Telecommun Syst (2010) 45: 37–45
DOI 10.1007/s11235-009-9232-3

Subscriber authentication technology of AAA mechanism for mobile IPTV service offer

Jong Hyuk Park

Published online: 4 December 2009

Abstract In the modern society, the rapid development of IT and distribution of the internet and computers through super-high speed networks have led to the new cultural turning point called u-knowledge-based society. Such a change has contributed to the environment where digital materials rapidly increase and communication infra is expanded, and thus image and sound information can be shared through IP network as demand for integrated service is increasing. In providing IPTV through IP network, IPTV may result in illegal control, illegal contents distribution, service theft, access of unapproved ones, sniffing, tapping, DoS (Denial of Service) attack, War Dialing attack, man-in-the-middle attack, Rogue Device attack, harmful software infection, which all indicates the security vulnerability. As such various weaknesses exist, this study research the subscriber authentication technology of AAA mechanism to provide mobile IPTV services so as to security and efficiency in terms of subscribers in the next generation mobile IPTV.

Keywords Authentication · Authorization · Accounting · Mobile IPTV

1 Introduction

IT technology is advancing into ubiquitous environment as the Internet and mobile devices develop. Such a change will provide users with various services, and require for them is increasing rapidly as users want services even while using mobile devices. When it comes to the domestic market scale of the next generation telecommunication, the use of services via mobile devices is expected to be ubiquitous environment centering.

However, in spite of the possibilities of advancement and various services, the wireless environment has many risks and weaknesses compared to existing wire networks. For example, wireless environment for mobile devices has risks of sniffing, tapping, DoS (Denial of Service) attack, man-in-the-middle attack, Rogue Device attack, harmful software infection, which show the security vulnerability, as well as the risks of existing wireless environment. In other words, in receiving IPTV via IP network, IPTV also has security vulnerability such as illegal control, illegal contents distribution, service theft, access of unapproved ones, sniffing, tapping, DoS attack, War Dialing attack, man-in-the-middle attack, Rogue Device attack, harmful software infection, etc. [6, 14]. With such various weaknesses, this study includes the research on subscriber authentication technology in AAA (Authentication, Authorization, Accounting) mechanism to provide mobile IPTV services. The organization of this paper is as follows. Section 2 presents the overview of IPTV and AAA, security threat of IPTV and security requirements. Section 3 analyzes CAS and DRM, the existing IPTV security technologies. Section 4 presents secure subscriber authentication technologies to provide mobile IPTV services. Section 5 analyzes proposed scheme, and lastly, Sect. 6 describes the conclusion and future study.

2 Background

This section presents the overview of bilinear pairing and AAA, and analyzes security threat and security requirements with regard to existing IPTV.

J.H. Park (✉)
Department of Computer Science and Engineering, Seoul National University of Technology, 172 Gongreung 2-dong, Nowon-gu, Seoul, 139-742, Korea
e-mail: parkjonghyuk1@hotmail.com

2.1 AAA

The AAA (Authentication, Authorization, and Accounting) standard devised by the IETF working group is applicable to the Diameter protocol. The stage was reached where an AAA protocol appropriate for the next-generation roaming environment was established, without restricting the existing RADIUS (Remote Authentication Dial In User Service) protocol. For this protocol standard, a formal working group was formed in December 1998, and the applicable AAA protocol was named Diameter. The basic structure of the Diameter protocol is divided into transmission protocols that include SCTP (Stream Control Transmission Protocol), a base protocol that includes accounting functions, and various high level application protocols.

With the extension of IP-based Internet, there is an increase in demand for accessing the network in wireless mobile environments. Even in wireless environments, there were multiple service environments for users, including QoS (Quality of Service) provision or pre-payment card and others. In order to satisfy requirements of users, wired and wireless businesses must provide secure and high level services for legitimate users. The AAA protocol is an essential element for such secure network access, mobile service, user authentication, authorization and accounting processing. In 1991, the AAA protocol was proposed with the Radius protocol by Livingston Company, and provides an AAA service for the SLIP (Serial Line Internet Protocol) or PPP (Point-to-Point Protocol) linkage service within the management domain in its first version. However, at present, service networks are gradually evolving into open-types, and networks are evolving into a series of multiple domain environments. Therefore, the IETF AAA working group is focused on the standardization of the Diameter protocol for providing AAA services appropriate for the roaming environments. In the case of domestic environments, within the recent mobile Internet business domain, the relevant businesses are quickly working on providing Mobile IPv4 and Mobile IPv6 services. For such mobile environments, AAA services between domains must be applied. For practical services in environments, there is a need for technological development in accordance with the existing standard, however, technological development of the mutual operation test is required, to determine if interworking is possible between the standard adaptability test and products. From domestic standardization organizations and foreign standardization organizations, once the Diameter protocol standard is completed and the mobile Internet environment is standardized, the use of the Diameter protocol will expand rapidly, and the market is expected to grow more rapidly [1–3, 5, 9, 10, 12].

2.2 Security technology of IPTV

As representative IPTV security technologies, the overview of CAS and DRM is presented, and the characteristics, advantage and disadvantage are analyzed.

2.2.1 CAS

CAS (Conditional Access System) has been used as the basic system to control users' access to charged broadcasting services since the time of analogue broadcasting. Access conditions of CAS control include subscription fee payment, receiving regions, receiving grades, etc. Thus, CAS in principle aims to protect the business and profits of charged broadcasting service providers.

When it comes to standard, DVB CAS in Europe, and ATSC CAS in USA were established. Besides, OpenCable CAS is the standard for digital cable TV in USA based on ATSC CAS. Although there are standards for CAS, the details regarding specific representation of CAS have yet to be defined. Coexistence of many CASs may be possible, but the compatibility of different kinds of CASs is not secured. The authority given to users who apply for certain broadcasting services is called Entitlement, and CAS controls the access so that only qualified users can receive the services. The items applied may be certain programs, or a set of TV channels.

CAS has gained reliability from various broadcasting service providers since it is a contents security solution that has been used for existing services, but the condition of IPTV service is somewhat different. This is a fundamental matter of CAS introduced based on the structure suitable for one-way broadcasting. CAS is a polling type system, not Request/Response structure, and has the fundamental problem wasting transporting streams. EMM (Entitlement Management Message) with information only for qualified users is transmitted via broadcasting media, and in consideration of the characteristic of broadcasting that all users share the bandwidth of one medium, every EMM chasing set-top box for a certain purpose always wastes the bandwidth. CAS standard adopts separate hardware such as smart cards and POD (Point Of Deployment) modules, and the necessity of such hardware results in service charge increase in general, and thus more burden to subscribers. As well as inner problems of CAS, the fact that CAS is an access controlling solution to transmitting channels for contents causes difficulties of directly responding to such functions as pure VOD (video on demand) and PVR (PVR (Private Video Recording) under the environment of IP network. In this regard, the POD module structure defines contents protection functions to some extent, but in the end, the basic problems are not solved since it is focused on only transmitting channel protection.

Especially as for hard disk contents storage, the advanced service of IPTV, illegal copy prevention and access control have yet to be provided. Management of safety keys to consistently manage saved contents and payment and authority control of various services such as VOD should be first dealt with in relation to IPTV service security [6, 13].

2.2.2 DRM

DRM (Digital Right Management) is a technology used to manage intelligent property of digital contents in Internet-based environment. To prevent illegal copy, data encryption of digital contents and license for certified users and terminals are required in controlling contents. License includes authority on contents and decryption keys. Only when the requirements for use are met, decryption is executed. By protecting the whole process through Tamper Resistance technology, illegal leak of contents by hackers is prevented.

Since DRM is a technology developed for Internet and PC based contents distribution, this is a contents protection technology suitable for IPTV service. Originally, this aimed to prevent contents illegal copy online, and thus CAS functions are presentable only with DRM as for IPTV services. Not only available are various payment methods such as subscription, PPV, VOD, Usage Metering, Prepay, Post Pay etc., but also cost-saving effects by excluding POD module or smart cards are outstanding as well. The modification and upgrade of security related modules mounted in a set-top box as well as the management of the key and authority of saved contents are very convenient because of the basic structure of DRM. In existing broadcasting systems, the leak through intermediate distribution channels was always possible, but DRM enables End-to-End Content Protection from the contents provider and end user, which is one of the most outstanding advantages. When there is no return path to apply for license issue, however, DRM as well needs ECM (Entitlement Control Message)/EMM function just as CAS [6, 14].

2.3 Bilinear pairing

Bilinear pairing is a problem in discrete mathematics about ellipses that was simplified by reducing it to a discrete logarithm of a finite field. It was originally proposed as a map that attacks a conventional crypto-system. Recently, an encryption map for information protection was used, instead of an attack map, so, Bilinear Pairing is equivalent to a Bilinear Map. The following terms are used as stated in this paragraph and this theory is defined below [11].

Characteristics that satisfy an Admissible Bilinear map are as follows.

- Bilinear: Define a map $\hat{e} = G_1 \times G_1 \to G_2$ as bilinear if $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ where all $P, Q \in G_1$, and all $a, b \in Z$.
- Non-degenerate: The map does not relate all pairs in $G_1 \times G_1$ to the identity in G_2. Observe that since G_1, G_2 are groups of prime order, this implies that if P is a generator of G_1, then $\hat{e}(P, P)$ is a generator of G_2.
- Computable: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P, Q \in G_1$.

Based on the bilinear premise, the following definition was constructed.

$$\begin{aligned}\hat{e}(aP, bQ) &= \hat{e}(P, bQ)^a = \hat{e}(aP, Q)^b \\ &= \hat{e}(P, Q)^{ab} = \hat{e}(abP, b) = \hat{e}(P, abQ)\end{aligned}$$

From this premise, for ellipses, the D-H (Diffie-Hellman) decision problem can be easily solved via the following equation.

$$\hat{e}(aP, bQ) = \hat{e}(cP, P) \Rightarrow ab = c$$

Therefore, the following is the basis for resolving the difficulties of the bilinear premise that is used as an encryption tool by many encryption protocols. When elements G_1, P, aP, bP, cP (BDHP, Bilinear Diffie-Hellman Problem) are given, this refers to $\hat{e}(P, P)^{abc}$ calculation problem. This problem can be solved if the ellipse curve discrete mathematics problem can be solved. For example, a can be calculated from aP, then $\hat{e}(P, P)^{abc}$ can be calculated through $\hat{e}(bP, cP)^a$.

2.4 Security threats and requirements

IPTV is a brand-new service combining the Internet and broadcasting. All risks in terms of security in existing Internet and broadcasting services remain, and some of them as for the subscribers are as follows.

2.4.1 Security threats

Security threats in IPTV include as follows:

- Personal information security exposure: there are possibilities that personal information security exposure through illegal access of a third party such as identification information and payment related information results in monetary loss to subscribers.
- Masquerade: a malicious third party may be disguised as a legal subscriber through a communication channel that is not secure, and receive authentication and services. Thus, security should be secured regarding such illegal access.
- Session hijacking: session hijacking is a way of attack detour an authentication procedure to a server or a system. First, an attacker blocks the user from accessing to a session in such ways as DoS attack, and then steals the session to a server to acquire the access authority without log-on. Not only sessions but also all information

exchanged between the server and user could be tapped through hijacking [5].

- Data tapping: Since the data transmitted via a communication channel may be exposed to an attacker, the possibilities to analyze confidential information even when a third party acquires data should be removed to prevent tapping attack.

2.4.2 Security requirements

Basically, the following security requirements should be taken into consideration:

- Confidentiality: the data used in communication should be recognizable only by legitimate users. Attackers must be prevented from noticing the source of data, destination, time, length, traffic characteristics of communication channels, etc. Confidentiality is secured through encryption preventing information analysis.
- Integrity: Data saved in an information system or transmitted through a network must be protected from falsification. When the data are falsified, deleted, or altered, the fact should be confirmable. Such ways as electronic signature are used to notice illegal modification of transmitted data.
- Authentication: it is vital to secure confidentiality in authentication services. The source of messages and electronic documents transmitted by a user, and whether the identification is false should be confirmable.
- Access control: Access authority over all reading and modification of resources should be clearly confirmed so as to prevent any unauthorized access. The access controlling level could be heightened by utilizing invasion preventing systems in networks and access controlling functions in operating systems. Besides, unauthorized users cannot use services.

3 Related work

This section describes existing KERBEROS authentication, mobile commerce schemes as well as their characteristics and advantages/disadvantages.

3.1 Kerberos

Kerberos uses the centralized authentication server and its encryption method uses the symmetric encryption for the authentication. So as the user to get the service, the user receives the ticket-granting ticket issued from the authentication server and service-granting ticket from the ticket granting server. The user should remember a password agreed in advance for accessing to each of Kerberos member. The current Kerberos protocol is developed from version 4 to version 5 and it is standardized to IETF RFC 4120 [8]. In this case, the Kerberos protocol has a weak point in password and ticket granting server distributes the session key so that the anonymity and privacy are not offered as it can reveal the message information transporting between the user and service providing server. Also, it has a problem generating the delay while requesting the authentication as Kerberos server is divided into authentication server and ticket granting server.

3.2 Authentication mechanism for anonymity and privacy assurance

This research designed a more efficient authentication mechanism by using the EAP-TLS authentication method and the Symmetric-Key Key Establishment scheme so the user gets provided various services through the Internet. The suggested mechanism provides SSO (Single-Sign On) service, user anonymity and privacy as the contents provider affiliated to the authentication server can use the service without a separate login process when the user gets the authentication from the AAA server through the authentication method. When the user uses the services requiring anonymity, it secures the anonymity of the user and exchanges the session key for the secure data transport between the user and content provider, without exposing it to the authentication server. It secures the user privacy as each content provider uses a different session key [7].

3.3 Mobile commerce AAA mechanism

Wireless LAN is rapidly becoming a crucial component in next-generation mobile communication. Despite this success, there are user privacy and access control issues such as authentication problems and accounting and billing problems. Especially in the accounting field, research about packet accounting based on IP is insufficient, thus, several ISP's adopted a fixed-sum accounting system. This paper presents a packet accounting model in AAA mechanism compatible with international standards of mobile commerce and the verification results [4]. However, the disadvantage is that the payment confirmation and recharge must proceed via a separate process and the home authentication server and billing server overhead may increase.

4 Subscriber authentication technology for mobile IPTV service offer

As to subscriber authentication technology to provide mobile IPTV services, Fig. 1 describes that in a home network environments, the device receives authentication from the home authentication server, receives the authorization ticket,

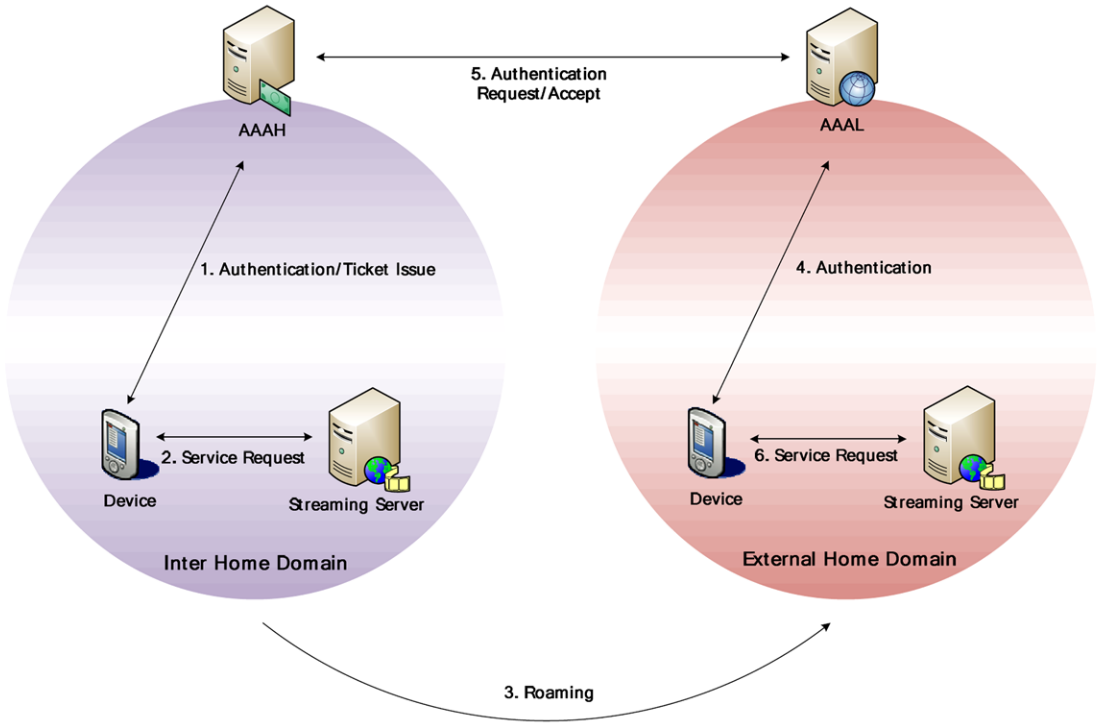

Fig. 1 (Color online) Whole flowchart

presents the authorization ticket to the home network service, and receives IPTV services. In addition, when the device uses IPTV services by another service provider, the authorization ticket issued by the inner home domain of the foreign home is provided, the authentication is given, and services are presented.

4.1 System parameters

The system parameters used in this scheme are as follows.

- *: Objects (D: Device, $AAAH$: Home Network Authentication Server, $AAAL$: Foreign Network Authentication Server, *Streaming Server*: IPTV Streaming Server)
- ID_*: Identification of *
- OTP: One-time password
- g: Generator with order $n-1$ in Z_n^*
- $h()$: One-way hash function
- CT: Synchronization counter value
- $e: G_1 \times G_1 \rightarrow G_2$ Bilinear map
- $E_*[\,]$: Encryption with key of *
- $Sign_*$: Signature of *
- KS: Shared symmetric key between D and $AAAH$
- *service_key*: Shared service key between $AAAH$ and *Streaming Server*
- KU_*: ID-based public key of *
- KR_*: ID-based private key of *

4.2 Proposed protocol

Proposed protocol consists of the IPTV device authentication and authorization issues phase in the home network, and the IPTV device authentication phase in foreign network. It is supposed that the symmetric key between the device and home network authentication server is distributed ahead of time.

4.2.1 IPTV device authentication and authorization ticket issue phase

When the device requests the home network authentication server to present authentication, the authentication server issues the proper authorization ticket, and transmits the authorization ticket and ID to the streaming server. The device presents the authorization ticket to use mobile IPTV services. Figure 2 shows the procedure IPTV device authentication and authorization ticket issue protocol.

Step 1. IPTV device generates OTP after XOR operation and hash of the serial number and symmetric key, and generates ID based private key/public key pair. To request the authentication, the device's ID, home authentication server ID, OTP and counter are encrypted by symmetric keys and transmitted.

$$OTP = h(PIN \oplus KS \oplus CT)$$

$$KU_D = ID_D$$

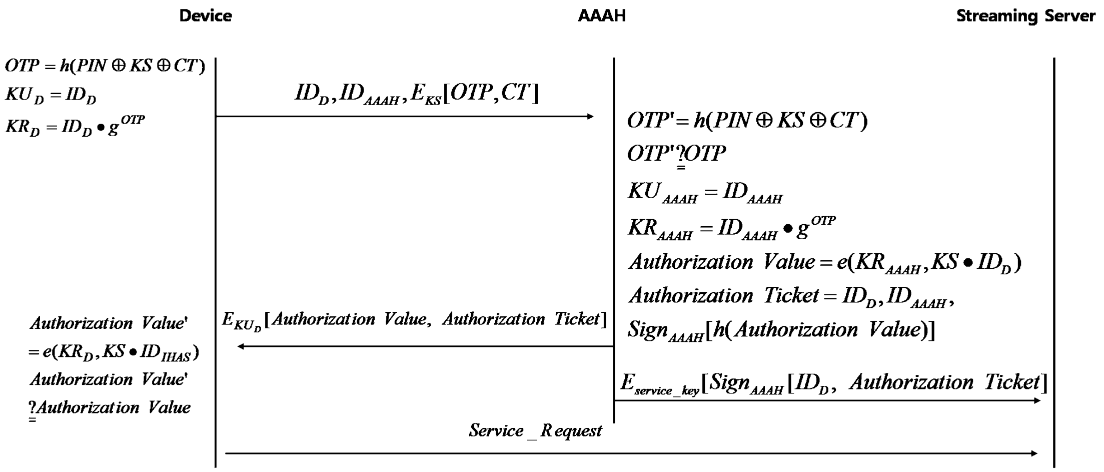
Device
AAAH
Streaming Server
OTP = h(PIN ⊕ KS ⊕ CT)
KU_D = ID_D
KR_D = ID_D • g^OTP
ID_D, ID_AAAH, E_KS[OTP, CT]
OTP' = h(PIN ⊕ KS ⊕ CT)
OTP' ?= OTP
KU_AAAH = ID_AAAH
KR_AAAH = ID_AAAH • g^OTP
Authorization Value = e(KR_AAAH, KS • ID_D)
Authorization Ticket = ID_D, ID_AAAH,
Sign_AAAH[h(Authorization Value)]
E_KU_D[Authorization Value, Authorization Ticket]
Authorization Value' = e(KR_D, KS • ID_IHAS)
Authorization Value' ?= Authorization Value
E_service_key[Sign_AAAH[ID_D, Authorization Ticket]
Service_Request

Fig. 2 IPTV device authentication and authorization ticket issue phase protocol

$$KR_D = ID_D \bullet g^{OTP}$$
$$ID_D, ID_{AAAH}, E_{KS}[OTP, CT]$$

Step 2. The home network authentication server generates OTP based on the values transmitted and saved in the database, and compares them with OTP sent by the device for authentication. Upon completion of authentication, the private key/public key pair are generated based on the ID of the home network authentication server, the authorization values and authorization ticket are generated and then encrypted through the device public key, and finally transmitted.

$$OTP' = h(PIN \oplus KS \oplus CT)$$
$$OTP \underset{=}{?} OTP'$$
$$KU_{AAAH} = ID_{AAAH}$$
$$KR_{AAAH} = ID_{AAAH} \bullet g^{OTP}$$
$$Authorization\ Value = e(KR_{AAAH}, KS \bullet ID_D)$$
$$Authorization\ Ticket = ID_D, ID_{AAAH}$$
$$, Sign_{AAAH}[h(Authorization\ Value)]$$
$$E_{KU_D}[Authorization\ Value, Authorization\ Ticket]$$

Step 3. The device certifies the values transmitted by the home network authentication server, especially the acquired private key, home network authentication server ID, and symmetric key, by means of Admissible Bilinear Map.

$$Authorization\ Value' = e(KR_{AAAH}, KS \bullet ID_D)$$
$$Authorization\ Value \underset{=}{?} Authorization\ Value'$$

Step 4. The home network authentication server encrypts the device ID and authorization ticket through the service key shared with the streaming server, signatures on them, and then broadcasts them.

$$E_{Service\ key_{AAAH-Streaming\ Server}}[Sign_{AAAH}[ID_D$$
$$, Authorization\ Ticket]$$

Step 5. The device presents the ticket to the home network service, the home network service certifies the ticket, and then provides the device with services.

4.2.2 IPTV device authentication phase in foreign network

In this step, for the device to move to foreign network and use mobile IPTV services, the foreign network authentication server is given the authorization ticket issued by the home network authentication server for authentication and providing services (refer to Fig. 3).

Step 1. The device encrypts the authorization ticket issued by the home network authentication server by means of the public key of the home network authentication server, and transmits to the foreign network authentication server with the ID.

$$ID_D, ID_{AAAH}, E_{KU_D}[Authorization\ Ticket]$$

Step 2. The foreign network authentication server transmits the values from the device to the home network authentication server, the home network authentication server certifies the authorization ticket, signs on the authorization ticket for services, and then transmits it to the foreign network authentication server. The foreign network authentication server broadcasts the ticket to the foreign streaming server.

$$E_{KU_{AAAH}}[Authorization\ Ticket]$$
$$Access\_Accept, Sign_{AAAH}[Authorization\ Ticket]$$
$$E_{Service\ key_{AAAH-Streaming\ Server}}[Sign_{AAAL}[ID_D$$
$$, Authorization\ Ticket]$$

Step 3. The device presents the ticket to the foreign streaming server, and then the streaming server certifies it, and prevents services to the device.

5 Analysis

The proposed methods are analyzed according to the general security requirements in Sect. 2, security requirements against attacks, and security requirements in different networks. Table 1 presents the analysis result.

5.1 Security threats analysis

- Personal information security exposure: Personal information of users may be exposed by illegal access or hacking of a third party, which can cause monetary loss. Thus, to prevent leak of personal information, data on a transmitting channel should be encrypted, and the authentication and authorization information should be managed in a form of a ticket to minimize the revealing of personal information.
- Masquerade: A third party may disguise himself as a legal user, and receive authentication or services. Thus, OTP is used, and the information is encrypted through ID based public key/private key pairs to protect it from masquerade.

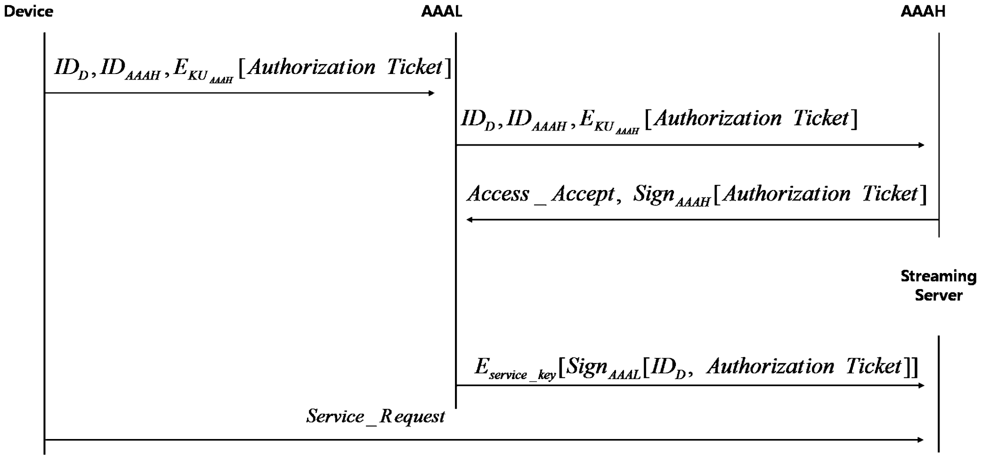
Device
AAAL
AAAH
$ID_D, ID_{AAAH}, E_{KU_{AAAH}}[Authorization\ Ticket]$
$ID_D, ID_{AAAH}, E_{KU_{AAAH}}[Authorization\ Ticket]$
$Access\_Accept,\ Sign_{AAAH}[Authorization\ Ticket]$
Streaming Server
$E_{service\_key}[Sign_{AAAL}[ID_D,\ Authorization\ Ticket]]$
$Service\_Request$

Fig. 3 IPTV device authentication phase protocol in foreign network

Table 1 Analysis of proposed scheme

	Kerberos	Authentication mechanism for anonymity and privacy assurance	Mobile commerce AAA mechanism	Proposed scheme
Confidentiality	Symmetric key	Public key and symmetric key	Symmetric key	Symmetric key and ID-based public key
Integrity	Non offer	Implicit integrity offer	Hash function	OTP and authentication
Authentication	Shared password	EAP-TLS	Challenge-response	Using OTP and Ticket
Access control	Unauthorized device is not accessed			
Personal information security exposure	•	•	•	Ticket
Masquerade	•	•		Signature
Session hijacking	Nonce	Timestamp and lifetime	Nonce and sequence	Counter-based OTP and authorization value
Data tapping	Secure			
Efficiency	Delay of ticket issue	Non offer roaming	Overhead of authentication server and roaming problems	Fast roaming authentication and reduced home authentication server

- Session hijacking: Attackers may acquire access without proper procedures by snapping sessions on the communication channel. They also may steal the session through hijacking and even tap all information exchanged between the server and user. Thus, the time limit for sessions is set through counter-based OTP, and the authentication values are not exposed even when the session is stolen to prevent any risk of hijacking.
- Data tapping: Since the data transmitted through communication channels may be exposed to attackers, to prevent any tapping attack, the secret values should be prevented from analyzing even when a third party acquires the data. In forming the secrete values, the data integrity and confidentiality are secured through hash values.

5.2 Security requirements analysis

- Confidentiality: The data used in communication must be readable only by legal users. The proposed method is the public key/private key pair ($KU_D = ID_D, KR_D = ID_D \bullet g^{OTP}$) based on the symmetric key *KS*) and ID shared between the device and home network authentication server. In each step, encryption secures confidentiality.
- Integrity: Any falsification and destruction of data transmitted through networks or saved in information systems should be prevented. The proposed method uses hash values to secure integrity.
- Authentication: The falsehood of a user should be certified. The proposed method uses synchronization OTP ($OTP = h(PIN \oplus KS \oplus CT)$), and certifies Admissible Bilinear Map based authorization values ($Authorization\ Value = e(KR_{AAAH}, KS \bullet ID_D)$) and authorization tickets to provide certified services.
- Access control: It is necessary to classify the authority over access such as reading and modifying information resources so as to prevent any unapproved access attempt. Any device without authentication cannot be given an authorization ticket as well as foreign network access and services.

6 Conclusion

As IT is rapidly developed, and the Internet and computers are widely distributed, which speeds up the expansion of digital materials and communication infra, image and voice information based on IP network connection are shared, and the demand for integrated services is increasing. In addition, the demand for mobile IP network that provides mobility among users based on the next generation network technology is more and more increasing. However, a number of problems are expected in terms of security on the other side of activation of IPTV services, and security threats will increase in mobile environment. Thus, development of security technology is of importance to provide mobile IPTV services safely and efficiently.

This study includes the investigation on subscriber authentication technologies in AAA mechanism to provide mobile IPTV services, and to present safe, efficient services regarding IPTV services by means of mobile devices. For subscriber authentication, counter-based OTP and Admissible Bilinear MAP based authorization ticket method are used, and even when the service channel is changed from home network to foreign network, the mobile IPTV services are consistently provided by means of authorization tickets. In the future, there should be ways to provide both service analysis and IPTV standards and compatibility through performance evaluation.

Acknowledgements This work was supported by the Korea Research Foundation Grant funded by the Korean Government (MOEHRD, Basic Research Promotion Fund) (KRF-2008-0174).

References

1. Calhoun, P. R., Loughney, J., Guttman, E., Zorn, G., & Arkko, J. (2003). Diameter base protocol. *RFC 3588*.
2. Kim, B.-J. (2001). Next generation authentication protocol DIAMETER AAA technical trend. In *TTA*.
3. Kim, D.-H. (2002). *A Study of Ticket based AAA Service for Mobile IP*. Yonsei: The Graduate School Yonsei University.
4. Kim, G., Lee, C., Park, S., Song, O., & Jung, B. (2003). A study on mobile commerce AAA mechanism for wireless LAN. In *HSI 2003* (pp. 719–724).
5. Kim, H. G., Lee, B. G., Choi, D. H., Yoo, S. K., Kim, M., Lee, H., & Yu, H. J. (2005). On the international standardization of AAA technology. *ETRI Journal*, *20*(1), 123–129.
6. Lee, C.-S., & Park, S.-C. (2007). IPTV content protection technology: CAS and DRM. *KISA Research paper*.
7. Lee, D.-M., Choi, H.-M., & Yi, O. (2005). Design of authentication mechanism for anonymity and privacy assurance. In *Proceedings of the 24rd KIPS autumn conference* (pp. 941–944).
8. Neuman, C., Yu, T., Hartman, S., & Raeburn, K. (2005). The Kerberos network authentication service. *RFC 4120*.
9. Park, J.-M., Bae, E.-H., Pyeon, H.-J., & Chae, K. (2003). A ticket-based AAA security mechanism in mobile IP network. In *ICCSA* (pp. 210–219).
10. Patel, B., & Crowcroft, J. (1997). Ticket based service access for the mobile user. In *Third annual ACM/IEEE international conference on mobile computing and networking* (pp. 223–233).
11. Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In *CRYPTO'84* (pp. 47–53).
12. Vollbrecht, J., Calhoun, P., Farrell, S., Gommans, L., Gross, G., de Bruihjn, B., Laat, C., Holdrege, M., & Spence, D. (2000). AAA authorization framework. *RFC 2904*.
13. Woo, J.-H., Roh, C.-H., & Lee, W.-B. (2006). IPTV content protection technology: CAS and DRM. *Korean Continence Society*, *6*(8), 157–164.
14. Xiao, Y., Du, X., Zhang, J., Hu, F., & Guizani, S. (2007). Internet protocol television: the killer application for the next-generation Internet. *IEEE Communication Magazine*, *45*(11), 126–134.

Jong Hyuk Park received his Ph.D. degree in Graduate School of Information Security from Korea University, Korea. From December, 2002 to July, 2007, Dr. Park had been a research scientist of R&D Institute, Hanwha S&C Co., Ltd., Korea. From September, 2007 to August, 2009, he had been a professor at the Department of Computer Science and Engineering, Kyungnam University, Korea. He is now a professor at the Department of Computer Science and Engineering, Seoul National University of Technology, Korea. Dr. Park has published about 100 research papers in international journals and conferences. He has been serving as chairs, program committee, or organizing committee chair for many international conferences and workshops. He was editor-inchief of the International Journal of Multimedia and Ubiquitous Engineering (IJMUE), the managing editor of the International Journal of Smart Home (IJSH). He is Associate Editor/Editor of 14 international journals including 8 journals indexed by SCI(E). In addition, he has been serving as a Guest Editor for international journals by some publishers: Springer, Elsevier, John Wiley, Oxford Univ. Press, Hindawi, Emerald, Inderscience. His research interests include security and digital forensics, ubiquitous and pervasive computing, context awareness, multimedia services, etc. He got the best paper award in ISA-08 conference, April, 2008. And he got the outstanding leadership awards from IEEE HPCC-09 and ISA-09, June, 2009.