International Journal of Internet, Broadcasting and Communication Vol.5 No.2 18-22 (2013)
http://dx.doi.org/10.7236/IJIBC.2013.5.2.18

IJIBC 13-2-5

Proxy-AAA Authentication Scheme with Forwarding Mode Supporting in PMIPv6 Networks

JeongBae Han[1], Jongpil Jeong[2] and Jun Jo[3]

[1]*Department of Information Security, Sungkyunkwan University, Korea*
ssanaii33@naver.com

[2]*College of Information and Communication Engineering, Sungkyunkwan University, Korea*
jpjeong@skku.edu

[3]*School of Information and Communication Technology, Griffith University, Korea*

Abstract

Mobile IPv6 (MIPv6) is a host-based protocol supporting global mobility while Proxy Mobile IPv6 (PMIPv6) is a network-based protocol supporting localized mobility. This paper makes its focus on how to reduce the longer delay and extra cost arising from the combination of authentication, authorization and accounting (AAA) and PMIPv6 further. Firstly, a novel authentication scheme (Proxy-AAA) is proposed, which supports fast handover mode and forwarding mode between different local mobility anchors (LMAs). Secondly, a cost analysis model is established based on Proxy-AAA. From the theoretical analysis, it could be noted that the cost is affected by average arrival rate and residence time.

Keywords: *Proxy-AAA, Forwarding, PMIPv6*

1. Introduction

Because of the characteristic of openness, the security issue of wireless networks is particularly important, especially for the user authentication to access networks. AAA technology is the best scheme so far for solving the delay problem when introducing the authentication process in mobile switching [1]. However, in spite of AAA technology has developed for many years, the research of mobility management is still not very mature yet. With the emergence of new access technologies, as well as the popularity of MIPv6 networks, the remote authentication dial in user service (RADIUS) protocol based on UDP can no longer meet the requirements. Diameter protocol, as an advanced version of RADIUS, has much enhanced ability for failure recovery, security and reliability [2].

But there are still some problems existing in the initial results: the delay brought by authentication and authorization impacts much on the process; AAA application of mobile IP cannot support the fast seamless handover well both in the intra-domain and the inter-domain [3-6]. Besides, another mobility management protocol, the PMIPv6 has also attracted considerable attention. PMIPv6 is an enhancement of MIPv6 and provides a network-based localized mobility management with support for legacy mobile devices. Due to their different characteristics, PMIPv6 can be deployed together with MIPv6. For example, [7] suggests that MIPv6 be used for global mobility and PMIPv6 be used for localized mobility.

Manuscript Received: Jun. 04, 2013 / Revised: Aug. 1, 2013 / Accepted: Aug. 9, 2013
Corresponding Author: ssanaii33@naver.com
Tel: +82-32-471-8264, Fax: +82-32-471-8264,
Dept. of Information and Communications, Sungkyunkwan University, Korea

Based on the shortcomings of above-mentioned schemes, this paper presents a Proxy-AAA authentication scheme. AAA server of the scheme will be deployed on LMA, making up the shortage of simple fast handover authentication and hierarchical authentication, further reducing the cost of intra-domain authentication. And the performance of MIPv6 and Proxy-AAA scheme to select the appropriate protocol to evaluate. Network status and mobility parameters can be selected according to the protocol better. For the proposed Proxy-AAA, signaling overhead is always less than the traditional AAA method. And in case of the MN moves farther away from the home domain, the proposed scheme is more efficient than traditional AAA scheme.

We first describe and compare basic MIPv6 and PMIPv6 in section 2. In section 3, we introduce our proposed Proxy-AAA and protocol selection scheme. In section 4, the performance of traditional AAA scheme and proposed Proxy-AAA scheme is compared. Section 5 concludes the paper with a summary of the key result of the work.

2. Comparison of MIPv6 and PMIPv6

MIPv6 requires a host-based mobility support in the MN and induces high mobility signaling overhead when then MN frequently hands over between subnets. Then PMIPv6 is proposed to cut down the signaling overhead by using network-based mobility management and does not require any host-based mobility stack in the MN. However, PMIPv6 is only able to support mobility within the localized mobility management domain. Fig. 1 shows the architectures of MIPv6 and PMIPv6.

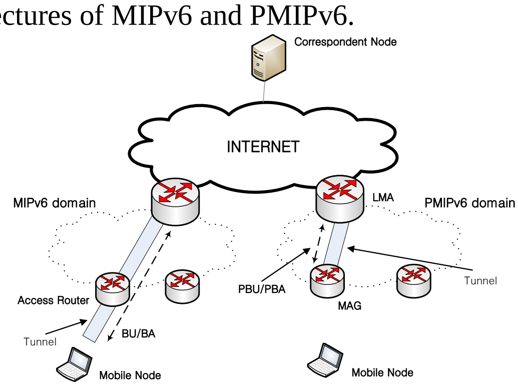

Figure 1. The architectures of MIPv6 and PMIPv6

MIPv6 supports mobility for the MN by providing it with at least two addresses: a Home Address (HoA) which is a fixed address provided by the Home Agent (HA) and a Care-of Address (CoA), which is obtained in the foreign access network and changes when MN moves to a new subnet. Being different from MIPv6, PMIPv6 introduces two important entities, Local Mobility Anchor (LMA) and Mobility Access Gateway (MAG), which manage all mobility-related signaling for the MN. As the MN hands over and changes its point of attachment from one MAG to another, the MN continues to use the same address which was obtained from its first MAG. Therefore, PMIPv6 provides a network-based solution although it can only handle localized mobility of MN within a Local Mobility Domain (LMD). PMIPv6 employs the per-MN-prefix model. A unique Home Network Prefix (HNP) is assigned to each MN and no other MN shares this prefix. The prefix follows the MN while the MN moves within a PMIPv6 domain, so the network layer movement detection and address configuration processes are not required when the MN moves within a PMIPv6 domain except its first attachment in a PMIPv6 domain. Thus the handover latency and signaling overhead can be reduced significantly. Besides, a bi-directional tunnel in PMIPv6 is established between LMA and MAG, not each MN. This is because MN is not involved in any mobility-related signaling. In this way, the location privacy of MN can be guaranteed [8].

3. Proposed Proxy-AAA Scheme

In the process of mobile IP handover, the introduction of authentication will lead to excessive costs. The current solutions cannot meet the requirements in some specific scenes well; therefore, based on this situation, this paper proposes the enhanced AAA authentication scheme based on mobile IPv6. The scheme introduces the thinking of hierarchical AAA, which supports the fast authentication, combining the mobile IP with diameter protocol. AAA server of the scheme will be deployed on LMA, making up the shortage of simple fast handover authentication and hierarchical authentication, further reducing the cost of intra-domain authentication. Proxy-AAA scheme improves the existing authentication schemes and binding updating methods, not only in intra-domain handover and authentication, but also in inter-domain process.

In the process of intra-domain handover and authentication, Proxy-AAA will re-use the session key based on LMA in the HMIPv6. In the inter-domain handover and authentication process, Proxy-AAA adopts the strategy of re-using session key on the AAA server, and also introduces the direct transmission strategy between the LMAs. The adjacent LMAs can communicate the information directly, rather than through the HA, thus further reducing the control overhead of the overall system, as shown in Fig. 2.

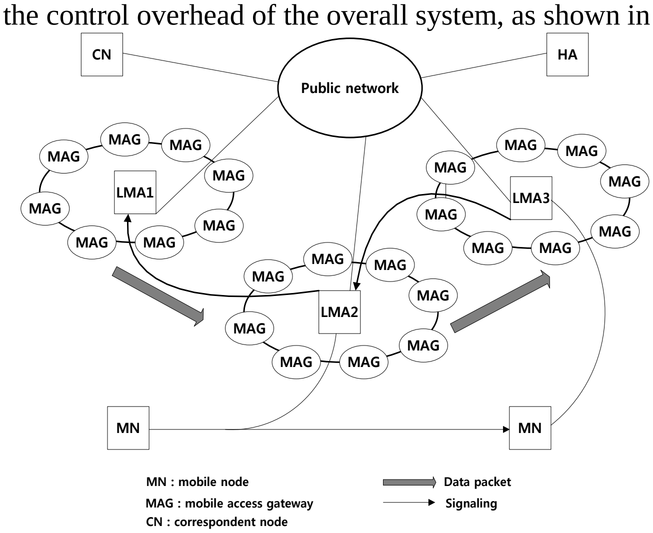

Figure 2. Forwarding scheme between different LMA

When MN moves into a network region from the left to the right, it passes by LMA1, LMA2 and finally to LMA3. When MN reaches the region of LMA2, it will send BU message to LMA2, and LMA2 will return it to LMA1. After receiving the message, LMA1 will compare the message with the LMA list and inquire the relevant information of this MN, updating the current LMA address of MN. Then, LMA1 relays the packet data to LMA2 directly rather than by HA.

4. Performance Evaluation

In this scheme, we deploy AAA server in visit domain (AAAV) on the LMA in its management region, and the AAA server will be responsible for all MAG's accounting, authentication and authorization in the LMA region of LMA. In Proxy-AAA scheme, the overhead of whole system is constituted by two parts: signaling control overhead C_{signal} and data transmission overhead C_{packet}. The signaling control overhead mainly includes authentication signaling control overhead C_{auth} and registration signaling control overhead C_{reg}. C_{reg} is mainly made of by the data transmission overhead from CN to MN ($C_{CN\text{-}MN}$). The specific Proxy-AAA network topology of system overhead analysis is shown in Fig. 3.

In view of the Proxy-AAA proposal aiming at reducing the signaling overhead brought by authentication and registration; therefore, this section will focus on comparison between Proxy-AAA scheme and the traditional AAA schemes. Note that, the traditional AAA is defined as a simple combination of AAA and HMIPv6. The relevant parameters and definition descriptions are given as Table 1.

Table 1. Parameter Definition

Parameter	Definition
$C_{MN\text{-}MAG}$	Signaling tramsmission cose between MN and MAG
$C_{MAG\text{-}LMA}$	Signaling tramsmission cose between MAG and LMA
$C_{HA\text{-}LMA}$	Signaling tramsmission cose between HA and LMA
$C_{LMA\text{-}LMA}$	Signaling tramsmission cose between LMA and LMA
$C_{AAAV\text{-}AAAH}$	Signaling tramsmission cose between AAAv and AAAh
P_{MAG}	Signaling processing cost of MAG
P_{HA}	Signaling processing cost of HA
P_{LMA}	Signaling processing cost of LMA
P_{AAA}	Signaling processing cost of AAA

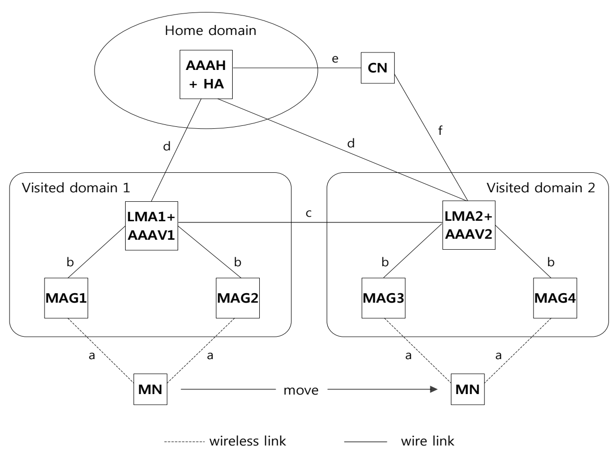

Figure 3. Cost analysis model of Proxy-AAA

Assuming that R is for the signaling overhead ratio of Proxy-AAA and traditional AAA schemes, then R can be expressed as $R = C_{signal\text{-}proposed} / C_{signal\text{-}traditional}$. By analyzing the signaling overhead calculation formula in the above LMA region, the average overhead for signaling is presented by $C_{signal\text{-}a} = C_{signal\text{-}proposed} / T_a$, in which T_a denotes the average residence time in this LMA region. It should be noted that in the actual network environment, the value must be smaller than 0.3.

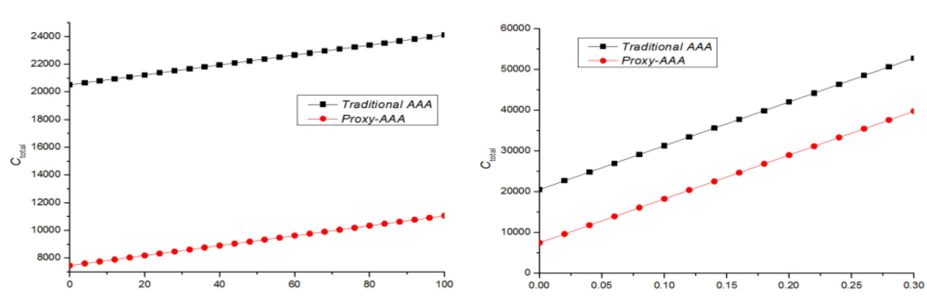

Figure 4. Total overhead (β = 0.01, λ = 1, left) and (p = 30, λ = 1, right)

Fig. 4 (left) shows analysis of the entire overhead based on PMR p increases. When pedestrian (β = 0.01) moves, we can see that as the value of p increases, entire overhead C_{total} increases. Fig. 4 (right) shows analysis of the entire overhead based on β increases. When PMR fixed, we can see that as the value of β increases, entire overhead C_{total} increases.

5. Conclusions

This paper presents a Proxy-AAA authentication scheme, which is not only suitable for the micro-mobility of MN in the LMA region, but also applies to the macro-mobility. This method has established the safety handover at the same time of improving the authentication efficiency, and reduces the signaling overhead caused by authentication. Especially when the mobility happens between the LMA domains, Proxy-AAA scheme efficiently makes up the shortage using traditional schemes which simply combines the current HMIPv6 with AAA authentication technology.

References

[1] C. de Laat, G. Gross, L. Gommans, L. Gommans, D. Spence, "Generic AAA Architecture," RFC 2903, August 2000.
[2] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, "Diameter Base Protocol," RFC 3588, September 2003.
[3] Le F, Patil B, Perkins C, et al, "Diameter mobile IPv6 application," Internet IETF Draft, 2004.
[4] Lee S Y, Huh E N, Kim S B, et al, "An efficient performance enhancement scheme for fast mobility service in MIPv6," Proceedings of the International Conference on Computational Science and its Applications (ICCSA'05), pp. 628-637, May 2005.
[5] Kim M, Kim M, Mun Y, "A hierarchical authentication scheme for MIPv6 node with local movement property," Proceedings of the International Conference on Computational Science and its Applications (ICCSA'05), pp. 550-558, May 2005.
[6] Song Mei, Wang Li, Song Jun-de, "A secure fast handover scheme based on AAA protocol in mobile IPv6 networks," The Journal of China Universities of Posts and Telecommunications, 15 (Sup1): pp. 14-18, 2008.
[7] G. Giaretta, "Interactions between PMIPv6 and MIPv6: scenarios and related issues," draft-ietf-netlmm-mip-interactions-04, June 2009.
[8] J. -F. Guan, et al, "Implementation and analysis of proxy MIPv6," Published Online, WCM, September 2009.