A Localized Authentication, Authorization, and Accounting (AAA) Protocol for Mobile Hotspots

Sungmin Baek, Sangheon Pack, Taekyoung Kwon, Yanghee Choi

A Localized Authentication, Authorization, and Accounting (AAA) Protocol for Mobile Hotspots

Sungmin Baek, Sangheon Pack, Taekyoung Kwon, and Yanghee Choi
School of Computer Science and Engineering
Seoul National University, Seoul, Korea
Email: {smbaek, shpack}@mmlab.snu.ac.kr and {tkkwon, yhchoi}@snu.ac.kr

***Abstract*— Mobile hotspots, i.e. Internet access services in moving networks (e.g. vehicular area networks (VAN) and personal area networks (PAN)) bring about new challenging issues. Even if the network mobility (NEMO) basic support protocol has been standardized as a mobility solution by the Internet Engineering Task Force (IETF), to the best of our knowledge, no studies have been conducted in the area of authentication, authorization, and accounting (AAA) protocol, which is a core technology for public mobile hotspots. In this paper, we propose a localized AAA protocol to retain the mobility transparency as the NEMO basic support protocol and to reduce the cost of the AAA procedure. In addition to providing mutual authentication, the proposed AAA protocol prevents various threats such as replay attack, man in the middle attack, and key exposure. Also, we develop an analytical model to evalutate the AAA signaling cost. Numerical results reveal that the proposed AAA protocol is a suitable solution for AAA services in different mobile hotspots.**

I. Introduction

With the advances of wireless access technologies (e.g., 3G, IEEE 802.11/16/20) and mobile communication services, the demand for Internet access in mobile vehicles such as trains, buses, and ships is constantly increasing [1]. In these vehicles, there are multiple devices constituting a vehicular area network (VAN) or personal area network (PAN) that may access to Internet. This kind of services are referred to *mobile hotspots* [2]. Recently, many studies have been conducted for mobile hotspots [3] [4] [5].

In terms of mobility management, the Internet Engineering Task Force (IETF) has established a working group called *NEMO* [6] and the NEMO working group has proposed an extended Mobile IPv6 protocol [7], i.e. the NEMO basic support protocol [8]. Throughout this paper, we assume the NEMO basic support protocol as a framework.

According to the terminologies in [9], a mobile network (MONET) is defined as a network whose point of attachment to the Internet varies as it moves about. A MONET consists of mobile routers (MRs) and mobile network nodes (MNNs). Each MONET has a home network to which its home address belongs. When the MONET is in the home network, the MONET is identified by its home address (HoA). On the other hand, the MONET configures a care-of-address (CoA) on the egress link when the MONET is away from the home network. At the same time, on the ingress link, the MNNs of the MONET configures CoAs, which are derived from the subnet prefix (i.e. mobile network prefix (MNP)). The MNP remains assigned to the MONET while it is away from the home network. The assigned MNP is registered with the home agent (HA) according to the NEMO basic support protocol [8].

The main goal of the NEMO basic support protocol is to preserve established communications between the MONET and correspondent nodes (CNs) during movements. Packets sent by CNs are first addressed to the home network of the MONET. Then, the HA intercepts the packets and tunnels them to the MR's registered address, i.e. the CoA on the egress link. To deliver packets towards the MR's CoA, the NEMO basic support protocol makes a bi-directional tunnel between the HA and the MR. This tunneling mechanism is similar to the solution proposed for host mobility support, i.e. Mobile IPv6 [7] without route optimization.

To make mobile hotspots feasible in public wireless Internet, well-defined authentication, authorization, and accounting (AAA) protocols should be accompanied. However, to the best of our knowledge, no specific AAA protocols have been proposed for mobile hotspots. Even if a number of AAA protocols have been proposed for host mobility, all of them are based on per-node AAA operations. Therefore, they cannot be directly applied to the MONET containing two different types MNNs: *local fixed nodes (LFNs)* and *visiting mobile nodes (VMNs)*. An LFN belongs to the subnet to the MR and is unable to change its point of attachment, while a VMN is temporarily attached to the MR's subnet by obtaining its CoA from the MNP. The VMN's home network may have different administrative policy (e.g. billing) from the current attached MONET. Therefore, a new AAA procedure for VMNs is required.

In this paper, we propose a localized AAA protocol that provides efficient AAA procedures for both LFNs and VMNs in mobile hotspots.

Our main contributions are summarized as follows.

1) The proposed AAA protocol is consistent with the NEMO basic support protocol. In other words, individual AAA operations for LFNs within a MONET are not performed; instead, the MR is authenticated on behalf of the LFNs. Conversely, each VMN attached to the MONET performs its AAA operation in an individual manner.
2) The proposed AAA protocol localizes the AAA procedure using a local AAA key when the MR hands off within the same foreign network. Therefore, the AAA traffic (also, AAA latency) can be reduced significantly.

3) The proposed AAA protocol allows mutual authentication. In addition, it prevents various security attacks, e.g. replay attack, man in the middle attack.
4) From the point of view of internet service providers (ISPs), how to charge a VMN for its network usage is a critical issue. The proposed AAA protocol supports an flexible billing mechanism in which the VMN is informed of a billing agreement between the MR's home network and the new foreign network. Accordingly, the proposed AAA protocol is a suitable solution when the MONET hands off between different networks with different billing or service policies.

The remainder of this paper is organized as follows. In Section II, an existing AAA protocol for Mobile IPv6 is introduced as a reference protocol. Section III describes the proposed AAA protocol for mobile hotspots. In Section IV, security of the AAA protocol is analyzed. In Section V, an analytical model for the AAA signaling cost is developed and numerical results are presented. Section VI finally concludes this paper.

II. AAA Protocol in Mobile IPv6

In this section, the AAA protocol in Mobile IPv6 is described as a reference model. Although several AAA protocols have been proposed in the literature, we adopt the DIAMETER extension for Mobile IPv6 protocol [11], which is the only valid IETF Internet draft as of this writing. The DIAMETER extension for Mobile IPv6 allows a Mobile IPv6 node to access a network of a service provider after the AAA procedures based on the DIAMETER protocol [10] is completed.

This protocol assumes a network architecture for AAA services, as illustrated in Figure 1. The AAAv is an AAA server in the foreign network, while the AAAh is an AAA server in the home network of the mobile node (MN). The AAA client operates in an entity in a foreign network. Hereafter, we assume that the AAA client is located at each access router (AR). The AAA client performs three tasks: (a) allowing the MN to be authenticated, (b) generating accounting data for the MN's network usage, and (c) authorizing the MN to use network resources.

In addition, followings are assumed by [11].

- An MN is identified by its network access identifier (NAI) [12], which is globally unique.
- An MN and its AAAh have a long-term key.
- Communication between the AAAv and AAAh is secure.

The basic information flow of the DIAMETER extension for Mobile IPv6 [11] is shown in Figure 2. When entering a new network or at power up, an MN listens to an AR's router advertisement (RA) message that has a local challenge and a visited network identifier. Then, the MN sends an authentication request (`AReq`) message to the AAA client (i.e. AR) based on the security key shared with its

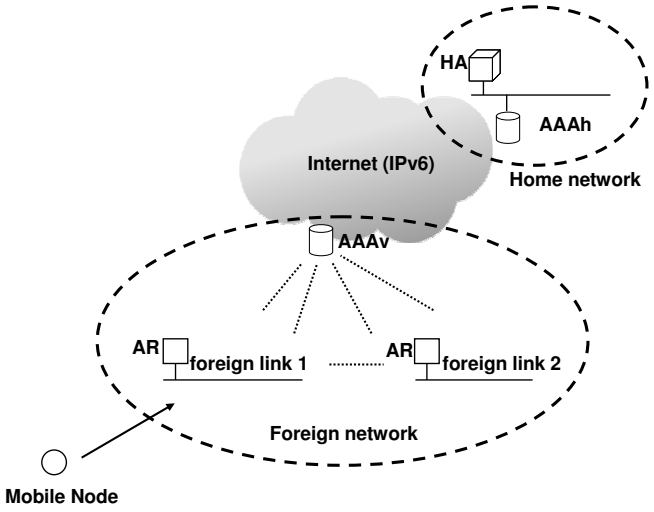

Fig. 1. Mobile IPv6 AAA Architecture

AAAh. When the AAA client receives an `AReq` message, it creates an `AA-Registration-Request Command (ARR)` message and sends it to the AAAv. Then, the AAAv relays it to the AAAh of the MN. When receiving the `ARR` message from the AAAv, the AAAh authenticates the MN by means of the NAI and sends the `Home-Agent-MIPv6-Request Command (HOR)` message to the MN's HA. Upon receipt of the `HOR` message, the HA creates a key to establish a security association (SA) with the MN and replies with the `Home-Agent-MIPv6-Answer Command (HOA)` message to the AAAh. Then, the AAAh constructs the `AA-Registration-Answer Command (ARA)` message that has an authentication result and sends it to the AAAv. When receiving the `ARA` message from the AAAh, the AAAv stores the authentication result locally and then forwards the message to the AAA client. The AAA client converts the `ARA` message into the authentication reply (`ARep`) message in order to inform the MN of the authentication result from the AAAh and deliver the established key (for the SA) to the MN.

III. AAA Protocol for Network Mobility

A. Network Architecture

In this section, the AAA architecture for mobile hotspots is introduced with basic assumptions and concepts such as SA and challenge/response authentication. Figure 3 illustrates the reference AAA architecture in mobile hotspots, which is similar to that of Mobile IPv6. The AAA architecture is based on the DIAMETER protocol [10].

The AAA architecture consists of multiple autonomous wireless networks, each of which is called a *domain*. Each domain has an AAAH server and/or an AAAL server in order to authenticate any node in a DIAMETER-compliant manner. The AAAH server of the MR has the profile of the MR and it shares a long-term key with the MR. Likewise, the AAAH server of the VMN shares a long-term key with the VMN.

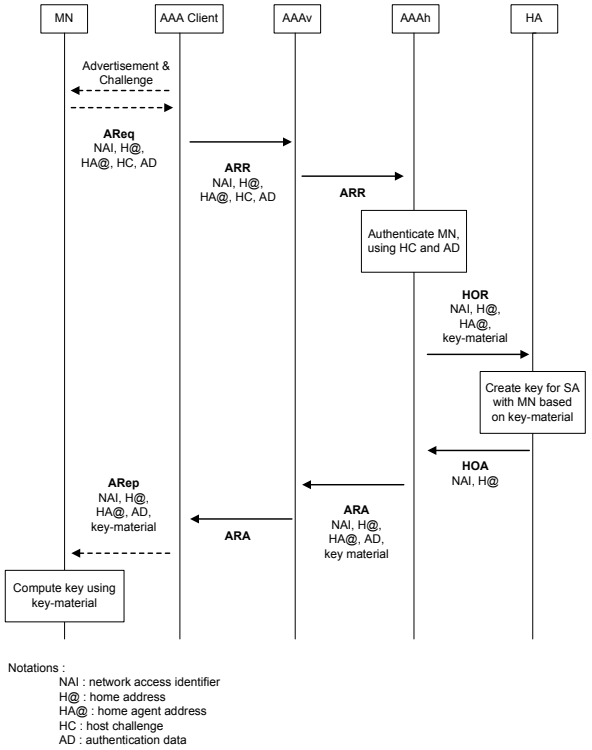

Fig. 2. Information flow in AAA protocol for Mobile IPv6

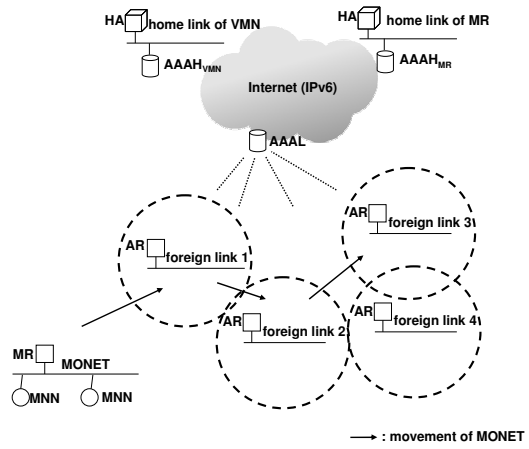

Fig. 3. An AAA Architecture for mobile hotspots

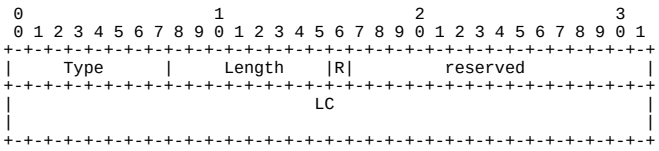

Fig. 4. Attendant advertisement option

The AAAL server takes charge of an AAA procedure for a visiting MONET (i.e. VMNs and MRs). The trust relationship between the MR's AAAH server and the AAAL server in the visited network is maintained through the DIAMETER protocol. When the MONET changes its point of attachment, the MR needs to be authenticated and authorized before it accesses a new domain in the same foreign network (i.e. *intra-domain handoff*) or a new foreign network (i.e. *inter-domain handoff*). To accomplish this, the MR and AR authenticate each other through a mutual authentication procedure that involves both the AAAH server of the MR and the AAAL server of the AR. An attendant (which is the same as a AAA client) is an entity that triggers authentication procedures to the AAA system. In Mobile IPv6 networks, ARs normally act as the attendants for an MN. In our protocol, the AR serves as an attendant for the MR's authentication, whereas the MR serves as an attendant for VMN's authentication. In the latter case, the MR broadcasts attendant advertisement messages and receives authentication request messages from VMNs within the mobile hotspot. In other words, an attendant (an AR or MR) requests the AAAL server to authenticate the mobile hotspot (the MR or VMN). When the AAAL server receives this authentication request, it verifies the identity of the MONET by cooperating with an AAAH server.

In terms of SAs, it is assumed that the MR's AAAH server and the VMN's AAAH server have a pre-established SA. In addition, it is assumed that the MR and LFNs have already authenticated each other by some mechanism, which is out of the scope of this paper.

Notations used throughout this paper are summarized in Table I. A local challenge (*LC*) is a random number for authentication procedures. An MR or VMN encrypts the *LC* using a pre-defined SA with its AAAH server. The encrypted value is called a credential (CR), which is used to authenticate an MR which creates it. MRs and VMNs are identified by their NAIs and a replay protection indicator (RPI) is used to protect from a replay attack. Either a time stamp or a random number can be used as an RPI. The size of the K_{AAA} field is 128 bytes by assuming a public key cryptography algorithm. As we adopt a symmetric key cryptography for dynamic keys (K_{LOCAL} and K_{HOME}, the size of each key is 32 bytes. Note that a dynamic key is used to establish a dynamic SA while a long-term key is to establish a long-term SA. Other notations will be elaborated later.

In our protocol, we define two ICMP messages [18] `Attendant Solicit` and `Attendant Advertisement` messages that are similar to `Router Solicit` and `Router Advertisement` messages, respectively. In those messages, we introduce a new `Attendant Solicit option`, which is used for the authentication of VMNs in case of intra-domain handoff. In addition, several DIAMETER messages, e.g. `AA-Mobile-Router-Request` , `AA-Mobile-Router-Answer`, are defined. Their functions will be described later.

TABLE I

NOTATIONS FOR THE AAA PROTOCOL

Field	Meaning	Typical Length (bytes)
LC	local challenge	8
MC	mobile challenge	8
NAI	identity of MR or VMN	20
RPI	replay protection indicator	4
H@	home address	16
HA@	home agent address	16
Co@	care of address of MR or VMN	16
K_{AAA}	pre-shared SA between an MR and an AAAH server	128 (public key)
K_{AH}	pre-shared SA between an AAAH server and an HA	128 (public key)
K_{AL}	pre-shared SA between an AAAH server and an AAAL server	128 (public key)
CR	credential	8
CR_L	local credential	8
CR_M	mobile credential	8
K_{LOCAL}	dynamic SA between an MR and an AAAL server	32 (symmetric key)
K_{HOME}	dynamic SA between an MR and its AAAH server	32 (symmetric key)
SP_{LOCAL}	security parameters for constructing K_{LOCAL}	12
SP_{HOME}	security parameters for constructing K_{HOME}	12

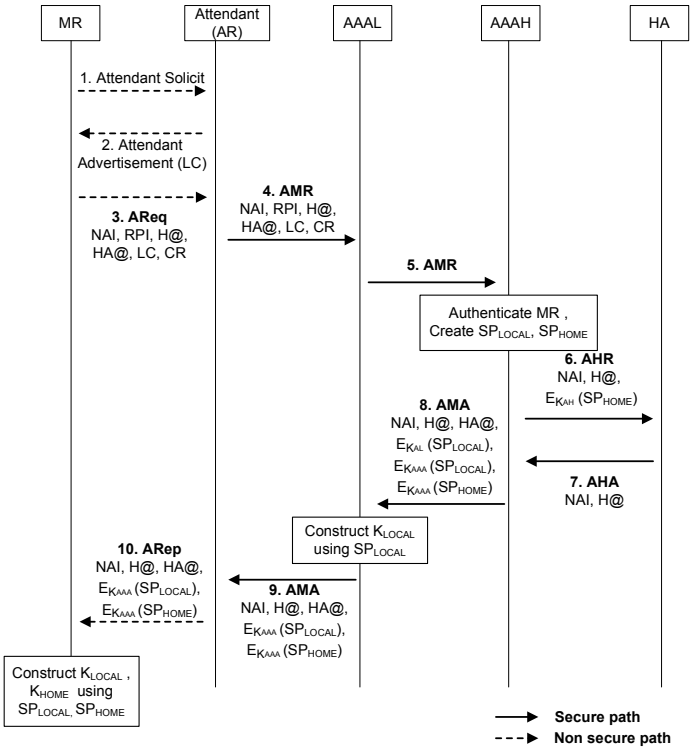

Fig. 5. The AAA procedure of an MR when the inter-domain handoff occurs

B. Mobile Router (MR) Authentication

1) Inter-Domain AAA Procedure: When a MONET enters a new foreign network domain, an inter-domain AAA procedure is initiated. Since the MR does not have any SA with the AAAL server in the foreign network domain, it should be authenticated with its AAAH server located in its home network domain. The message flows for the inter-domain AAA procedure are depicted in Figure 5.

1) The MR sends an `Attendant Solicit` message to the attendant, i.e. AR.

2) As a response to the `Attendant Solicit` message, the AR sends an `Attendant Advertisement` message including an *LC*. Even without the `Attendant Solicit` message, the AR broadcasts `Attendant Advertisement` messages periodically.

3) The MR encrypts the received *LC* value using its long-term SA with the AAAH server and makes a *CR*, which is used for the MR's AAAH server to authenticate the MR. Then, the MR sends an `AReq` message that contains the *LC* and *CR* to the attendant (i.e. AR). The `AReq` message also contains the MR's NAI and RPI, which are used for the AAAL server to identify the MR's home domain and to protect from replay attack.

4) When the attendant (i.e. AR) receives the `AReq` message, the attendant converts it into an `AA-Mobile-Router-Request(AMR)` message. After then, the attendant sends the `AMR` message to the AAAL server in the foreign domain.

5) The AAAL server detects that it cannot authenticate the MR locally by checking the NAI field and hence forwards the `AMR` message to the MR's AAAH server.

   When the AAAH server receives the `AMR` message, it encrypts the *LC* using the pre-established SA and compares the result with the *CR* value. If these two values are identical, the MR is successfully authenticated. Then, the AAAH server generates two dynamic keys: one is a K_{LOCAL} (to be explained later) for intra-domain AAA procedures in the foreign domain and the other is a K_{HOME} for a secure

bi-directional tunnel between the MR and the MR's HA.

To enable the MR to generate K_{LOCAL} and K_{HOME}, the AAAH server also generates SP_{HOME} and SP_{LOCAL} and sends them to the MR. These security parameters are encrypted using the long-term key between the MR and AAAH server to avoid the possibility of exposure to other network entities.

6) The AAAH server informs the HA of the MR's NAI and SP_{HOME} by the `AA-Home-Agent-Request (AHR)` message.

7) The HA constructs K_{HOME} by using SP_{HOME} and replies with an `AA-Home-Agent-Answer (AHA)` message as confirmation.

8) The `AA-Mobile-Router-Answer (AMA)` message is used for the AAAH server to notify the AAAL server of the authentication result. When the AAAL server receives the `AMA` message with authentication approval, the AAAL server decrypts the message using the long-term key (K_{AL}) with the AAAH server, records the MR's NAI, and constructs K_{LOCAL}.

9) The AAAL server re-encrypts the received `AMA` message from the AAAH server after excluding $E_{K_{AL}}(SP_{LOCAL})$ and sends it to the attendant.

10) When receiving the `AMA` message, the attendant learns that the MR is authenticated and grants the MR's network access. In addition, the attendant informs the MR of the result by the `ARep` message containing SP_{HOME}, SP_{LOCAL}, home agent address, etc.
On receipt of the `ARep` message with authentication approval, the MR can access the foreign network. At the same time, the MR generates K_{HOME} and K_{LOCAL} using SP_{HOME} and SP_{LOCAL}, respectively.

2) Intra-Domain AAA Procedure: To support real-time multimedia applications in mobile hotspots, it is important to reduce the latency related to AAA operations. Therefore, when a MONET changes its point of attachment within the same foreign domain, our protocol enables the MR to be authenticated through a localized AAA procedure with the AAAL server in the foreign network without any interaction with its AAAH server. That is, the AAAL server of the foreign network can authenticate the MR using K_{LOCAL}, which was introduced for the inter-domain AAA procedure in the previous section.

Figure 6 illustrates the intra-domain AAA procedure. As a response to the `Attendant Advertisement` message, the MR sends the `AReq` message containing CR_L, which is different from CR used in the inter-domain AAA procedure. At this time, the `AReq` message contains MC for

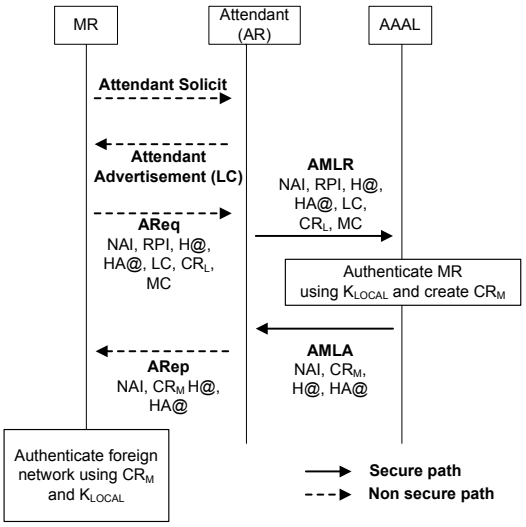

Fig. 6. The AAA procedure of an MR when the inter-domain handoff occurs

mutual authentication. The CR_L is an authentication code generated using K_{LOCAL}. Then, the attendant constructs an `AA-Mobile-Router-Local-Request (AMLR)` DIAMETER message and sends it to the AAAL server. When the AAAL server receives the `AMLR` message, the AAAL server authenticates the MR by using K_{LOCAL}, which has been already stored at the AAAL server during the inter-domain AAA procedures. Moreover, the AAAL server constructs CR_M by encrypting the MC value and informs the attendant of the result via the `AA-Mobile-Router-Local-Answer (AMLA)` message. Then, the attendant will transmit the result (i.e. the `ARep` message) to the MR. The MR receiving the `ARep` message also verifies the CR_M value to authenticate the foreign network.

C. Visiting Mobile Node (VMN) Authentication

A VMN is a visiting MN that accesses the Internet through an MR in mobile hotspot services. According to the NEMO basic support protocol [8], the VMN does not need to know whether its attached router is the AR or the MR. Therefore, the AAA protocol for VMNs should be consistent with this issue. The VMN in a MONET uses the home network prefix of the MR as its IPv6 network prefix. Accordingly, the VMN will deem it to be in the MR's home network. In our AAA protocol, the MR serves as an attendant for VMNs and the MR's AAAH server serves as an AAAL server.

Figure 7 illustrates message flows for the AAA procedure when a VMN is attached to a MONET. As mentioned above, the MR acts as an attendant. Hence, the MR broadcasts `Attendant Advertisement` messages periodically or responds to an `Attendant Solicit` message from the VMN with an `Attendant Advertisement` message. The VMN creates a CR using a pre-shared SA with its AAAH

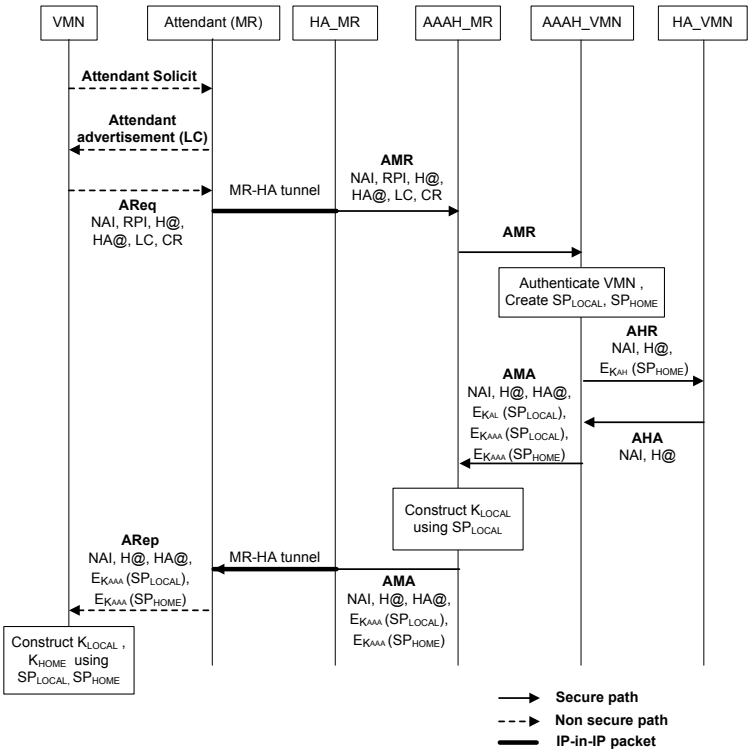

Fig. 7. The AAA porcedure of a VMN

server (i.e $AAAH_{VMN}$) and sends an AReq message to the MR. Then, the MR converts the AReq message into a DIAMETER message, AMR, and sends it to the MR's AAAH server ($AAAH_{MR}$) through a secured bi-directional tunnel. When the $AAAH_{MR}$ receives the AMR message, it sends the AMR message to the $AAAH_{VMN}$ that has a shared SA and requests the AAA procedure for the VMN . Then, the $AAAH_{VMN}$ authenticates the VMN. During this steps, K_{HOME}, K_{LOCAL}, SP_{HOME}, and SP_{LOCAL} are created, similarly to the inter-domain AAA procedure of the MR (see section III-B.1). After completion of AAA procedures, the VMN registers its CoA (configured using the MNP) with its HA.

Only after initial authentication and binding update procedures, VMNs within a MONET do not need to know whether the MONET changes its point of attachment or not. Thus, VMNs do not have to register their locations to their HAs when the MONET hands off. This mobility transparency is the key advantage of the NEMO basic support protocol [8]. However, if the mobility transparency is strictly provided, the AAAL server in the foreign network cannot detect the existence of VMNs. Even if the mobility transparency is beneficial to reduce the binding update traffic, it makes the accounting of VMNs' network usages hard. In our protocol, the AAAL server in the foreign domain accounts the total network usage of the MONET (not individual VMNs) and then this collective accounting information is delivered to the MR's AAAH server. At the same time, the MR's AAAH server maintains the accounting information for the MR as well as individual VMNs[1]. Consequently, the MR's AAAH server can differentiate the accounting information for MRs and VMNs. In addition, we assume that the MR's AAAH server and the VMN's AAAH server have a trust relationship and a shared SA. Therefore, the accounting information collected at the MR's AAAH server is securely transferred to the VMN's AAAH server for suitable billing.

In addition, the mobility transparency causes another problem, i.e. how to authorize VMNs when the MONET moves to a foreign domain with a different billing policy. To solve this problem, an MR sends an `Attendant Advertisement` message with a set R bit when the foreign domain has a different policy and a new AAA procedure is required. Hence, from the `Attendant Advertisement` message, the VMN determines whether it should perform a new AAA procedure or not. In this paper, we assume that each network domain can have different policies, so that the VMN performs a new AAA procedure per inter-domain handoff.

IV. Security Analysis

In this section, we show that the proposed AAA protocol provides mutual authentication. Then, we consider security attacks, e.g. key exposure, replay attack, man in the middle attack.

[1]In the NEMO basic support protocol [8], all packets destined to MNNs are tunneled at the MR's HA, so that the MR's HA can keep track of network usages of individual LFNs and VMNs. We assume that the MR's HA will report this information to the AAAH server.

A. Mutual Authentication

Mutual authentication is a security feature in which a client (i.e. the MR and VMN) must prove its identity to a service (i.e. network), and the service must prove its identity to the client. Therefore, to provide mutual authentication in our protocol, the following requirements should be met.

1) the MR or VMN authenticates the foreign network.
2) the foreign network authenticates the MR or VMN.

Specifically, mutual authentication is achieved as follows.

First, in the case of the inter-domain authentication, mutual authentication is achieved by establishing a session key, K_{LOCAL}. In the other word, the objective of inter-domain authentication protocol is that the MR and the AAAL server believe that they share K_{LOCAL} with each other.

The MR creates CR as

$$CR = E_{K_{AAA}}(LC), \tag{1}$$

where $E_K(\cdot)$ is an encryption function using a key of K.

The AAAH server can verify the MR's identity by comparing with CR sent by the MR and the CR constructed by the AAAH server itself. If two values are equal, the MR is authenticated successfully. Otherwise, the authentication fails. In our protocol, a malicious MR cannot create the correct CR because it does not have K_{AAA}.

After verifying the identity of the MR, the AAAH server transmits $E_{K_{AAA}}(SP_{LOCAL})$ and $E_{K_{AL}}(SP_{LOCAL})$ to the AAAL server through a secure path. When the AAAL server receives, it constructs K_{LOCAL} using $E_{K_{AL}}(SP_{LOCAL})$ and forwards $E_{K_{AAA}}(SP_{LOCAL})$ to the MR. At last, the MR constructs K_{LOCAL} using $E_{K_{AAA}}(SP_{LOCAL})$. After this procedure, the MR and the AAAL server share K_{LOCAL}.

In the case of the intra-domain authentication, the AAAL server in the foreign network verifies the identity of the MR by comparing $E_{K_{LOCAL}}(LC)$ constructed by the AAAL server with CR_L sent by the MR.

On the other hand, to authenticate the foreign network, the MR uses an MC and CR_M. The AAAL server in the foreign network sends CR_M that is created by

$$CR_M = E_{K_{LOCAL}}(MC). \tag{2}$$

Then, the MR can authenticate the AAAL server in the foreign network by verifying that $E_{K_{LOCAL}}(MC)$ is equal to CR_M.

Consequently, a malicious network cannot offer fake services to an MR because it cannot compute CR_M.

B. Key Exposure

K_{AAA} is a pre-shared key between an MR and an AAAH server and K_{LOCAL} and K_{HOME} are created using security parameters (i.e. SP_{LOCAL} and SP_{HOME}). Thus, it is desirable not to leak these keys to the other network entities.

In terms of K_{LOCAL}, the AAAH server encrypts SP_{LOCAL} and sends it to the AAAL server and the MR using K_{AL} and K_{AAA}, respectively. The value encrypted by K_{AL} can be decrypted by the AAAL server, while the other value encrypted by K_{AAA} is decrypted by the MR. Therefore, as K_{AL} and K_{AAA} are not exposed, other entities except the AAAL server and the MR cannot know SP_{LOCAL} and hence cannot construct K_{LOCAL}. As similar to K_{LOCAL}, SP_{HOME} is encrypted using K_{AH} and K_{AAA} and delivered to the HA and MR, respectively. Therefore, K_{HOME} derived from SP_{HOME} is not revealed to other entities except the HA and MR.

C. Replay Attack

Replay attack involves the passive capture of data and its subsequent retransmission to produce an unauthorized effect. A malicious node keeps an `AReq` message and then it can retransmit an old `AReq` message to trick the AAAL server for false authentication. This replay attack can be prevented as follows. LC is created randomly and hence it always changes. Therefore, the malicious node cannot replay the old `AReq` message. When even the same LC can be selected by the attendant by chance, RPI (e.g. time stamp) can prevent the replaying attack.

D. Man in the Middle Attack

A man in the middle attack is that an attacker is able to read, insert, and modify messages between two parties without either party knowing that the link between them has been compromised. In a mobile hotspot scenario, we can imagine an attack that a malicious MR in the middle relays authentication messages and then it intends to use network resource illegally. Figure 8 illustrates the man in the middle attack of a malicious MR in the case of inter-domain authentication. The malicious MR acts as an AR and relays authentication messages between the victim MR and the AR. After the authentication procedures, the malicious MR still can relay all of the traffic between the victim MR and AR. However, the malicious MR cannot use any network resource because it cannot know the K_{LOCAL} and K_{HOME}. Suppose that the object of an authentication protocol is an establishing a fresh session key, the malicious MR cannot compromise the authentication procedure between the MR and the AAAL server.

V. Performance Evaluation

Through the analytical model, we evaluate the AAA cost (C_{AAA}), which is defined the volume of AAA-related messages delivered over the network. Therefore, the unit of C_{AAA} is $bytes * hops$ [13], [14]. Reducing the AAA cost is an important requirement in mobile hotspots where a MONET moves with a high velocity and hence AAA procedures are frequently performed (e.g. train or car). Suppose there are i total handoffs (intra-domain handoffs and inter-domain handoffs) and j inter-domain handoffs for each session. The AAA cost of the MR authentication in the proposed AAA protocol is given by

$$C^{MR}_{AAA}(i,j) = (i-j)\cdot C^{MR}_{intra} + j\cdot C^{MR}_{inter}, \quad i \geq j \tag{3}$$

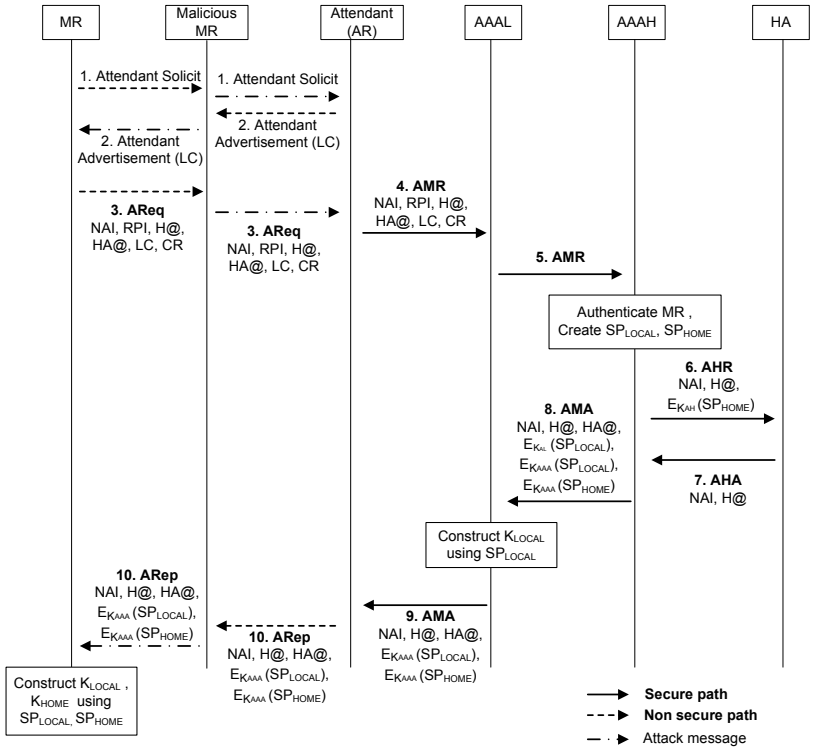

Fig. 8. The scenario of man in the middle attack of the malicious MR

where C_{intra}^{MR} and C_{inter}^{MR} are the costs for intra-domain AAA and inter-domain AAA operations.

The AAA cost of the MR authentication without the localized AAA procedure is given by

$$C_{AAA}^{MR}(i,j) = i \cdot C_{non-local}^{MR}, \tag{4}$$

where $C_{non-local}^{MR}$ is the cost for an AAA operation without the localized AAA procedure.

In this paper, we assume the subnet residence time of the MONET follows a general distribution with a mean of $1/\mu_S$, whose probability density function (PDF) is $f_S(t)$ and its Laplace transform is $f_S^*(t)$. The domain residence time of the MONET follows a general distribution with a mean of $1/\mu_D$, whose PDF is $f_D(t)$ and its Laplace transform is $f_D^*(s)$. When the inter-session arrival time is assumed to be an exponential distribution with a mean of $1/\lambda_I$, the PDFs of i and j are given by [15]

$$\alpha(i) = \begin{cases} 1 - \frac{1}{\rho_S}\left[1 - f_S^*(\lambda_I)\right] & i = 0 \\ \frac{1}{\rho_S}\left[1 - f_S^*(\lambda_I)\right]^2 \left[f_S^*(\lambda_I)\right]^{i-1} & i > 0 \end{cases}$$

$$\beta(j) = \begin{cases} 1 - \frac{1}{\rho_D}\left[1 - f_D^*(\lambda_I)\right] & j = 0 \\ \frac{1}{\rho_D}\left[1 - f_D^*(\lambda_I)\right]^2 \left[f_D^*(\lambda_I)\right]^{j-1} & j > 0 \end{cases}$$

where $\rho_S = \lambda_I/\mu_S$ and $\rho_D = \lambda_I/\mu_D$.

Consequently, the average AAA cost of the MR is given by

$$C_{AAA}^{MR} = \sum_j \sum_i C_{AAA}^{MR}(i,j) \cdot \alpha(i) \cdot \beta(j). \tag{5}$$

In terms of VMN's AAA cost, we consider the AAA cost incurred while the VMN is attached to the MONET. Assume that the VMN's attachment time follows an exponential distribution with a mean of $1/\eta_A$. In addition, let k be the number of inter-domain handoffs during the attachment time. Then, the PDF of k is given by

$$\gamma(k) = \begin{cases} 1 - \frac{1}{\rho_A}\left[1 - f_D^*(\eta_A)\right] & k = 0 \\ \frac{1}{\rho_A}\left[1 - f_D^*(\eta_A)\right]^2 \left[f_D^*(\eta_A)\right]^{k-1} & k > 0 \end{cases}$$

where $\rho_A = \eta_A/\mu_D$.

The AAA cost of the VMN when there are k inter-domain handoffs during the attachment time is given by

$$C_{AAA}^{VMN}(k) = k \cdot C_{AAA}^{VMN}, \tag{6}$$

where C_{AAA}^{VMN} is the cost for each VMN's AAA operation. Then, the average AAA cost of the VMN is expressed as

$$C_{AAA}^{VMN} = \sum_k C_{AAA}^{VMN}(k) \cdot \gamma(k). \tag{7}$$

A. Numerical Results

In this section, we evaluate the effects of mobility and a distance between a foreign network and a home network on the AAA cost (i.e. C_{AAA}^{MR} and C_{AAA}^{VMN}). The numerical results are plotted based on the assumptions introduced in Section V. The parameters and the size of each AAA message are shown in Tables II and III, respectively, based on [10], [17]. The weight for a wireless link is set to 10 [16] and the number of subnets in a domain is set to 49. The distances between an $AAAL$

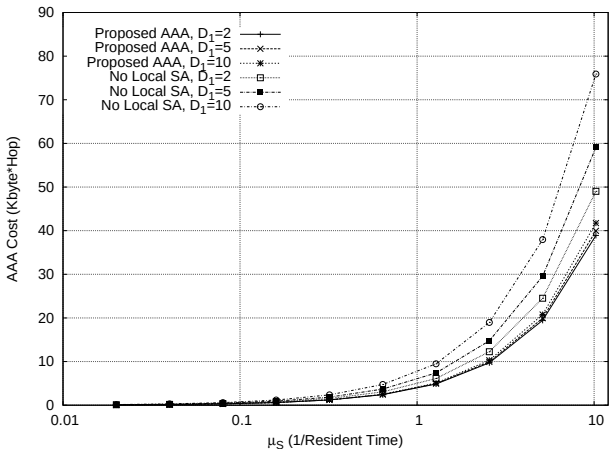

Fig. 9. The AAA cost of an MR

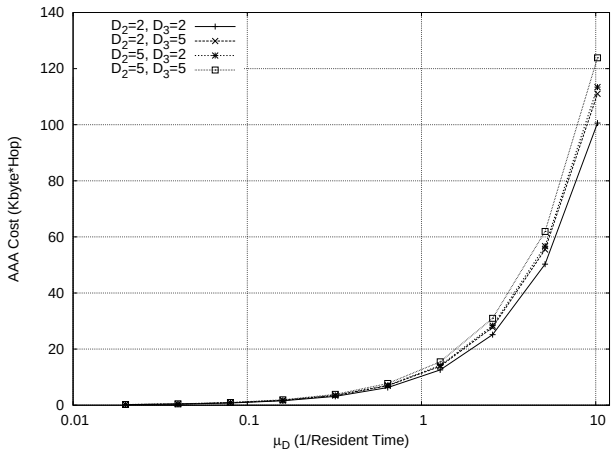

Fig. 10. The AAA cost of a VMN

server and an $AAAH_{MR}$ server, between an MR and its HA, and between an $AAAH_{MR}$ server and an $AAAH_{VMN}$ server are D_1, D_2, and D_3, respectively. λ_I and η_A are normalized to 1.0. By the fluid flow model, μ_D is equal to $\mu_S/\sqrt{N}$ [19].

As shown in Figure 9, C_{AAA}^{MR} increases as μ_S increases (i.e. as the subnet residence time of the MONET decreases). This is because the number of inter- or intra-handoffs is reduced when the mobility (i.e. μ_S) is low. Figure 9 also shows the AAA cost variation for different D_1 (i.e. D_1=2, 5, 10). Since C_{intra}^{MR} and C_{inter}^{MR} are proportional to D_1, C_{AAA}^{MR} increases with increase of D_1. However, in the proposed protocol, the effect of D_1 is not notable. It means that our protocol is effective regardless of the distance between the home network and the foreign network.

On the other hand, if the localized AAA using the K_{LOCAL} is not supported, the MR's AAA cost increases more significantly as μ_S increases. Also, the performance gain becomes more remarkable as μ_S and/or D_1 increase. The effect of D_1 is more clear in the non-localized AAA scheme because an AAA procedure is always performed at the AAAH server in the non-localized AAA scheme. Note that this AAA cost is analyzed for a single MR. As the mobile hotspots services are proliferated, the reduction of the AAA cost (AAA traffic) will be a significant issue.

Figure 10 plots the AAA cost of a VMN, which exhibits a similar trend to Figure 9. Note that the AAA cost when (D_2, D_3) is (5,2) is higher than the AAA cost of (2,5). This is due to IP-in-IP packet tunneling overhead between the MR and its HA. Namely, as D_2, which denotes the distance between the MR and its HA, increases, more tunneling overheads incur and then the AAA cost also increases. As similar to Figure 9, the AAA cost of the VMN is not highly dependent on distance values in our protocol, so that it is concluded that out protocol is less sensitive the distance between the home network and the foreign network.

VI. Conclusion

In this paper, we propose a localized AAA protocol for public mobile hotspots. The proposed AAA protocol is consistent with the NEMO basic support protocol in that the mobility transparency is supported. We analyzed the security concerns in the proposed AAA protocol in terms of mutual authentication, key exposure, replay attack, and man in the middle attack. The central idea behind the proposed AAA protocol is to introduce a shared key between the MR and the AAA server in the foreign network, so that the AAA procedure for the MR in intra-domain handoffs is localized. Performance evaluation results reveal that the localized AAA procedure reduces the AAA traffic significantly in mobile hotspot environment. Furthermore, the localized AAA procedure is less sensitive to the distance between the home network and the foreign network. Although the mobility transparency has the advantage of keeping the VMNs from sending binding update traffic, it causes an accounting problem that the AR cannot know the network usage of VMNs. We suggest that as the MR's HA can keep track of the network usage of individual VMNs, the MR's home network can exchange VMN's accounting information with the AR's network. This way enables a flexible billing mechanism between different domains.

Acknowledgement

This work was supported in part by the Brain Korea 21 project of the Ministry of Education.

References

[1] J. Ott and D. Kutscher, "Drive-thru Internet: IEEE 802.11b for "Automobile" Users," in *Proc. IEEE INFOCOM*, March 2004.
[2] D. Ho and S. Valaee, "Information Raining and Optimal Link-Layer Design for Mobile Hotspots," *IEEE Transactions on Mobile Computing*, to appear, 2005.
[3] OCEAN Project: http://ocean.cse.unsw.edu.au/.
[4] InternetCar Project: http://www.sfc.wide.ad.jp/InternetCAR/.
[5] OverDRIVE Project: http://www.ist-overdrive.org.
[6] IETF Network Mobility (NEMO) Working Group: http://www.ietf.org/html.charters/nemo-charter.html.

TABLE II

PARAMETERS FOR NUMERICAL RESULTS

wireless weight	number of ARs in a domain	λ_I	η_A	D_1	D_2	D_3
10	49	1	1	2, 5, 10	2, 5	2, 5

TABLE III

MESSAGE LENGTHS (BYTES)

Attendant Solicit	Attendant advertisement	AReq	ARep	AMR	AHR	AHA	AMA	AMLR	AMLA
52	84	116	120	172	144	136	166	180	152

[7] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," IETF RFC 3775, June 2003.

[8] R. Wakikawa, A. Petrescu, P. Thubert, "Network Mobility (NEMO) Basic Support Protocol," IETF RFC 3963, January 2005.

[9] T. Ernst and H. Lach, "Network Mobility Support Terminology," Internet draft (work in progress), draft-ietf-nemo-terminology-03.txt, Feburuary 2005.

[10] P. Calhoun, J. Loughney, E. Guttman, G. Zor, J. Arkko,"Diameter Base Protocol," IETF RFC 3588, September 2003.

[11] F. Le, B. Patil, C. Perkins, S. Faccin, "Diameter Mobile IPv6 Application," Internet draft (work in progress), draft-le-aaa-diameter-mobileipv6-04.txt, November 2004.

[12] B. Aboda and M. beadles, "The Network Access Identifier," IETF RFC 2486, January 1999.

[13] S. Lo, G. Lee, W. Chen, and J. Liu, "Architecture for Mobility and QoS Support in All-IP Wireless Networks," *IEEE Journal on Selected Area on Communications (JSAC)*, vol. 22, no. 4, May 2004, pp. 691-705.

[14] A. Stephane and A. Aghvami, "Fast Handover Schemes for Future Wireless IP Networks: A Proposal and Analysis," in *Proc. IEEE 53rd Vehicular Technology Conf. (VTC)*, 2001.

[15] Y. Lin, "Reducing Location Update Cost in a PCS Network," *IEEE/ACM Transactions on Networking*, vol. 5, no. 2, pp. 25-33, February 1997.

[16] J. Xie and I. Akyildiz, "A Distributed Dynamic Regional Location Management Scheme for Mobile IP," *IEEE Transactions on Mobile Computing*, vol. 1, no. 3, July 2002.

[17] T. Narten, E. Nordmark, W. Simpson, "Neighbor Discovery for IP version 6 (IPv6)," IETF RFC 2461, December 1998.

[18] A. Conta, S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)," IETF RFC 2463, December 1998.

[19] X. Zhang, J. G. Castellanos, and A. T. Capbell, "P-MIP: Paging Extensions for Mobile IP," *ACM Mobile Networks and Applications*, vol. 7, no. 2, pp. 127-141, 2002.