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], and Tai-Myoung Chung[1](✉)

[1] College of Information and Communications Engineering, Sungkyunkwan University, Suwon, Kyunggi-do 440-745, Republic of Korea
tgb017@nate.com

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

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

Abstract. Recently, with the development of IoT technology, a wireless sensor network technology capable of real-time management by receiving information wirelessly through various kinds of sensors has been actively developed. Hence, reducing the signaling cost becomes an important issue because most of the sensors are powered by battery only. In addition, since the Internet of objects is open on the Internet in object environments, security issues related to authentication of users accessing wireless networks are very important. AAA technology is the best possible way these days of resolving delay issue when introducing authentication process of mobile switching. However, despite long development in AAA technology, the mobility management in wireless network environment has yet to be researched further. To solve these problems, we propose a Proxy-Authentication Authorization Accounting (Proxy-AAA) authentication scheme. This places the AAA server in the LMA so as to the cost of authentication by means of a short, simple mobile authentication. The proposed method reuses the LMA-based session key in the authentication process when moving within the domain, and reuses the AAA server based session key when moving between domains. The AAA server of the scheme will be deployed on Local Mobility Anchor (LMA), making up for the shortage of simple fast handover authentication and hierarchical authentication, and further reducing the cost of intra-domain authentication.

Keywords: Proxy-AAA authentication · Fast handover · Forwarding · Wireless Body Area Networks (WBAN)

J.-H. Lee and S. Pack (Eds.): QShine 2016, LNICST 199, pp. 22–35, 2017.
DOI: 10.1007/978-3-319-60717-7_3

1 Introduction

The potential of the Future Internet is not limited to smart phones. Internet of Things (IoT) is another emerging area of the Future Internet, which is offering a higher integration of the cybernetic and physical world. The main goal of the IoT is collecting data from the real-world entities and events. In order to maintain a reliable connection of distributed IoT equipment, it is important to establish a secure link for end-to-end communication using appropriate authentication. In the internet of things environment, due to the openness of the IoT, the security issue related to authentication of user accessing wireless network is extremely important. AAA technology is the best possible way these days of resolving delay issue when introducing authentication process of mobile switching [1,2]. However, despite long development in AAA technology, the mobility management in wireless network environment has yet to be researched further. Due to the deployment of MIPv6 networks and the development of new access technologies, the RADIUS protocol, which provides centralized authentication and authorization services, can no longer meet requirements. Diameter protocol, an improved version of 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]. To solve these problems, we propose a Proxy-Authentication Authorization Accounting (Proxy-AAA) authentication scheme. This places the AAA server in the LMA so as to the cost of authentication by means of a short, simple mobile authentication. The proposed method reuses the LMA-based session key in the authentication process when moving within the domain, and reuses the AAA server based session key when moving between domains. The AAA server in the scheme will be deployed on Local Mobility Anchor (LMA), making up for the shortage of simple fast handover authentication and hierarchical authentication, and further reducing the cost of intra-domain authentication [8]. We analyzed the performance of the MIPv6 protocol and the proposed scheme using the mathematical analysis and the network simulation tool. The signaling overhead of the proposed Proxy-AAA scheme is always smaller than that of the existing AAA scheme regardless of the LMA domain or inter-domain movement. When the mobile node (MN) moves away from the home domain, the signaling overhead of Proxy- Efficiency is increased. We first describe and compare basic MIPv6 and PMIPv6 in Sect. 2. In Sect. 3, we introduce our proposed Proxy-AAA and protocol selection scheme. In Sect. 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

Recently, mobility solutions are divided into two trends: evolutionary research that follows an IPv6-based approach, and a clean-slate trend. The clean-slate trend is based on new concepts such as identifiers and location-partitioning architectures. This kind of architecture has the advantage that the mobility is directly supported since the session recognition and the locator of the equipment are separated. However, this type of solution has the overhead incurred by a limited network such as 6LoWPAN and the cost incurred by replacing the current hardware and infrastructure. Another trend is evolutionary research, and the main protocol following evolutionary research is MIPv6. MIPv6 uses two IPv6 addresses; one is the initial address of the device, and the home address is mainly used as identification data. The other is Care-of-address, which is newly issued in the visited network and used as the locator of the equipment. The MIPv6 protocol extends the IPv6 header to manage the binding between these two addresses and provides a signaling message. In particular, it defines IPSec tunneling between the mobile node and the home agent, and defines a return routability mechanism that performs route optimization to avoid triangle routing [9]. This ensures the security and authentication of the mobile node to the binding update when the node needs to register a new Care of address. However, MIPv6 is considered to be unsuitable for 6LoWPAN nodes because it transmits very heavy messages during handover processing and requires high processing requirements [10]. PMIPv6 is a Network Mobility (NEMO) [11,12] based protocol proposed to reduce MN overload. This does not require mobile functionality in the IPv6 stack because it delegates mobility signaling message processing from the MN to MAG equipment acting as a proxy. This protocol is suitable for 6LoWPAN because it avoids MN's involvement in mobility-related signaling. We configure the sensor node information to be received by the monitoring system via the gateway. The sensor node resource receiving method is a method of establishing an information request in an external network and a polling method in which a gateway periodically requests information to a sensor network [13,14]. When the polling request method is used for sensor information collection, inefficient battery consumption may occur due to the wireless signaling used continuously by the sensor. In this paper, we used an asynchronous method to transmit data to a gateway in case of data fluctuation, instead of a polling method, to provide sensing data of a sensor network. To this end, the sensor node transmits the information to the MN acting as a gateway of the sensor when the sensing data fluctuates. Such a scheme transmits information only at the time of change, and thus enables efficient use of radio resources. The MN, acting as a gateway, stores the received sensing data in the cache and delivers the information stored in the cache by the monitoring system request.

3 Proposed Scheme

3.1 Handoff Scheme Using Virtual Layer Between the LMA

Recently, with the development of IoT technology, a wireless sensor network technology capable of real-time management by receiving information wirelessly through various kinds of sensors has been actively developed. In addition, a wireless network called WBAN (Wireless Body Area Network) [15] can be configured to exchange data such as biometric signals through a network composed of people wearing clothes or various devices attached to the human body. In this regard, the Low Power Wireless Personal Area Network (LoWPAN) has attracted a lot of attention recently because it can support the communication of Internet of Things. 6LoWPAN is a network-based low-power technology based on IEEE 802.15.4, which it uses a limited processing capability and power. Because the sensor must be directly involved in mobility-related signaling, PMIPv6, the network-based mobility protocol, is considered to be the most suitable for supporting the mobility of WBAN. However, it is a heavy burden for the sensor itself to send a message related to mobility to the agent. Hence, reducing the signaling cost becomes an important issue because most of the sensors are powered by battery only. In addition, the introduction of authentication in the process of mobile IP handover incurs extra costs. Most solutions available today fail to satisfy some of the requirements in specific circumstances. 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 scheme, on the other hand, offers a better way to improve authentication and binding update processes not only for the intra-domain handover and authentication processes, but also for the inter-domain mobilization. Proxy-AAA reuses the session keys based on LMA of HMIPv6 in both authentication processing and intra-domain handover. In inter-domain handover and processing authentication, Proxy-AAA reutilizes session keys derived from the AAA server and performs a direct transmission between multiple LMAs [16].

3.2 Operation Procedures of Sensor Proxy-AAA

Figure 1 shows the flow of signals and data packets between different LMAs when the MN moves. When the MN reaches the LMA2 area while moving to the LMA3 area, the MAG in the area sends a BU message to the LMA2. This causes LMA2 to respond to LMA1. On receiving the message from LMA2, LMA compares the received message with the LMA list and updates the current LMA address of the MN. The packet data is then transmitted directly from LMA1 to LMA2.

Figure 2 shows the specific message flow in inter-domain handover. When the MN reaches the LMA2 area while moving to the LMA3 area, the MN sends an RS message to the nMAG of the area. On receiving the RS message, nMAG sends an Authentication Request command to the pMAG, and the pMAG encrypts the session key S_{MN-MAG} and S_{MAG-HA} using $K_{pMAG-LMA}$ and sends it to the pLMA. pLMA passes the encrypted session key back to nLMA. After the nLMA stores the session key, it sends a notification message to the nMAG about session key reuse. nMAG forwards the response message to the pMAG for session key reuse and sends the PBU message to nLMA [17]. Upon receiving

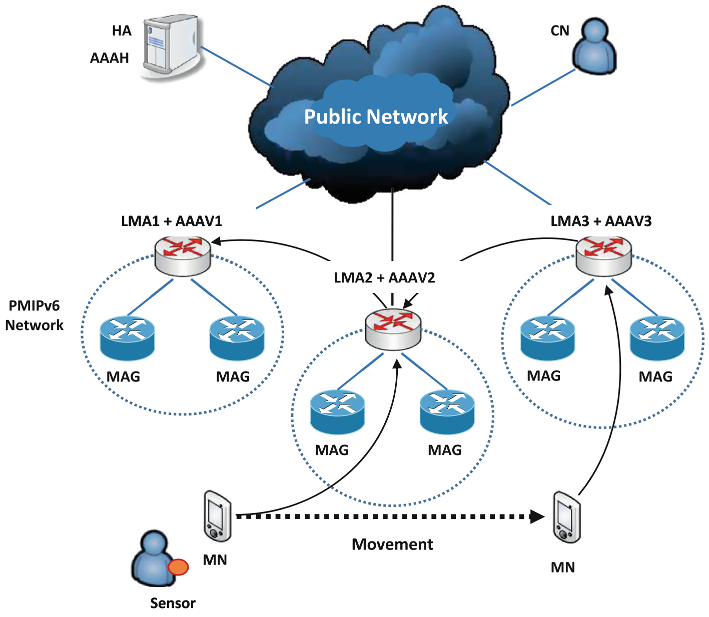

Fig. 1. Forwarding scheme between different LMA.

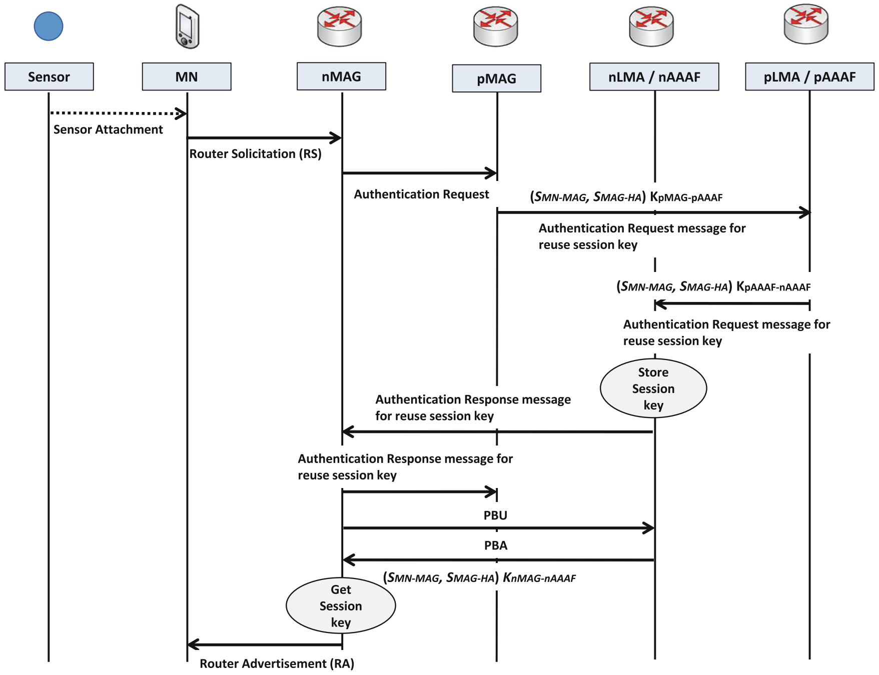
Sensor
MN
nMAG
pMAG
nLMA / nAAAF
pLMA / pAAAF
Sensor Attachment
Router Solicitation (RS)
Authentication Request
(SMN-MAG, SMAG-HA) KpMAG-pAAAF
Authentication Request message for
reuse session key
(SMN-MAG, SMAG-HA) KpAAAF-nAAAF
Authentication Request message for
reuse session key
Store
Session
key
Authentication Response message
for reuse session key
Authentication Response message for
reuse session key
PBU
PBA
(SMN-MAG, SMAG-HA) KnMAG-nAAAF
Get
Session
key
Router Advertisement (RA)

Fig. 2. Inter-domain handover flow.

the PBU message, nLMA encrypts the session key S_{MN-MAG} and S_{MAG-HA} using $K_{pMAG-LMA}$, and transmits the value to the nMAG by including it in the PBU. After obtaining the session key, nMAG responds with an RA message to the MN. Accordingly, a reliable binding UPDATE channel between the MN and the LMA is created. Figure 3 shows the specific flow process of intra-domain handover. After a reliable binding update channel between the MN and the LMA is established, the sensor node can start transmitting the sensing data. When the sensing data is generated, the sensor node asynchronously transmits the corresponding information to the MN, and the MN stores the information in the cache, and converts the information according to the IPv6 protocol.

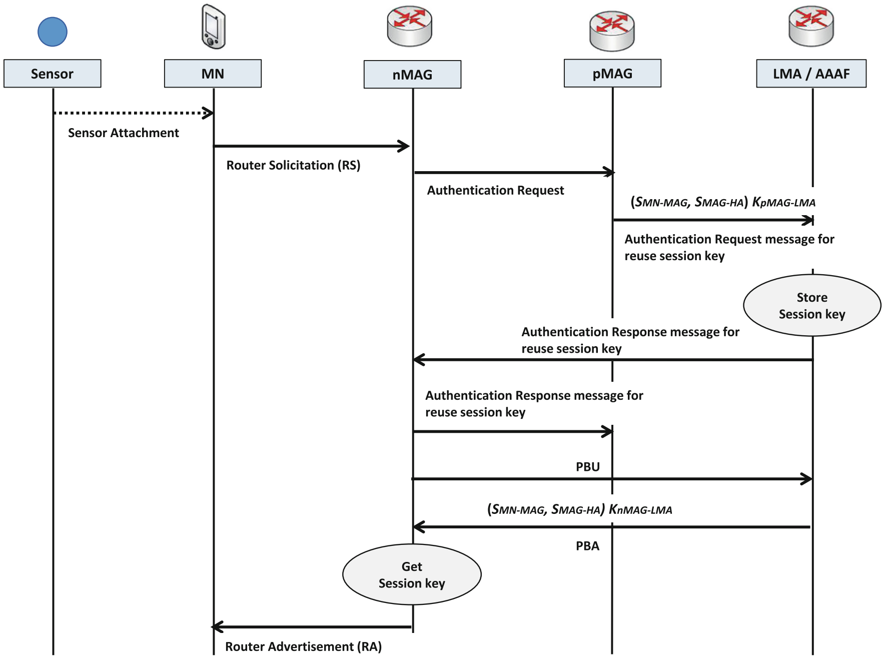
Sensor
MN
nMAG
pMAG
LMA / AAAF
Sensor Attachment
Router Solicitation (RS)
Authentication Request
(SMN-MAG, SMAG-HA) KpMAG-LMA
Authentication Request message for reuse session key
Store Session key
Authentication Response message for reuse session key
Authentication Response message for reuse session key
PBU
(SMN-MAG, SMAG-HA) KnMAG-LMA
PBA
Get Session key
Router Advertisement (RA)

Fig. 3. Intra-domain handover flow.

3.3 Protocol Selection

To select the most suitable mobility management protocol for the network and MNs, during the authentication process, the MAG examines the profiles of the MNs and finds the MN's preferences. In the authentication process, MAG searches MNs profile for MNs preference. From the search, in case MNs preferred protocol matches what was provided from access network, the matching protocol will be selected [18]. 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 Proxy-AAA schemes, MAG finds the path response time through the search process. While the route is being searched, the MAG sends two proving messages to the LMA. 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 after the path search for (z_n) hours can be calculated as follows.

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

The parameter α represents the weight of past events in the average calculation. In a similar manner, the average RTT for the Proxy-AAA scheme can be calculated and denoted as t_n. When MN's movement frequency is low, the path response time of existing MIPv6 is smaller than our Proxy-AAA. On the other hand, when the MN's movement frequency is high, the basic MIPv6 response time is higher than our Proxy-AAA scheme. In appropriately selecting the better protocol according to network condition and mobility parameters, protocol selection can be used.

$$\begin{aligned} \frac{\overline{t_n}-\overline{z_n}}{N_h} &< H_t, \quad selectProxy-AAAscheme \\ \frac{\overline{t_n}-\overline{z_n}}{N_h} &\geq H_t, \quad\quad selectBasicMIPv6 \end{aligned} \tag{2}$$

Here, N_h is a handover frequency, $\overline{t_n}-\overline{z_n}/N_h$ is an index for judging a protocol with better performance, and H_t is a quality threshold value for determining which protocol should 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 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 4 shows the network topology of a specific Proxy-AAA for a system overhead analysis.

$$C_{total} = C_{signal} + C_{packet} = \beta\left(C_{reg} + C_{auth}\right) + \alpha C_{CN-MN} \tag{3}$$

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

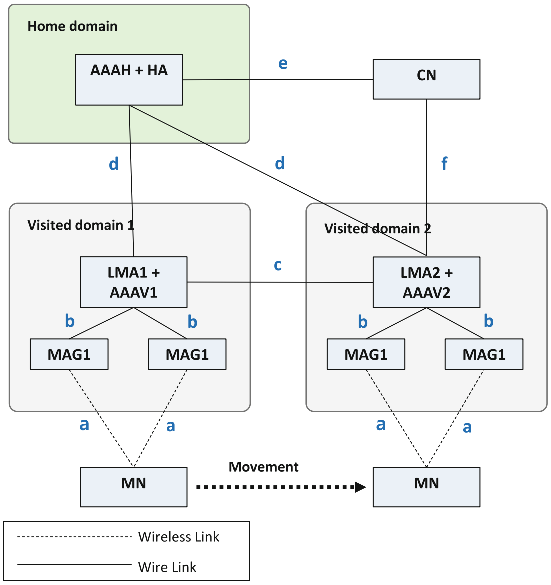

Fig. 4. Cost analysis model of Proxy-AAA.

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 [19]. 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 $l = l_d/l_s$.

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 definition descriptions are shown in Table 1.

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.

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

4.2 Numerical Ruserts

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		

We analyze the different data packet transmission overhead by separating the case where the MN is located in the pedestrian and the vehicle. Figure 5 shows the data packet transmission overhead under a condition that MNs are pedestrians ($\beta = 0.01$) and vehicles ($\beta = 0.2$). From the analysis, it can be seen that the data packet transmission overhead C_{packet} increases as PMR p increases.

Figure 6 shows the data packet transmission overhead value when the value of PMR $p = 10$, $p = 50$ or $p = 100$. It can be seen that the data packet transmission overhead C_{packet} increases as the average switching rate increases as the MN moves.

Figure 7 shows the average signaling overhead of Proxy-AAA. This shows that the signaling overhead C_{signal} increases as the arrival rate of the authentication events λ increases. In other words, the frequent arrival of MN in LMA

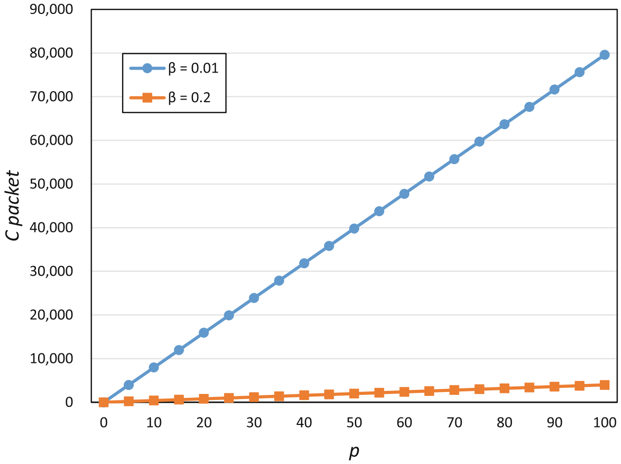

Fig. 5. Packet data transmission overhead ($\mu = 0.1$).

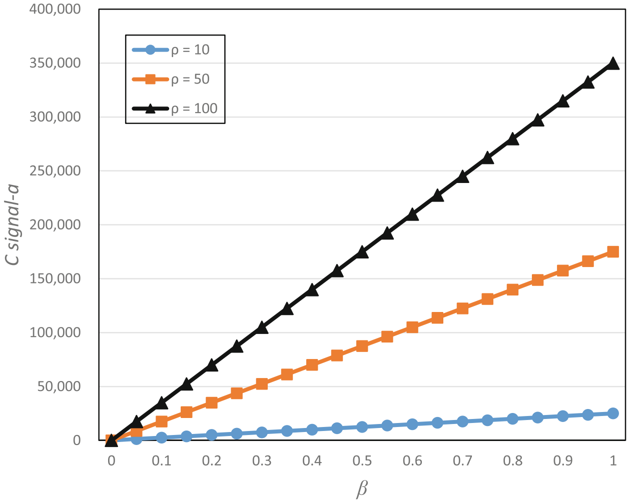

Fig. 6. Packet data transmission overhead ($\mu = 0.1$).

area increases the arrival rate of authentication events and increases signaling overhead during authentication between domains and registration. In addition, we can see that R decreases as λ increases. It can be seen that the efficiency of Proxy-AAA increases as MN moves away from home domain.

Figure 8 analyzes the average signaling overhead of Proxy-AAA. This indicates that the signaling overhead C_{signal} decreases as the residence time T_a increases. That is, if the residence time is long in the same LMA domain of mn, the exchange and authentication between the domains is small and the signaling overhead in the whole system is also low.

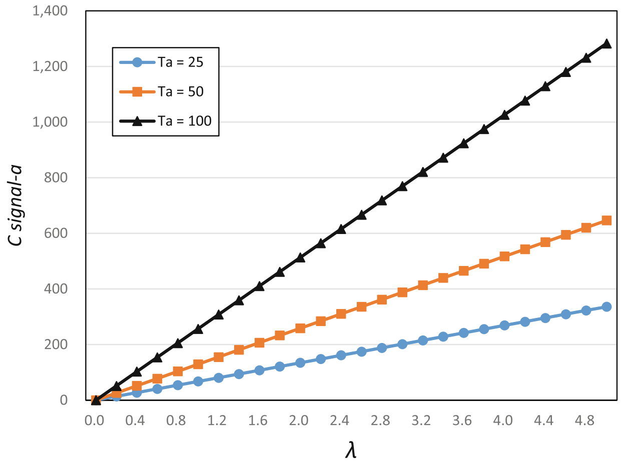

Fig. 7. Packet data transmission overhead ($\mu = 0.1$).

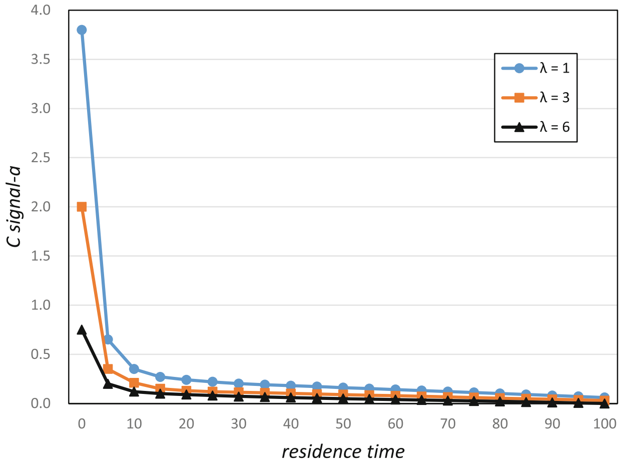

Fig. 8. Packet data transmission overhead ($\mu = 0.1$).

Figure 9 shows analysis of the entire overhead based on PMR p increases ($\beta = 0.01$, $\lambda = 1$). This shows that the total overhead C_{total} increases as the value of p increases when the pedestrian ($\beta = 0.01$) moves.

Figure 10 is an analysis of the overall overhead as the value of β increases. This shows that as the average switching rate of the MN increases, the overall overhead C_{total} increases as the PMR p is fixed.

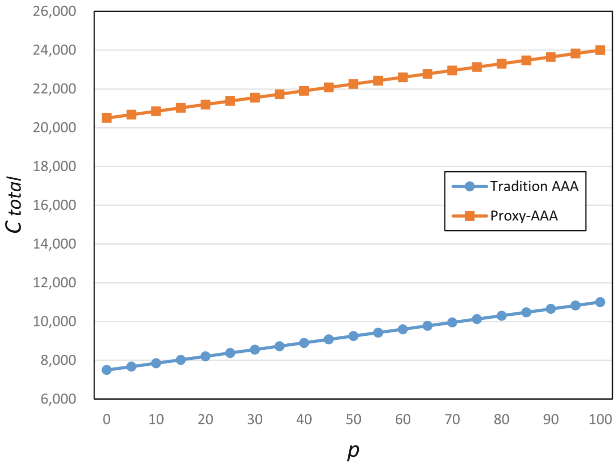

Fig. 9. Signaling overhead ($l_{AAAV-AAAH} = 50$).

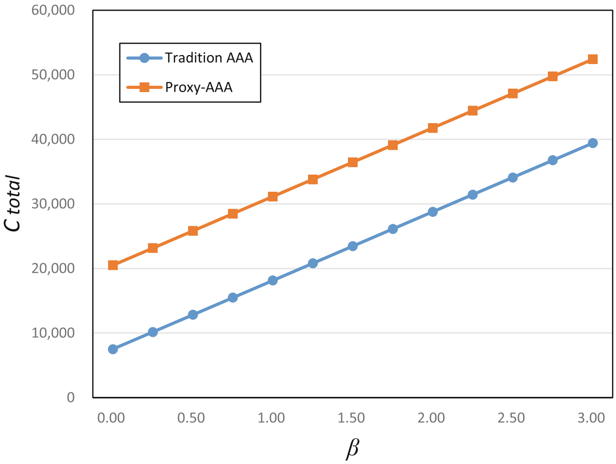

Fig. 10. Signaling overhead ($l_{AAAV-AAAH} = 50$).

5 Conclusions

In this paper, we propose a sensor proxy AAA authentication scheme based on fast handover and forwarding mode for IP-based Internet. This can be applicable not only to micro-mobility but also macro-mobility of MNs in an LMA region. This scheme has established a safe handover by efficiently reducing signaling overhead generated by authentication processes. This study proposes a way of reducing delay time and additional delay from movement of mobile devices in mobile IP environment by means of 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. Therefore, this allows efficient movement between domains from forwarding mode at PMIPv6 supporting local mobility by means of AAA Authentication Scheme. Also, during movement between LMA domains, it was confirmed that the farther the distance between RAAAS (Root AAA Server) and home domain, the higher the performance efficiency.

6 Competing Interests

The authors declare that they have no competing interests.

7 Author's Contributions

This scheme has established a safe handover by efficiently reducing signaling overhead generated by authentication processes. This scheme has established a safe handover by efficiently reducing signaling overhead generated by authentication processes.

References

1. De Laat, C., Gross, G., Gommans, L., Vollbrecht, J., Spence, D.: Grid information services for distributed resource sharing. In: Generic AAA architecture (2000). ISSN 2070-1721
2. Palmieri, F., Fiore, U., Castiglione, A.: Automatic security assessment for next generation wireless mobile networks. Mob. Inf. Syst. **7**(3), 217–239 (2011)
3. Calhoun, P., Loughney, J., Guttman, E., Zorn, G., Arkko, J.: Diameter base protocol (2003). ISSN 2070-1721
4. Le, F., Patil, B., Perkins, C.E., Faccin, S.: Diameter mobile IPv6 application. draft-le-aaa-diametermobileipv6-04 txt Iinternet Draft (2004)
5. Lee, S.-Y., Huh, E.-N., Kim, S.-B., Mun, Y.: An efficient performance enhancement scheme for fast mobility service in MIPv6. In: Gervasi, O., Gavrilova, M.L., Kumar, V., Laganà, A., Lee, H.P., Mun, Y., Taniar, D., Tan, C.J.K. (eds.) ICCSA 2005. LNCS, vol. 3480, pp. 628–637. Springer, Heidelberg (2005). doi:10.1007/11424758_66
6. Kim, M., Kim, M., Mun, Y.: A hierarchical authentication scheme for MIPv6 node with local movement property. In: Gervasi, O., Gavrilova, M.L., Kumar, V., Laganà, A., Lee, H.P., Mun, Y., Taniar, D., Tan, C.J.K. (eds.) ICCSA 2005. LNCS, vol. 3480, pp. 550–558. Springer, Heidelberg (2005). doi:10.1007/11424758_57
7. Mei, S., Li, W.: SONG J-d.: a secure fast handover scheme based on AAA protocol in mobile IPv6 networks. J. China Univ. Posts Telecommun. **15**, 14–18 (2008)
8. Durresi, A., Durresi, M., Barolli, L.: Secure authentication in heterogeneous wireless networks. Mob. Inf. Syst. **4**(2), 119–130 (2008)

9. Son, S., Jeong, J.: Cost-effective handoff scheme based on mobility-aware dual pointer forwarding in proxy mobile IPv6 networks. SpringerPlus **3**(1), 57 (2014)
10. Johnson, D., Perkins, C., Arkko, J.: Mobility support in IPv6 (2004). ISSN 2070-1721
11. Jara, A.J., Zamora, M.A., Skarmeta, A.F.: An initial approach to support mobility in hospital wireless sensor networks based on 6LoWPAN (HWSN6). J. Wirel. Mob. Netw. Ubiquit. Comput. Dependable Appl. (JoWUA) **1**(2/3), 107–122 (2010)
12. Bag, G., Shams, S.S., Akbar, A.H., Raza, H.M.T., Kim, K.-H., Yoo, S.W.: Network assisted mobility support for 6LoWPAN. In: CCNC 2009 6th IEEE Consumer Communications and Networking Conference. IEEE (2009)
13. Moon, Y., Lee, J., Park, S.: Sensor network node management and implementation. In: ICACT 2008 10th International Conference on Advanced Communication Technology. IEEE (2008)
14. Aishwarya, V., Enigo, V.F.: IP based wireless sensor networks with web interface. In: 2011 International Conference on Recent Trends in Information Technology (ICRTIT). IEEE (2011)
15. Xing, J.: A survey on body area network, networking and mobile computing. In: Proceedings of International Conference on Wireless Communications, p. 14, September 2009
16. Han, J., Jeong, J., Jo, J.: Proxy-AAA authentication scheme with forwarding mode supporting in PMIPv6 networks. Int. J. Internet Broadcast. Commun. **5**(2), 18–22 (2013)
17. Jeong, J., Kang, M., Cho, Y., Choi, J.: 3S: scalable, secure and seamless inter-domain mobility management scheme in proxy mobile IPv6 networks. Int. J. Secur. Appl. **7**(4), 51–70 (2013)
18. Ra, D.-K., Jeong, J.-P.: Cost-effective mobility management scheme in proxy mobile IPv6 networks with function distributor support. J. Inst. Internet Broadcast. Commun. **12**(1), 97–107 (2012)
19. Jain, R., Raleigh, T., Graff, C., Bereschinsky, M.: Mobile internet access and QoS guarantees using mobile IP and RSVP with location registers. In: 1998 ICC 98 Conference Record 1998 IEEE International Conference on Communications. IEEE (1998)