. The MN listens to a Router Advertisement (RA) messages from the AR in the new administrative domain.
2. The MN sends an *Authentication Request* (AReq) message to the AR based on the security key shared with its *h*AAA.
3. When the AR receives an AReq message, it creates an *AA-Registration-Request Command* (ARR) message and sends it to the *f*AAA.

4. At a given time, the *f*AAA predicts and selects one or more candidate *f*AAA for a given MN based on prediction algorithm. When the *f*AAA receives the ARR message, it adds the information about the candidate *f*AAAs to this message then it forwards the message to the *m*AAA of the MN.
5. Upon receiving the ARR message from the *f*AAA, the *m*AAA generates and sends *AA-Registration-Answer Command* (ARA) message that has an authentication result and sends it to the candidate *f*AAAs.
6. The candidate *f*AAAs stores the authentication result locally and the current *f*AAA who sent the ARR message to the *m*AAA forwards the ARA message to the AR.
7. The AR modifies the ARA message into the *Authentication Reply* (ARep) message and forwards it to the MN. Based on this message, the MN now knows the authentication result from the *m*AAA and the established key for the SA.

The MAP performs similar processes as above at the MAP domain level. That is, each *m*AAA of the MAP domain divides its network into subnets at the initial phase. It also creates a MAP-level reference table and maintains the table by observing the movement of the MNs in its domain. Based on the probability field of the reference table, it predicts one or more candidate *m*AAA for any given MN. When current *m*AAA receives ARR message from the *f*AAA but if it does not have the security credentials of the MN, the *m*AAA processes the following sequence of actions:

1. At a certain time, the *m*AAA predicts and selects one or more candidate *m*AAA for a given MN based on the prediction algorithm. When the *m*AAA receives the ARR message, it adds the information about the candidate *m*AAAs to it and then forwards it to the *h*AAA of the MN.
2. Upon receiving the ARR message from the *m*AAA, the *h*AAA should now contact HA to get a certification of the MN. In order to do this, it generates a *Home-Agent-HMIPv6-Request Command* (HOR) message and sends it to the MN's HA.
3. The HA processes this message and creates a key to establish a SA with the MN. It then responds with a *Home-Agent_HMIPv6-Answer Command* (HOA) message.
4. After receiving a positive answer, the *m*AAA generates and sends *AA-Registration-Answer Command* (ARA) message that has an authentication result to the candidate *f*AAAs.

We have showed how our DAAA scheme could be applied for the HMIPv6. Under the scheme, we require the *f*AAA to select some candidate neighboring *f*AAAs that are likely to be the next *f*AAAs of the MN. After selecting the candidate *f*AAAs, it sends an ARR or *Request* message to the *m*AAA of the MN. This message contains the information about the candidate neighboring *f*AAAs. The ARA message is transmitted form the *m*AAA as long as the *m*AAA already has the security credentials of the MN.

Owing to these properties, our scheme has two advantages over other schemes. First, it reduces message overhead because the *h*AAA and *m*AAA send a message for establishing security association only to limited number of *m*AAA and *f*AAAs, respectively. Second, the MN can be managed in a more secure manner since the scheme prevents other neighboring *m*AAAs or *f*AAAs from keeping the credential information of the MN. Moreover, our scheme does not introduce any additional time overhead since the *f*AAAs do not need to contact the *m*AAA and the *m*AAA does not need to contact the *h*AAA whenever a new MN sends a registration request. As a result, our DAAA scheme guarantees a registration time that is as fast as the fastest existing scheme.

4. Performance

We evaluate the performance of the proposed scheme by using computer simulation. In mobile IP networks, there are a lot of MNs and these nodes have different mobility tendencies in general. Thus, in our simulation, we assume there are 10,000 MNs (*SN(i)* =10,000) in a subnet and these nodes have an independent mobility tendency and their initial location is randomly generated. We also assume there are 9 subnets in a MAP domain. Subsequently, each subnet has 8 neighboring subnets (*SN(i)* = 8). We also assume that there are initially 36 sectors ($N_S(i)$=36) in a subnet. Our simulation model is depicted in Fig. 4.

The speeds of the users range from 4km/hr to 130km/hr. We categorize these users into three groups depending on their speeds: low speed users with a speed of 4 km/hr – 6 km/hr, medium-speed users with a speed of 15 km/hr – 55 km/hr, and high-speed users with speed above 55 km/hr up to 130 km/hr. Finally, we assume all sectors are square and all users can move in eight directions: East, Southeast, South, Southwest, West, Northwest, North, and Northeast.

In order to show that our scheme works generally well in various environments, we use three different types of movement traces including one real trace and two artificially generated traces. First, we use real MN's movement records from Stanford University [9]. They divided a certain region into equal size subnets and recorded the MN's movements in between the subnets for the time slot. We call this the ***M*1** type model. Second, we consider a more general case such as a metropolitan area where most users are low or medium-speed users. Based on this, we assume a composition of 40% low-speed users, 40% medium-speed users, and 20% high-speed users. We call this the ***M*2** type model. Lastly, we consider one extreme but reasonable case such as a highway where most users are high-speed users. Here, we assume a composition of 5% low-speed users, 15% medium-speed users, and 80% high-speed users. We call this the ***M*3** type model. In order to consider more general cases, we restrict the moving directions of the MNs depending on their speeds.

- In case of the low-speed users such as a pedestrian, their moving direction is randomly generated every time unit.
- In case of the medium-speed users such as power walkers or low speed drivers, their moving direction can also be random but we need to consider that many of them will keep their previous directions. Hence, we decide to make 50% of the medium-speed users keep their previous directions. The other 50% of the medium-speed users will change their directions every 7 time unit.
- In case of the high-speed users such as high-speed drivers, their moving direction can also be random but we need to consider that most of them will keep their previous directions. Therefore, we decide to make 90% of the high-speed users keep their previous directions. The other 10% of high-speed users will change their directions every 10 time unit.

Each *m*AAA in a MAP domain and *f*AAA in a subnet domain keeps tracking the MN's movements from the initial position, calculate their next subnet or sectors considering their speeds and directions, and update the reference table whenever a MN moves to another MAP domain or subnet domain.

4.1. Error rate

Our scheme can keep the prediction error rate very close to 0 by using enough data for setting up the table and reasonable probability threshold *T*. Fig. 6 shows that the error rate decreases as we increase the threshold *T*. It also indicates the most reasonable threshold is 0.9. Fig. 7 shows how the error rate can be decreased when we use more data for reference table setup with a threshold 1. We used 70% of data for the reference table setup. In the case of the ***M*3** model with the DAAA, we can see that the error rate is 0.1018% when we use 10,000 data. As we will see, our small penalty can be sufficiently compensated by the reduced number of control messages and more secure property. When the MN arrives at the subnet located at the edge of the MAP domain, it is possible that both *m*AAA of the MAP domain and *f*AAA of the subnet domain try to predict the next *m*AAA or *f*AAA. According to our observation, this situation did not occur because we assume that each *f*AAA does not have any information of other *f*AAAs which are located in the different MAP domain. As a result, other *f*AAAs of the different MAP domain cannot be contained in the candidate *f*AAAs list of the given MN.

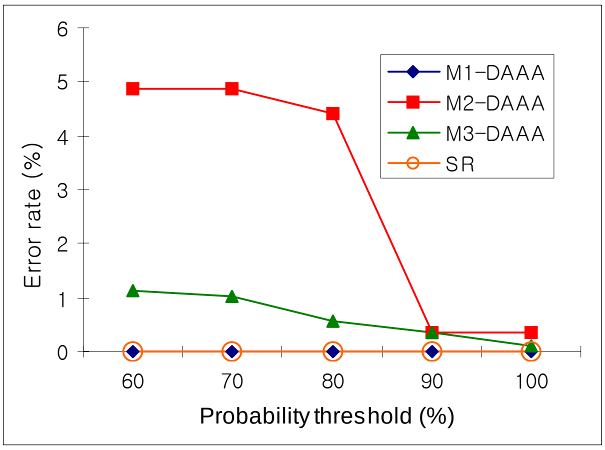


Fig. 6 The error rate vs. the probability threshold *T*

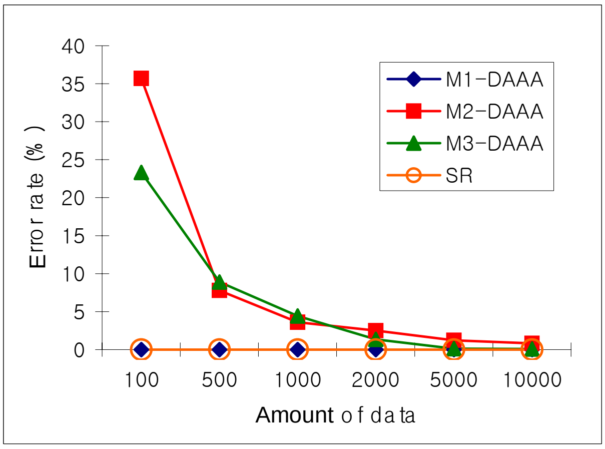


Fig. 7 The error rate vs. the number of data (*T* = 1)

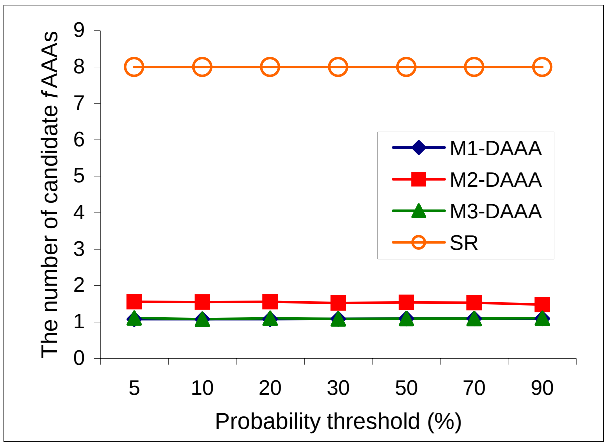


Fig. 8 The number of candidate *f*AAAs vs. probability threshold *T*

4.2. The number of candidate *f*AAAs

Fig. 8 shows the average number of the candidate *f*AAAs of each MN in DAAA is less than 2 while it is always 8 in the shadow registration scheme. Our performance is consistent regardless of the threshold *T*. This reduced number of the candidate *f*AAAs indicates that our scheme can significantly reduce the message overhead compared to the shadow registration scheme.

4.3. Disruption time

Our scheme can significantly reduce the disruption time compared to the HMIPv6 without DAAA support, because one or more neighboring *f*AAAs have the credential information of the MN before the MN actually handoff to the *f*AAAs. In this section, we make an analytic comparison in terms of the disruption time for handoff. In our analysis, we make the following assumptions:

- The average round-trip time between the MN and the AR is $RTT_{<MN,\ AR>}$(=10ms), which is the average round-trip time to send and receive a message over the wireless link;
- The average round-trip time between the MN and the *f*AAA is $RTT_{<MN,\ fAAA>}$(=12ms), which is the average round-trip time to send and receive a message over the subnet;
- The average round-trip time between the MN and the *m*AAA is $RTT_{<MN,\ mAAA>}$(=15ms), which is the average round-trip time to send and receive a message over the MAP domain;
- The average round-trip time between the MN and the *h*AAA is $RTT_{<MN,\ hAAA>}$(=25ms), which is the average round-trip time to send and receive a message from the home network;
- The average round-trip time between the MN and the CN is $RTT_{<MN,\ CN>}$, and the average round-trip time between the MN's home network and the CN is $RTT_{<HA,\ CN>}$. This delay varies.
- Finally, we assume all control messages for initial registration and handoff are reliably delivered.

In the HMIPv6, the total required time for subnet handoff is given by

$$T_{HMIPv6} = RTT_{<MN,\ WL>} + RTT_{<MN,\ mAAA>} + RTT_{<MN,\ CN>} \quad (1)$$

In the HMIPv6 with SR support, the total required time is given by

$$T_{HMIPv6\_SR} = RTT_{<MN,\ WL>} + RTT_{<MN,\ fAAA>} + RTT_{<MN,\ CN>} \quad (2)$$

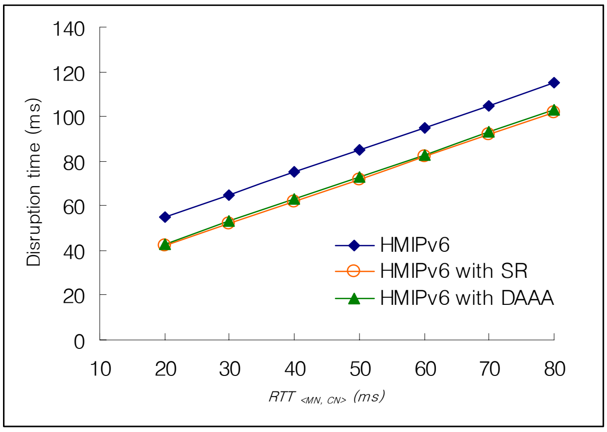


Fig. 9 Disruption time for Mobile IP models vs. $RTT_{<MN,CN>}$

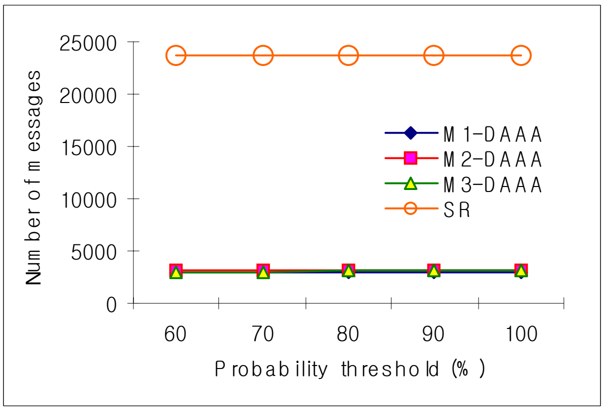


Fig. 10 The number of messages vs. the threshold *T*

In the HMIPv6 with DAAA support, the disruption time can be reduced depending on the error rate *E*. In our simulation, we set *E* to 0.003.

$$T_{HMIPv6\_DAAA} = RTT_{<MN, WL>} + RTT_{<MN, fAAA>}(1-E) + RTT_{<MN, mAAA>}E + RTT_{<MN, CN>} \quad (3)$$

As we can see in Fig. 9, the DAAA shows almost the same performance as the SR in terms of the disruption time when it is applied to HMIPv6.

4.4. The number of messages

Our scheme significantly reduces the number of the AMA messages compared with the shadow registration scheme, because the *h*AAA and *m*AAA of the MN transmits the messages to a relatively small number of the *m*AAAs and *f*AAAs. Fig. 10 shows the number of ARA messages as a function of probability threshold *T*. As we can see, our scheme always achieves very low message overhead with reasonable threshold *T*. Our scheme reduces about 87% of the message overhead compared to the shadow registration scheme for HMIPv6 model.

5. Conclusion

We propose that the *m*AAA and *f*AAA respectively select some candidate neighboring *m*AAAFs and *f*AAAs that are likely to be the next *m*AAAs or *f*AAAs of the MN in a HMIPv6 network. Our scheme sometimes miss-predicts the actual *m*AAA or *f*AAA of the MN, imposing an additional round trip time penalty between the actual *m*AAA or *f*AAA of the MN and the *h*AAA of the MN. However, we can keep this error rate very close to 0. This minor penalty can be sufficiently compensated by a significantly reduced message overhead. It also prevents the credential information from being exposed to other *m*AAAs or *f*AAAs.

References

[1] R. Chellappa, A.Jennings, and N. Shenoy, "A Comparative Study of Mobility Prediction in Fixed Wireless Networks and Mobile Ad hoc Networks," *In Proc. of the IEEE ICC 2003*, pp. 891-895, May 2003.

[2] B. Goode, "Voice over Internet Protocol (VoIP)," *In Proc. of the IEEE,* 90(9):1495–1517, September 2002.

[3] E. Gustafsson, A. Jonsson, and C. Perkins, "Mobile IP Regional Registration", *Internet Draft, draft-ietf-mobileip-reg-tunnel-02.txt*, March 2000.

[4] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," draft-ietf-mobileip-ipv6-24, June 2003.

[5] T. T. Kwon, M. Gerla, S. Das and S. Das, "Mobility Management for VoIP Service: Mobile IP vs. SIP," *IEEE Wireless Communications,* 9(5):66-75, October 2002.

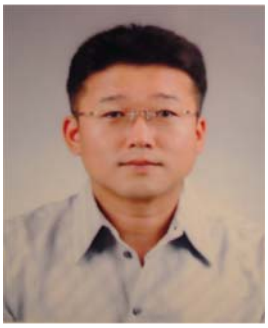
[6] E. Lee, J. Baek, and S. Huang, "A Dynamic Mobility Management Scheme for VoIP Services," *In Proc. of the 3rd International Conference on Information Technology: New Generations*, pp. 340-345, April 2006.

[7] C. Perkins, "IP Mobility Support," *IETF RFC 2002*, 1996.

[8] C. Perkins, "Route Optimization in Mobile IP," *Internet Draft, draft-ietf-mobileip-08.txt*, September 2001.

[9] Stanford University, "Stanford University Mobile Activity Traces," available at http://www-db.standford.edu/sumatra (Access Date: January 2006).

[10] H. Soliman, C. Castelluccia, K. El Malki, and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)," *IETF RFC* 4140, August 2005.



Jinsuk Baek

is Assistant Professor of Computer Science at the Winston-Salem State University (WSSU). He is the director of Network Protocols Group at the WSSU. He received his B.S. and M.S. degrees in Computer Science and Engineering from Hankuk University of Foreign Studies (HUFS) in Yougin, Korea in 1996 and 1998, respectively and his Ph.D. in Computer Science from the University of Houston in 2004. Dr. Baek was a post doctorate research associate of the Distributed Multimedia Research Group at the University of Houston. His research interests include scalable reliable multicast protocols, mobile computing, network security protocols, proxy caching systems, and formal verification of communication protocols. He is a member of the IEEE.

Eunjung Lee

received her B.S. degree in Computer Science and Engineering from Hankuk University of Foreign Studies (HUFS) in Yougin, Korea in 1998 and M.S. degree in Computer Science from the University of Houston in 2005. She served as a software developer at Kinesix Software in Houston, TX for two and a half years. She is currently working at the PSF technologies as a research scientist. Her research interests include mobile computing, image processing, and network security protocols.