EAI Endorsed Transactions
on Mobile Communications and Applications
Research Article EAI.EU

Design and Performance Analysis of Sensor Proxy-AAA Authentication Scheme Based on Fast Handover and Forwarding Mode for IP-based Internet of Things

Chulhee Cho[1], Byung-Hun Song[2], Jongpil Jeong[3], Tai-Myoung Chung[1,*]

[1]College of Information and Communications Engineering, Sungkyunkwan University, Suwon, Kyunggi-do, 440-745, Republic of Korea

[2]IoT Convergence Research Center, Korea Electronics Technology Institute (KETI), Seongnam, Republic of Korea

[3]Department of Human ICT Convergence, Sungkyunkwan University, Suwon, Kyunggi-do 440-745, Republic of Korea

Abstract

Recently interest in Internet of Things(IoT) is increasing, and a variety of the security technologies that are suitable for Internet of Things has being studied. In order to maintain the trustworthy connectivity and the accessibility of distributed IoT, it is important to establish secure links for end-to-end communication with proper authentication. AAA technology is currently the best way of resolving delay issue when introducing authentication process of mobile switching. However, there are still a number of issues among which the delay time issue from authentication and authorization greatly influences the process. AAA application in mobile IP environment cannot fluently support continuous and fast handover in both intra-domain and inter-domain. Mobile IPv6 (MIPv6) is a host-based protocol supporting global mobility. On the other hand, Proxy Mobile IPv6 (PMIPv6) is a network-based protocol supporting localized mobility. This paper, the additional cost from combination of PMIPv6, authentication, authorization and accounting (AAA) and the way of reducing extended delay time will be explained. First, a new authentication scheme (Proxy-AAA) is proposed that supports forwarding mode and fast handover mode between other local mobility anchors (LMAs). Second, configur cost analysis model based on Proxy-AAA. Based on theoretical analysis, it was confirme that the cost is affected by average arrival rate and residence time.

Received on 26 November 2016; accepted on 13 July 2017; published on 13 September 2017

Keywords: Proxy-AAA, Forwarding, inter-domain handover, re-using the session key

doi:10.4108/eai.13-9-2017.153338

1. Introduction

Recently interest in Internet of Things(IoT) is increasing, and a variety of the security technologies that are suitable for Internet of Things has being studied. Especially sensor network area of the device is an increased using and diversifie for a low specification devices because of characteristic of the Internet of Things. Many entities sensor nodes may move around in a real world environment, thus making the IoT devices attached to them mobile. In order to maintain the trustworthy connectivity and the accessibility of distributed IoT, it is important to establish secure links for end-to-end communication with proper authentication. In the internet of things environment, due to the open characteristic of internet of things, the security issue related

★This article is a revised and expanded version of a paper entitled "Design and Performance Analysis of Sensor Proxy-AAA Authentication Scheme Based on Fast Handover and Forwarding Mode for IP-based Internet of Things", presented at 12th EAI International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, JULY 7-8, 2016 | SEOUL, SOUTH KOREA.

*Corresponding author: Tai-Myoung Chung, Ph.D., research fie d: distributed computing. Email: tmchung@ece.skku.ac.kr

to authentication of user accessing wireless network is extremely important. AAA technology is currently the best way of resolving delay issue when introducing authentication process of mobile switching [1, 2]. However, despite long development of AAA technology, the mobility management in wireless network environment has yet to be researched further. With the distribution of MIPv6 network and development of new access technologies, the UDP-based Remote Authentication Dial-In User Service (RADIUS) protocol can no longer satisfy requirements. Diameter protocol, an improved version from RADIUS, provides extremely improved functions in failure recovery, security and reliability [3]. However, the delay from authentication and authorization process greatly influences the process and AAA application in mobile IP has a number of issues such as failing to support continuous and fast handover in both intra-domain and inter-domain [4–7]. Moreover, another mobility management protocol called PMIPv6 is in the limelight. PMIPv6 is an enhancement of MIPv6 and provides a network-based localized mobility management with support for legacy mobile devices [8]. Due to its different characteristics from MIPv6, PMIPv6 can be introduced along with MIPv6. For example, MIPv6 can be used for global mobility while PIMPv6 can be used in intra-domain mobility [9]. To address the shortcomings of the above mentioned schemes, this paper presents a Proxy-Authentication Authorization Accounting (Proxy-AAA) authentication scheme. In this proposed technique, the AAA server will be implemented on Local Mobility Anchor (LCA) to implement fast handover authentication and hierarchical authentication as well as reduce intra-domain authentication cost [10, 11]. The performance of Mobile IPv6 (MIPv6) and Proxy-AAA scheme to select the appropriate protocol was evaluated. Network status and mobility parameters can be better selected according to the protocol. For the proposed Proxy-AAA, signaling overhead is always less than with the traditional AAA method. Also, in cases where the Mobile Node (MN) moves farther away from the home domain, the proposed scheme is more efficient than the traditional AAA scheme [12, 13]. We first describe and compare basic MIPv6 and PMIPv6 and describe 6LoWPAN network in section 2. In section 3, we introduce our proposed Proxy-AAA and protocol selection scheme. In section 4, the performance of the traditional AAA scheme and proposed Proxy-AAA scheme is compared. Section 5 concludes the paper with a summary of the key results of this work.

2. Related Work

2.1. Comparison of MIPv6 and PMIPv6

MIPv6 supports host-based mobility to MN and reduces high mobility signaling overhead while MN implements frequent handover between subnets [14, 15]. PMIPv6 was proposed to reduce signaling overhead using network-based mobility management without the need of host-based mobility stack at MN. However, PMIPv6 only supports intra-domain mobility and cannot support global mobility between domains. Figure 1 shows the architectures of MIPv6 and PMIPv6 [16]. MIPv6 supports mobility for the MN by providing it with at least two addresses: A fixed address called Home Address (HoA) is provided to Home Agent (HA). Care-of Address (CoA) is gained from foreign access network and is changed when MN moves to a new subnet. Unlike MIPv6, PMIPv6 introduces two major elements including Local Mobility Anchor (LMA) that manages mobility-related signaling of MN and Mobility Access Gateway (MAG). When MN hands over and changes the access point from current MAG to another MAG, the MN can use the same address it gained from the previous MAG. Therefore, PMIPv6 provides the network-based solution for processing MN's localized mobility within Local Mobility Domain (LMD). PMIPv6 employs the per-MN-prefix model. Home Network Prefix (HMP), the unique code allocated to each MN, is not shared with other MNs. When MN moves within the PMIPv6 domain, the prefix follows MN and when MN moves within PMIPv6 domain except the first access of MN in PMIPv6 domain, it does not require network layer movement detection or address configuration processes. Thus the handover latency and signaling overhead can be reduced significantly. Also, because MN does not get involved in mobility-related signaling in PMIPv6 environment, the two-way tunnel is generated between LMA and MAG instead of with MN. As a result, this can assure the location privacy of MN [17].

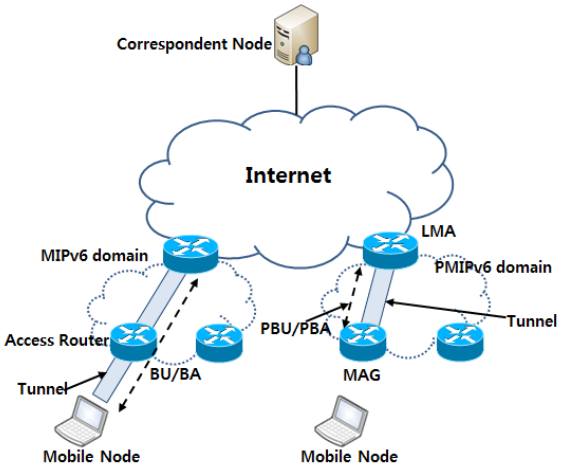

Figure 1. The architectures of MIPv6 and PMIPv6.

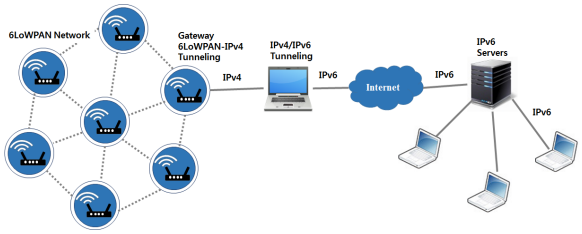

Figure 2. 6LoWPAN Network.

2.2. 6loWPAN

The Internet Engineering Task Force (IETF) define IPv6 Low-power Personal Area Networks (6LoWPAN) which is an IPv6-based LoWPAN on the basis of IEEE 802.15.4 for communications with the Internet. 6LoWPAN (IPv6-based Low-power Wireless Personal Area Networks) is a IP sensor networking technology to implement a low power and low cost, therefore, It is a technology for a wireless environment for IP-based applications. Conventional sensor network technology is less compatible with IP Networks. On the other hand, 6LoWPAN (IPv6-based Low-power Wireless Personal Area Networks) which is one of the IP-USN technology has an advantage that may be directly linked with the Internet infrastructure of the existing IPv4, IPv6, WiBro, WiFi, etc. With its vast address space, 6LoWPAN allows global connectivity between a large number of IPv6 intelligent devices over large areas. The protocol also enables the nodes to be self-organized i.e. can do self-detection, self-healing, and self-configuring without human intervention [18]. Figure 2 shows the architectures of 6LoWPAN Network.

3. Proposed Scheme

3.1. Operation procedures of sensor Proxy-AAA

The adaptation of authentication in mobile IP handover process can lead to excessive cost. Current solutions cannot sufficiently meet these requirements. To deal with these issues, this study proposes an advanced AAA authentication scheme based on mobile IPv6. This proposed technique supports quick authentication and introduces the concept of hierarchical AAA to mobile IP combined with diameter protocol. In this proposed technique, AAA server will be implemented on Local Mobility Anchor (LMA) to implement simple and fast handover authentication and hierarchical authentication as well as reduce intra-domain authentication cost. Proxy-AAA technique improves the previous authentication schemes and binding updating methods in intra-domain handover and authentication as well as inter-domain process [19]. In the process of intra-domain handover and authentication, Proxy-AAA will reuse the session key based on LMA on HMIPv6. The proposed Proxy-AAA

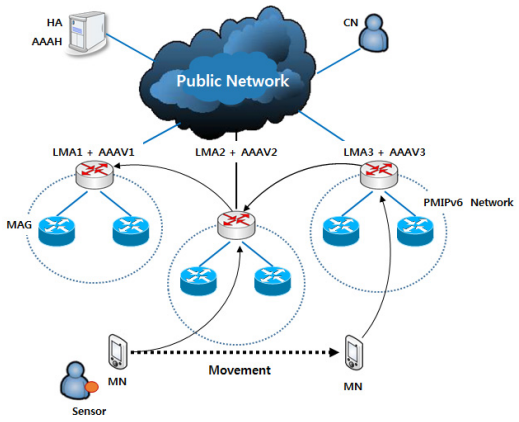

Figure 3. Forwarding scheme between different LMA.

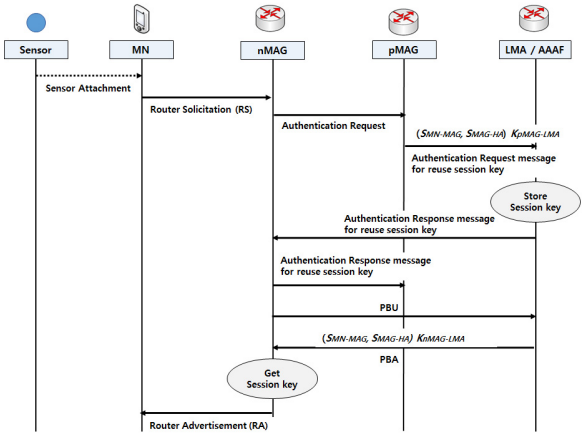

Figure 4. Intra-domain handover flow.

scheme adapts direct transmission strategy between LMAs in inter-domain handover and authentication process, and chooses the strategy for reusing session key on AAA server [20]. As shown in Figure 3, because information can be directly delivered between LMAs in close vicinity , the control overhead of overall system can be saved compared to communication via HA.

When an MN moves into a network region, from the left to the right in the figure it passes by LMA1, LMA2 and finally reaches LMA3. When an MN reaches LMA2, it immediately sends a BU message to LMA2. This will make LMA2 respond to LMA1. Upon receipt of the message, LMA1 compares the message with ones in the list of LMA, makes a request for information on the MN, and updates the current LMA address of the MN. This will be followed by a direct transmission of packet data, from LMA1 to LMA2, without leveraging HA failover.

Figure 4 shows the specifi flow process of intra-domain handover. Let's assume that data generated from sensor node within network is being collected by adding the fixe data collection function called Resource Directory at MN. Also, because sensor node

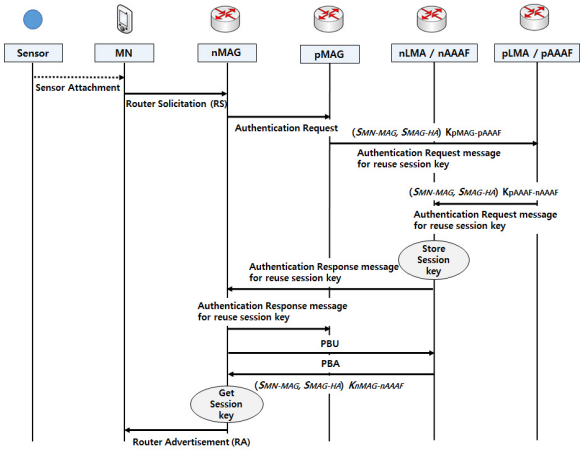

Figure 5. Inter-domain handover flow.

registers node name, type and lifetime in RD, this RD can have the information of all nodes. MN delivers the collected data to information demander via internet working. On receiving notification from MN, nMAG sends authentication request message to pMAG to reuse the session key [21]. On receiving the request message, the mPAG encrypts session keys S_{MN-MAG} and S_{MAG-HA} using $K_{pMAG-LMA}$ and then delivers it to the LMA. LMA saves the received session key and returns the response message on reusing session key to nMAG. nMAG delivers the received response message to pMAG and sends PBU message to LMA. On receiving PBU message, LMA delivers PBA including the encrypted value of session keys S_{MN-MAG} and S_{MAG-HA} using $K_{nMAG-LMA}$ to nMAG. nMAG delivers the encrypted session key to MN. Here, a reliable binding update channel between MN and LMA is formed. In addition, Figure 5 gives the specifi message flow in inter-domain handover.

3.2. Protocol selection

To select the most appropriate mobility management protocol, the mobility management protocol provided by network and MN's mobility management protocol environment need to be taken into consideration. In the authentication process, MAG searches MN's profil for MN's preference. From the search, in case MN's preferred protocol matches what was provided from access network, the matching protocol will be selected [22]. Otherwise, the MN's preference has higher priority. In case MN does not have a preference, the network is responsible to assess the performance of basic MIPv6 and Proxy-AAA technique and select the appropriate protocol. To evaluate the performance of basic MIPv6 and the Proxy-AAA scheme, the related path latency is probed by MAG. While searching for path, MAG sends two types of proving messages to LMA several times. One is sent through nLMA and then redirected to pLMA and the related round-trip time (RTT) is denoted as $RTT_{proxy-AAA}$. The other probing message is sent directly to pLMA and the related RTT is denoted as RTT_{mip}. The average RTT of the MIPv6 path (z_n) after path probing for times can be calculated as

$$\overline{z_n} = \alpha RTT_{mip}(n) + (1-\alpha)\overline{z_{n-1}} \quad (1)$$

Where α reflect the significanc of past events in the calculation of the weighted average. For example, we set α to 0.8 in this paper, and then the most recent value z_{n-1} will contribute to the calculated z_n value with 20% weighting. This will avoid hysteresis if the value of α is carefully selected [23]. The variable z is initialized with the following value:

$$\overline{z_0} = RTT_{mip}(0) \quad (2)$$

In a similar manner, the average RTT for the Proxy-AAA scheme can be calculated and denoted as t_n. When path latency of MIPv6 hands over to much smaller and lower frequency than path latency and MN of Proxy-AAA technique, the performance of MIPv6 will be improved. On the other hand, in case the latency of MIPv6 is not much smaller than the latency of Proxy-AAA technique and hands over at higher frequency of MN, the performance of proposed Proxy-AAA technique will be improved. In appropriately selecting the better protocol according to network condition and mobility parameters, protocol selection can be used.

$$\begin{aligned} \frac{\overline{t_n} - \overline{z_n}}{N_h} &< H_t, \quad \text{select Proxy-AAA scheme} \\ \frac{\overline{t_n} - \overline{z_n}}{N_h} &\geq H_t, \quad \text{select Basic MIPv6} \end{aligned} \quad (3)$$

Here, N_h is the handover frequency and the value of $\overline{t_n} - \overline{z_n}/N_h$ is used as the quality indicator to judge which protocol can provide better performance, and H_t is the quality threshold to determine which protocol shoul d be selected.

4. Performance Evaluation

4.1. System Modeling

In this scheme, we construct an AAA server on the LMA residing in the visit domain (AAAV), and the AAA server is wholly responsible for accounting, authentication, and authorization of the MAG in the LMA domain of LMA. In the proxy-AAA method, the overhead of the entire system is composed of two parts: signaling control overhead C_{signal} and

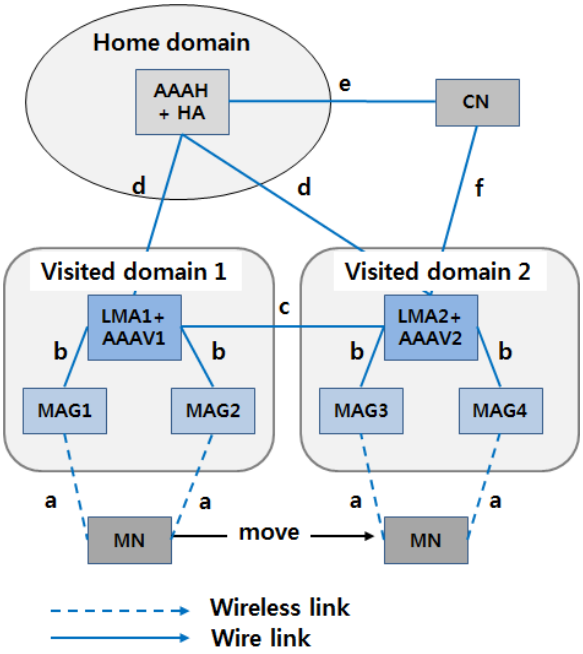

Figure 6. Cost analysis model of Proxy-AAA.

data transmission overhead C_{packet}. Signal control overhead is composed of authentication signaling control overhead C_{auth} and registration signaling control overhead C_{reg} in general, and C_{reg} is mainly made of the data transmission overhead from CN to MN(C_{CN-MN}).

Figure 6 shows the network topology of a specifi Proxy-AAA for a system overhead analysis. As shown in Figure 6, the proposed hospital contains three floors, each with two wards. The hospital is considered as a one SPMIPv6 domain, in which sensor nodes are deployed on the patient body as well as over the environment, ARs are used to control wards. Patients can get real-time care while moving between rooms, wards, and floors, or when the patient moves to another branch of the hospital.

$$C_{total} = C_{signal} + C_{packet} = \beta\left(C_{reg} + C_{auth}\right) + \alpha C_{CN-MN} \quad (4)$$

Here, α refers to the average velocity of packet data, transmitted from the CN to the MN (the average arrival rate of packet data), and β is the average switching rate of an MN when it transfers from a subnet to another, which is referred to as MN's switching rate per unit time [24]. When it is assumed that the number of packets transmitted from an MN to a CN remains constant, we can express the packet to mobility ratio (PMR) of the packets received by the MN as $p = \alpha/\beta$. Also, $p = \alpha/\beta$ refers to the average number of packets received by a peer CN. PMR is the ratio of packet arrival rate and mobility rate, and it is a crucial indicator for the present study. The larger PMR is, the larger the arrival rate is than the mobility rate, meaning that the data transmission cost becomes larger. When PMR becomes smaller, the arrival rate becomes smaller than the mobility rate, meaning the binding update cost becomes larger. Also, the average length of data packets is referred to as l_d, and signaling packets as l_s. The ratio of these is supposed to be $l = l_d/l_s$. For the convenience of calculation, $l_d = 1024\,B$ and $l_s = 100\,B$ are set by leveraging parameters offered by [25]. The overhead of transmitting signaling packets is associated with the distance between entities, while the overhead required for a data packet transmission should be l times of that for a signaling packet transmission.

$$C_{total} = \beta\left(C_{reg} + C_{auth}\right) + \alpha l_d L_{CN-MN} = \beta l_s\left(L_{reg} + L_{auth}\right) + \alpha l_d L_{CN-MN} \quad (5)$$

The present study adopts Ethernet LAN of 10Mbit/s for the wired network environment and single-hop WLAN of 2Mbit/s for the wireless environment. For the calculation of time delays in wired and wireless links, we use an empirical formula respectively expressed by $T_{rt}(h,k)$ and $W_{rt}(k)$:

$$T_{rt}(h,k) = 3.63k + 3.21(h-1),\ W_{rt}(k) = 17.1k \quad (6)$$

Where k is for the packet length, with the unit KB (kilobytes), and h is for the routing hops. The following section will provide some assumptions. η represents the cost of signaling packets in wired transmission per unit distance. The cost in wireless transmission is 10η. In addition, σ represents the cost of data packets in wired transmission per unit distance. The cost in wireless transmission is 5σ.

$$C_{packet} = \alpha C_{CN-MN} = \alpha l_d\left[\sigma\left(l_{CN-HA} + l_{HA-LMA} + l_{LMA-MAG}\right) + 5\sigma l_{MAG-MN}\right] \quad (7)$$

MN's mobility is described by the simple equality fluid model. It is assumed that the area covered by the LMA is a $150\,m \times 150\,m$ square. When the pedestrian walks at a speed of 3 miles/hour (mph), $\beta = 0.01$; when the vehicle travels at a speed of 60 mph, $\beta = 0.2$. Then,

$$C_{packet} = \beta p l_d \left[\sigma \left(l_{CN-HA} + l_{HA-LMA} + l_{LMA-MAG} \right) + 5\sigma l_{MAG-MN} \right] \quad (8)$$

As the suggested Proxy-AAA scheme aims to reduce the signaling overhead generated in authentication and registration processes, this section compares Proxy-AAA with traditional AAA schemes. Note that the traditional AAA is defined as a simple combination of HMIPv6 and AAA. The relevant parameters and definitions are shown in Table 1.

Table 1. The parameter Definition.

Parameter	Definition
C_{MN-MAG}	Signaling transmission cost between MN and MAG
$C_{MAG-LMA}$	Signaling transmission cost between MAG and LMA
C_{HA-LMA}	Signaling transmission cost between HA and LMA
$C_{LMA-LMA}$	Signaling transmission cost between LMA and LMA
$C_{AAAV-AAAH}$	Signaling transmission cost 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

Assuming that MN moves out of the LMA region m times in a certain period of time, then the authentication will be performed m times. The earlier $m-1$ authentications are intra-domain authentications, and the last one is for inter-domain authentication. Suppose that the authentication process as a result of MN's movement is in line with Poisson distribution with λ, then

$$p(n) = \int_{t=0}^{\infty} p(n,t) f(t)\, dt = \int_{t=0}^{\infty} \frac{(\lambda t)^n}{n!} e^{-\lambda t} f(t)\, dt = (-1)^n \frac{\lambda^n}{n!} \frac{d^n F(s)}{ds^n}\bigg|_{s=\lambda} \quad (9)$$

Assuming that the time for which MN is in the region of LMA accords with Gamma distribution, and the expectation and variance of density function $f(t)$ can be expressed as $1/\mu$ and v, the Laplace transform can be expressed as

$$F(s) = (1 + \mu v s)^{-1/\mu^2 v} \quad (10)$$

$$\frac{d^n F(s)}{ds^n} = (-\mu v)^n \left[\prod_{j=0}^{n-1} \left(\frac{1}{\mu^2 v} + j \right) \right] (1 + \mu v s)^{-\left(\frac{1}{\mu^2 v} + n\right)} \quad (11)$$

However, $f(t)$ can vary depending on the exponential distribution, if $\mu^2 v = 1$. In that case, the expected authentication time (m) can be expressed as follows.

$$E(m) = \sum_{n=1}^{\infty} nP(n) = \sum_{n=1}^{\infty} n \frac{\mu \lambda^n}{(\lambda + \mu)^{n+1}} = \frac{\lambda}{\mu} \quad (12)$$

Through cost model analyses based upon HMIPv6, the inter-domain and intra-domain signaling overhead for a binding update under PMIPv6 can be expressed as follows.

$$BU_{intra}^{PMIPv6} = 2C_{MN-MAG} + 2C_{MAG-LMA} + 2P_{MAG} + P_{LMA} \quad (13)$$

$$BU_{inter}^{PMIPv6} = 2C_{MN-MAG} + 2C_{MAG-LMA} + 2C_{LMA-HA} + 2P_{MAG} + 2P_{LMA} + P_{HA} \quad (14)$$

In addition, the authentication delay under traditional AAA methods can be expressed as follows.

$$A^{traditional} = 2C_{MN-MAG} + 2C_{MAG-LMA} + 2C_{LMA-AAA} + 2C_{AAAV-AAAH} + 2C_{LMA-HA} + P_{AAA} + 2P_{MAG} + 4P_{LMA} + P_{HA} \quad (15)$$

Through this analysis, the entire signaling overhead in the LMA region under the traditional AAA scheme can be expressed as follows.

$$C_{signal-traditional} = BU_{total} + A^{traditional} E(m) = BU_{intra}^{PMIPv6} (E(m) - 1) + BU_{inter}^{PMIPv6} + A^{traditional} E(m) \quad (16)$$

Through the analysis of the proposed Proxy-AAA scheme, the entire signaling overhead of its LMA region could be expressed as follows.

$$C_{signal-proposed} = BU_{LMA} + A_{intra}^{Proxy-AAA} (E(m) - 1) + A_{inter}^{Proxy-AAA} = BU_{intra}^{PMIPv6} (E(m) - 1) + BU^{Proxy-AAA} + A_{intra}^{Proxy-AAA} (E(m) - 1) + A_{inter}^{Proxy-AAA} \quad (17)$$

It is assumed that under the proposed Proxy-AAA scheme, the binding update signaling cost incurred by MN movements between LMA domains is expressed as follows.

$$BU^{Proxy-AAA} = 2C_{MN-MAG} + 2C_{MAG-LMA} + 2C_{LMA-LMA} + 2P_{MAG} + 3P_{LMA} \quad (18)$$

When using the Proxy-AAA scheme, LMA coexists with AAAV. Assuming $l_{LMA-AAA} = 0$, then the authentication signaling overhead for inter and intra domain can be expressed as follows.

$$A_{intra}^{Proxy-AAA} = 2C_{MN-MAG} + 2C_{MAG-MAG} + 2C_{MAG-LMA} + 4P_{MAG} + P_{LMA} \quad (19)$$

$$A_{inter}^{Proxy-AAA} = 2C_{MN-MAG} + 2C_{MAG-MAG} + 2C_{MAG-LMA} + C_{LMA-LMA} + 2C_{AAAV-AAAH} + 4P_{MAG} + 2P_{LMA} + P_{AAA} \quad (20)$$

$$C_{MN-MAG} = 10\eta l_{MN-MAG} l_s C_{MAG-MAG} = \eta l_{MAG-MAG} l_s C_{MAG-LMA} = \eta l_{MAG-LMA} l_s \quad (21)$$

$$C_{LMA-HA} = \eta l_{LMA-HA} l_s C_{LMA-LMA} = \eta l_{LMA-LMA} l_s C_{LMA-AAA} = \eta l_{LMA-AAA} l_s \quad (22)$$

$$C_{AAAV-AAAH} = \eta l_{AAAV-AAAH} l_s \quad (23)$$

$$A_{intra}^{Proxy-AAA} = \left(20\eta l_{MN-MAG} + 2\eta l_{MAG-MAG} + 2\eta l_{MAG-LMA}\right) l_s + 4P_{MAG} + P_{LMA} \quad (24)$$

$$A_{inter}^{Proxy-AAA} = \begin{pmatrix} 20\eta l_{MN-MAG} + 2\eta l_{MAG-MAG} \\ +2\eta l_{MAG-LMA} + \eta l_{LMA-LMA} \\ +2\eta l_{AAAV-AAAH} \end{pmatrix} l_s + 4P_{MAG} + 2P_{LMA} + P_{AAA} \quad (25)$$

Assuming that the signaling overhead ratio of Proxy-AAA and traditional AAA schemes is R, R can be expressed as $R = C_{signal-proposed} / C_{signal-traditional}$. The

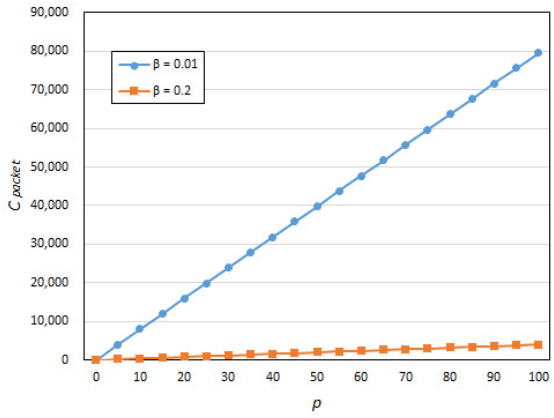

Figure 7. Packet data transmission overhead ($\mu = 0.1$).

average overhead for signaling can be expressed as $C_{signal-a} = C_{signal-proposed} / T_a$ by analyzing the signaling overhead equation in the LMA region above. In this expression, T_a refers to the average residence time in this LMA region. It should be noted that the value must be smaller than 0.3 in the actual network environment.

4.2. Numerical Results

This section will compare the system overhead. Specific parameters and values are shown in Table 2.

Table 2. The parameter Definition.

Parameter	Value	Parameter	Value
$l_{MAG-LMA}$	5	l_{MN-MAG}	1
P_{MAG}	4	l_{HA-LMA}	10
$l_{LMA-LMA}$	10	$l_{LMA-AAA}$	10
σ	0.05	η	0.1
P_{LMA}	3	P_{HA}	4
P_{AAA}	3	l_{CN-HA}	50
$l_{MAG-MAG}$	1		

First of all, we establish MNs as a vehicle and pedestrian, analyzing their different data pocket transmission overheads individually. Figure 7 shows the data packet transmission overhead under a condition that MNs are pedestrians ($\beta = 0.01$) and vehicles ($\beta = 0.2$). We can see that the data pocket transmission overhead C_{packet} increases when the PMR p increases.

Figure 8 shows how the data packet transmission overhead changes when the value of PMR $p = 10$, $p = 50$ or $p = 100$. We can see that as the average switching rate increases when the MN moves, the data packet transmission overhead C_{packet} increases.

Figure 9 analyzes the average signaling overhead of Proxy-AAA. This implies that the signaling overhead C_{signal} increases with the increases as the arrival

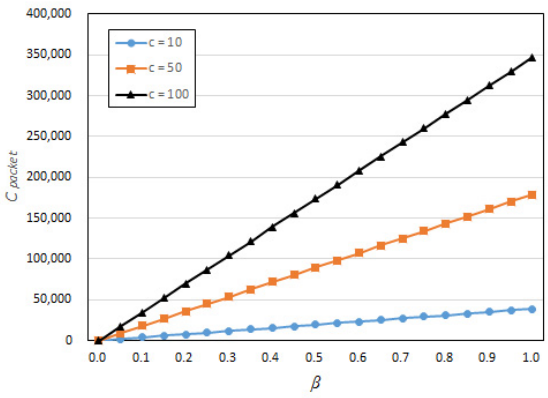

Figure 8. Packet data transmission overhead ($\mu = 0.1$).

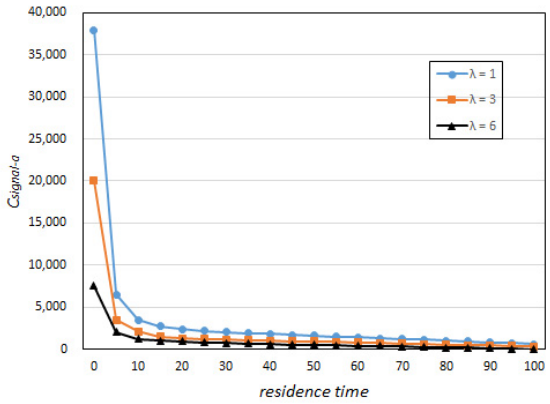

Figure 10. Signaling overhead ($l_{AAAV-AAAH} = 50$).

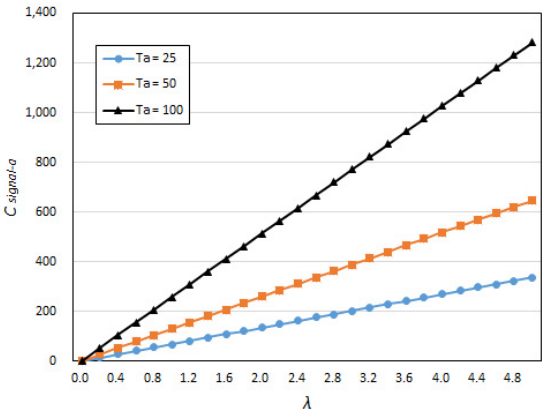

Figure 9. Signaling overhead ($l_{AAAV-AAAH} = 50$).

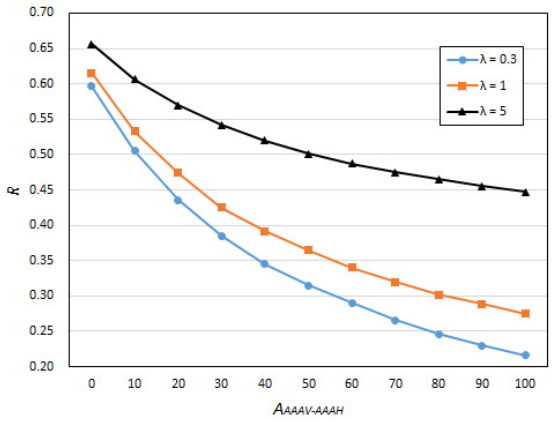

Figure 11. Ratio of signaling overhead (Proxy-AAA / traditional AAA).

rate of authentication events λ increases. Frequent arrival of MN brings increase in authentication events arrival rate and indicates an increase in intra-domain authentication in LMA domain and signaling overhead in registration.

Figure 10 analyzes the average signaling overhead of Proxy-AAA. This shows that the increase of residence time leads to a reduced signaling overhead C_{signal}.

Figure 11 analyzes the signaling overhead ratio R between Proxy-AAA and traditional AAA schemes. This shows that R must be less than 1 all times. In other words, the signaling overhead of the proposed Proxy-AAA scheme is always smaller than signaling overhead value of traditional AAA schemes irrelevant of whether MN moves between domains or to the same LMA region.

Figure 12 shows the changes of the signaling overhead ratio between traditional AAA schemes and Proxy-AAA schemes, when the value of $A_{AAAV-AAAH} = 10$, $A_{AAAV-AAAH} = 50$ and $A_{AAAV-AAAH} = 100$, respectively. This shows that an increase in arrival rate of authentication event reduces signaling overhead ratio between proposed Proxy-AAA schemes and traditional AAA schemes.

Figure 13 shows analysis of the entire overhead based on PMR p increases ($\beta = 0.01$, $\lambda = 1$). When the pedestrian ($\beta = 0.01$) moves, we can see that as the value of p increases, entire overhead C_{total} increases.

Figure 14 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

In this paper we proposed a sensor Proxy-AAA Authentication Scheme based on Fast Handover and Forwarding Mode for IP-based Internet of Things. In this study, the way of reducing the long delay time and

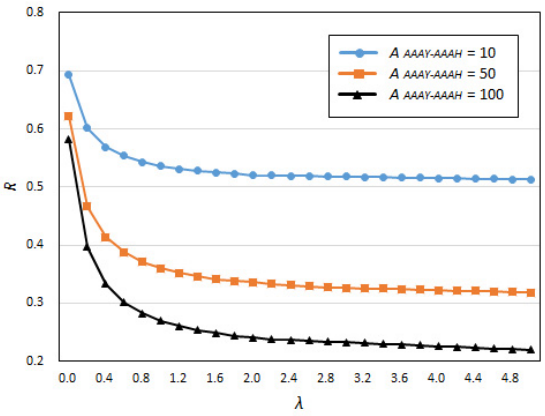

Figure 12. Change of signaling overhead ratio (Proxy-AAA / traditional AAA).

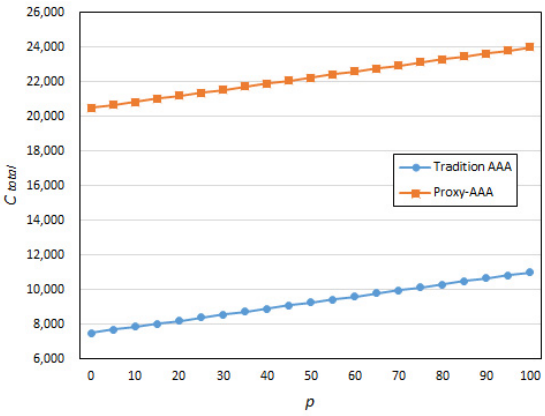

Figure 13. Figure 12 Total overhead ($\beta = 0.01$, $\lambda = 1$).

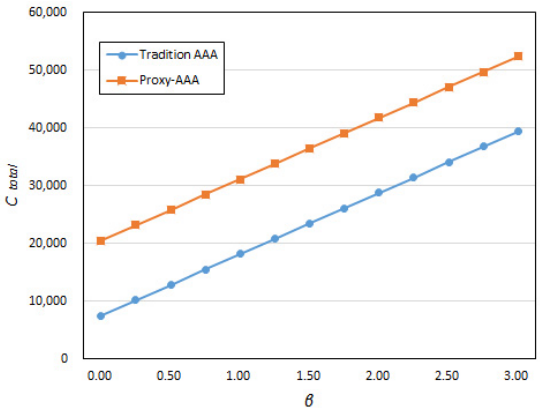

Figure 14. Figure 13 Total overhead ($p = 30$, $\lambda = 1$).

additional overhead from movement of mobile device in mobile IP environment by combining AAA and PMIPv6. This scheme has established a safe handover by efficiently reducing signaling overhead generated by authentication processes. Here we could confirm that fast mobility mode and forwarding mode between various LMAs were supported. Moreover, the overall signaling overhead also showed that proposed Proxy-AAA scheme always has smaller value than previous traditional AAA schemes, hence enabling efficient movement between domains by AAA Authentication Scheme in forwarding mode at PMIPv6 supporting local mobility. Also, during movement between LMA domains, it was confirme that the farther the distance between RAAAS (Root AAA Server) and home domain, the higher the performance efficiency.

Acknowledgement. This work was supported by the Technology Innovation Program (10054486, Development of Open Industry IoT (IIoT) Smart Factory Platform and Factory-Thing Hardware Technology) funded By the Ministry of Trade, industry & Energy (MI, Korea).

This work was supported by ąřThe Components & Materials Technology Development Program (10043800, Development of Micro Smart Environmental Sensor Measurement Module, Control Chip, and Application Program)ąś funded by the Ministry of Trade, Industry & Energy (MI, Korea).

This work was supported by the Energy Technology Development Program (2013T100200078, development of integrated demand response system technology for co-residential resources and demonstration of business model) funded by the Ministry of Trade, Industry & Energy (MOTIE, Korea).

This work was supported by Global Creative Software (GCS) Project (No. 2014-044-028-001, Development of ICT Convergence Technology for Design Optimization and Construction Technology Innovation of the Structural Frame and Envelope) funded by the Ministry of Science, ICT & Future Planning (MSIP).

References

[1] C. de Laat and G. Gross and L. Gommans and D. Spence (2000) *Generic AAA Architecture*(RFC 2903).

[2] Francesco Palmieri and Ugo Fiore and Aniello Castiglione (2011) *Automatic security assessment for next generation wireless mobile networks*(Mobile Information Systems), Volume 7, pp. 217-239.

[3] P. Calhoun and J. Loughney and E. Guttman and G. Zorn and J. Arkko (2003) *Diameter Base Protocol*(RFC 3588, September 2003).

[4] Le F and Patil B and Perkins C, et al (2004) *Diameter mobile IPv6 application*(Internet IETF Draft, 2004).

[5] Lee S Y and Huh E N and Kim S B, et al (2005) *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.

[6] Kim M and Kim M and Mun Y (2005) *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.

[7] Song Mei and Wang Li and Song Jun-de (2008) *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.

[8] Ilsun You and Takahiro Hara (2010) *Mobile and Wireless Networks*(Mobile Information Systems), Volume 6, pp. 1-3, 2010.

[9] G. Giaretta (2009) *Interactions between PMIPv6 and MIPv6: scenarios and related issues*(draft-ietf-netlmm-mip-interactions-04, June 2009).

[10] Arjan Durresi and Mimoza Durresi and Leonard Barolli (2008) *Secure authentication in heterogeneous wireless networks*(Mobile Information Systems), Volume 4, pp. 119-130, 2008.

[11] Hakseon Hwang and Jongpil Jeong (2013) *Reduction of Authentication Cost Based on Key Caching for Inter-MME Handover Support*(The Journal of the Institute of Webcasting, Internet and Telecommunication), Volume 13, pp.209-220, October 2013.

[12] JeongBae Han and Seung-Hyun Lee and Dongryeol Shin and Jongpil Jeong (2011) *Performance Analysis of Proxy-AAA Authentication Scheme in PMIPv6 Networks with Forwarding Mode Supporting*(The Fourth Workshop on Information Technologies and Communication - WOTIC 2011), pp. 81, October 2011.

[13] Seung-Hyun Lee and Dong-Ryeol Shin and Jongpil Jeong (2012) *Performance Analysis of Proxy-AAA Authentication Scheme in PMIPv6 Networks with Forwarding Mode Supporting*(Journal of Korean Society for Internet Information), Volume 13, pp.15-25, February 2012.

[14] Se-Won Yoo and Jongpil Jeong (2012) *Analytical Approach of Fast Inter-Domain Handover Scheme in Proxy Mobile IPv6 Networks with Multicasting Support*(The KIPS Transactions:PartC), Volume 19C, pp.153-166, April 2012.

[15] Hyun-Suk Chai and Jongpil Jeong (2012) *Security Analysis and Implementation of Fast Inter-LMA domain Handover Scheme in Proxy Mobile IPv6 Networks*(The KIPS Transactions:PartC), Volume 19C, pp.99-118, June 2012.

[16] Jae-Hoon Kim and Jongpil Jeong (2011) *Performance Analysis of Cost-Effective Handoff Scheme in PMIPv6 Networks with DNS Supporting*(The 3rd International Conference on Internet - ICONI 2011), pp. 149-153, December 2011.

[17] J.-F. Guan, et al (2009) *Implementation and analysis of proxy MIPv6*(Published Online, WCM), September 2009.

[18] A.J. Jara and M. A. Zamora and A. F. G. Skarmeta (2010) *An Initial Approach to Support Mobility in Hospital Wireless Sensor Networks based on 6LoWPAN (HWSN6)*(Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications), vol. 1, no. 2/3, pp. 107-122, 2010.

[19] SeungYoon Park and Jongpil Jeong (2013) *On Pointer Forwarding Based Mobility Management for Cost-Optimized Proxy Mobile IPv6 Networks*(2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing - IMIS 2013), pp. 29-36, July 2013.

[20] Do-Kyoung Ra and Jongpil Jeong (2012) *Cost-Effective Mobility Management Scheme in Proxy Mobile IPv6 Networks with Function Distributor Support*(The Journal of the Institute of Webcasting, Internet and Telecommunication), Volume 12, pp.97-107, February 2012.

[21] J. Jeong and M. Kang and Y. Cho and J. Choi (2013) *3S: Scalable, secure and seamless inter-domain mobility management scheme in proxy mobile IPv6 networks*(International Journal of Security and its Applications), Volume 7, Issue 4, pp. 51-70, July 2013.

[22] Jongyoun Kim and Jongsun Park and Jongpil Jeong (2012) *LC-GM2: Low-Cost Global Mobility Management Scheme in Proxy Mobile IPv6 Networks*(KIPS Transactions on Computer and Communication Systems), Volume 1, pp.193-204, December 2012.

[23] D.-G. Anderson (2005) *Improving end-to-end availability using overlay networks*(Massachusetts Institute of Technology), February 2005.

[24] Jain R and Raleigh T and Graff C, et al (1998) *Mobile Internet access and QoS guarantees using mobile IP and RSVP with location registers*(Proceedings of International Conference on Communications (ICC'98)), Vol 3, pp. 1690-1695, June 1998.

[25] Lee K and Mun Y (2005) *An efficient macro mobility scheme supporting fast handover in hierarchical mobile IPv6*(Proceedings of the International Conference on Computational Science and its Applications (ICCSA'05)), pp. 408-417,May 2005.