http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 10 (11): 2044-2051, 2011
ISSN 1812-5638 / DOI: 10.3923/itj.2011.2044.2051

Secure Migration Service for Mobile IPTV using DCAS

Aymen Abdullah Alsaffar and Eui-Nam Huh
Kyung Hee University, China

Abstract: In this study, we provide a secure migration services for MIPTV using DCAS. DCAS is known as downloadable conditional access system and it is used to download conditional access (DCAS code) software to user mobile so they get authenticated and authorized to receive MIPTV services (e.g., video, audio, data, etc). We use session manager to manage and monitor multicast stream. Furthermore, allowing user to conveniently switching between access networks with less delays (e.g., Wifi, UMTS, etc). The proposed mechanism allows user to securely migrate their mobile devices using DCAS. Therefore, provides a strong security to user mobile and protect multimedia from being compromised. The provided security will overcome the security vulnerabilities that might accrue in the migration process.

Key words: Mobile IPTV, DCAS, secure migration, multimedia contents, session manager, AAA authentication

INTRODUCTION

In the present, Internet Protocol Television (IPTV) services are increasingly receiving a tremendous interest by user now-a-days. In order for IPTV provider to extend their services to mobile user, a mobile IPTV (MIPTV) services have to be offered for mobile user devices to receive MIPTV services anytime anywhere in the world.

MIPTV is known as Mobile Internet Protocol TV which is a technology that enables users to transmit and receive multimedia traffic including television signal, video, audio, text and graphic services. However, it is inconvenient for consumer to turn-off one device such as mobile devices and then turn-on another device such as STB to watch their programs in one hand. In another hand, in wireless environment, mobile user has to be secured from well known attacks such as Denial of Service attack (DoS), replay attack and man-in-the-middle attack. In addition, multimedia content must be protected from being compromised or misused when wireless network environment is used. To overcome these vulnerabilities and provide mobile user with a feasible, fast secure methods to receive MIPTV services, a secure migration services for MIPTV using DCAS is presented in this study. The Migration process will solve the problem where the user switches between different devices and terminals (e.g., Wifi, 3G, etc). Downloadable Conditional Access System (DCAS) is used to prevent unauthorized or uncharged user from receiving MIPTV services after receiving DCAS code (also known as CA Client image) which will be unique for each mobile user, stored in their devices and updated whenever it is needed.

RELATED WORK

Downloadable conditional access system in MIPTV security system: DCAS is known as downloadable conditional access system. DCAS is an advanced technology to deliver securely the software code (DCAS code) for key management of CAS to a customized chip in a DCAS host such as microprocessor chip which it can replace a current hardware-base CAS module (Borza and Al-Hawtin, 2008). The downloadable CA code via the secure DCAS network is supposed to be unhackable and it can prevent illegal subscriber from accessing digital content. The protocol defines a series of messages to be transferred between a DCAS headend (service provider side) and DCAS host such as STB or mobile user. Some of DCAS advantage is more cost-effective and easier to deploy, more flexible and easier to manage and distribute CAS module through a secure channel. Another one is it can be applied to a variety of devices including a secure microprocessor chip and it can be updated online in case the previous DCAS code being hacked (Borza and Al-Hawtin, 2008).

Session manager: Session Manager (SM) is used for multicast session control and monitoring. It manages all user-to-content and content-to-user relations. Furthermore, manages all media server signaling that necessary to deliver a demanded content to consumer or mobile user and provide session mobility (Riede *et al*., 2007). It keeps information of what the user have been viewing, time of viewed program or show. Thus, user are not only able to move across a variety of access networks

Corresponding Author: Aymen Abdullah Alsaffar, Kyung Hee University, China

but also able to suspend session from one access network and resume it on another (e.g., UMTS xDSL, WiFi etc) (Guyot *et al*., 2005).

Authentication, authorization and accounting procedures (AAA): When mobile user migrate their devices from one network area such as wifi at home to another one such as 3G outside, mobile user need to be re-authenticated and authorization by the visited network area (i.e., wifi, 3G) to use the resource in that area. A mobile IP defines a method that allows a mobile user to change its point of attachment to the internet with minimal services disruption (Glass *et al*., 2003). However, Mobile IP alone cannot provide the necessary support for mobility across different network which limit the applicability of mobile IP in a large scale. AAA protocols such as diameter precisely enable users to roam and obtain service in networks that may not necessarily be owned by their home services provider. For mobile IP to be deployed in networks there has to be AAA support for the protocol (Glass *et al*., 2003).

Authentication mechanisms for user mobile devices: Here we will describe previously used authentication mechanisms for users such as Kerberos, EAP-TLS, Wireless Transport Layer Security (WTLS) and their advantages and disadvantages (Alsaffar *et al*., 2010). In addition, we will provide a comparison between our proposed authentication mechanism and previously used authentication mechanism to authenticate mobile user.

Kerberos authentication mechanism: In a distributed denizens, Kerberos is well known authentication mechanism which it uses a third party authentication server that enable users and servers to trust each other and therefore, a securely communication established between them. A symmetric encryption for authentication is used to encrypt (Alsaffar *et al*., 2010). However, it has two drawbacks; firstly, the user may have access to workstation where he/she can pretend to be anyone (Alsaffar *et al*., 2010). Secondly, a user can eavesdrop on messages exchanges and use a replay attack to access the server. In previously, Kerberos mechanism was used as authentication. Due to its vulnerability in security issues, it does not provide a strong security features against the security issues mentioned previously.

Authentication mechanism for anonymity and privacy assurance: The combination of Extensible Authentication Protocol Transport Layer Security (EAP-TLS) authentication and symmetric key (PKI) are well known authentication mechanism which enable the user with a various methods of receiving internet services. User anonymity, privacy and Single Sign On (SSO) is provided as a unique feature where content provider affiliated to the authentication server can receive service without signing more than once when user authenticated by Authentication, Authorization and Counting server (AAA) (Alsaffar *et al*., 2010). To secure the user identity and provide the user with feasible way to exchange session key to acquire secure data transportation between user service providers, anonymity is used through the service.

As a result, exposition it to authentication server is not necessary. Furthermore, the security of TLS is considered as a strong. However, there is an overhead of client side certificate which does not make it a strong mechanism (Alsaffar *et al*., 2010). Single Sign On (SSO) is a mechanism where user sign on once and have unlimited access to many resources when initially authenticated. The drawback of this feature is that it increases the negative impact in case the credentials are available to other persons and abused. Thus, the rapidly required focuses on the protection of the user credentials give its weakness (Alsaffar *et al*., 2010).

Wireless transport layer security (WTLS): It is a well known security protocol which designed for securing communications and transactions over wireless networks (Kwak *et al*., 2002). The main objective of the WTLS layer is to provide feature such as confidentiality, data integrity and authentication between two wireless communication applications. However, its handshake has several drawbacks as an Authentication and Key Agreement (AKA) protocol for mobile networks along with an end to end problem which is a WLTS architectural problem. There is an exposure of user certification and lack of forward secrecy in handshake which make it the focus of current study. Forward secrecy (Kwak *et al*., 2002) is one possible security feature provided by key establishment protocol which is concerned with dependency of a common session key on a secret key. Forward secrecy promises to keep the common session keys established in the protocol runs from being compromised even if the discloser of a secret key to an adversary is occurred. Nevertheless, in the WLTS handshake message flow, the user certificate is send to the server without encryption or another cryptographic scheme. As such, if a passive attacker takes the certificate from the air-interface, he can figure out the user information using certificate. Furthermore, if the long term secret keys are disclosed, the pre-master secret will be revealed in the client key exchange message and the master key will be revealed before the finish message (Kwak *et al*., 2002). Thus,

handshake does not satisfy the features of user anonymity and forward secrecy which will provide a weak authentication.

SECURE MIGRATION SERVICE FOR MOBILE IPTV USING DCAS

Here, we provide three phases of a secure migration services for mobile IPTV using DCAS. We provide general system architecture as shown in Fig. 1. In addition, we provide system sequence diagram for other phases as well. Table 1 illustrates the notation used in this study.

Table 1: The system parameters

Notation	Description
M_{ID}	Mobile identification
M_{LIC}	Mobile license
STB_{ID}	Set-top box identification
STB_{PW}	Set-top box password
STB_{LIC}	Set-top box license
U_{INFO}	User information
U_{SI}	User session
U_{RC}	User request content
$Nonce_{M}$	Mobile generated nonce
$Nonce_{STB}$	Set-top box generated nonce
$DCAS_{CODE}$	Downloadable conditional access system code
$DCAS_{CEK}$	DCAS code encryption key

Registration phase: In this phase, the mobile user is registering their mobile devices in order to receive Mobile IPTV services via STB or 3G. We are assuming that the mobile user has already applied to receive IPTV service at home. Therefore, in this phase we are only registering user mobile to be able to receive Mobile IPTV service.

System architecture: Here, we will briefly describe the system architecture in Fig. 1. The mobile user will migrate their device to their home STB via Access Point (AP). The STB will forward the user request to Service Provider (SP). SP consist of DCAS, SM and SS. SP will forward mobile user request to Trust Authority (TA) where mobile user are registered, authenticated and their information are stored. After completion of registration, DCAS in SP will receive user information from TA and generate Mobile license, encryption key and DCAS code which will be send to mobile user after it is encrypted with the generated key. The license will be stored in user mobile along with the generated encryption key. When user wishes to receive MIPTV service, it will send request with mobile license to DCAS in SP, DCAS will compare it with the one stored in TA, validate it and then send request to Session Manager (SM). Session Manager sends request to Content Server (CS) where the content will be prepared

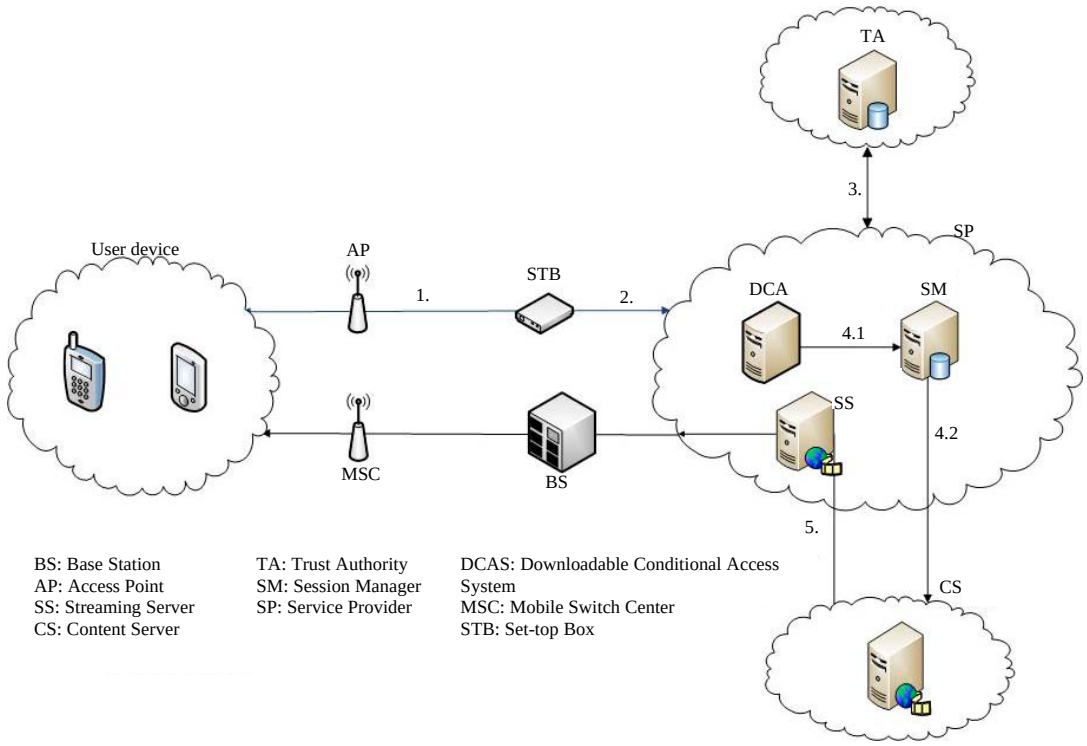

Fig. 1: Registration phase of secure migration services for mobile IPTV using DCAS

and forward to Streaming Server (SS). Streaming Server will stream the requested encrypted content to user mobile via STB or 3G where it will be decrypted and viewed.

The following components of system architectures are defined in this study:

- **User devices:** The user mobile device will have a smart card (USIM) which contains information about the user such as identification, password and user license (Foster and Kesselman, 1999)
- **Access point (AP):** It provides access for devices to connect to STB
- **STB:** It will also have smart card (USIM) provided by service provider. USIM will have information about the user such as identity, password, encryption and content viewing rights
- **Trusted authority (TA):** It will register and store information about the user mobile
- **Downloadable conditional access system (DCAS):** It will provide user devices with CA software which grant them the right to view MIPTV content. It will generate encryption key to encrypt the CA software before send to user mobile. Entitlement Management Message (EMM) and Entitlement Control Message (ECM) also send to user mobile. EMM will have entitlement key which will be used to decrypt ECM which has the Control Word where it is used by user mobile to scramble the video and finally view it
- **Session manager (SM):** It is used for multicast session control and monitoring. It manages all user-to-content and content-to-user relationship. Furthermore, manages all media server signaling that is necessary to deliver a demanded content to demanding user (Guyot *et al*., 2005). It will also provide user with feasible way to switch between different terminals and continue watching their program from where they left
- **Content server (CS):** It prepares the requested contents, encrypt them and send them to Streaming Server
- **Streaming server (SS):** It receives the encrypted contents from the Content Server and stream it to user mobile device or STB (Foster and Kesselman, 1999)

When a mobile user request MIPTV services using DCAS for the first time to be viewed in their mobile devices, user has to apply for the services. In details, the user will register their mobile device to receive MIPTV services. The user migrate their devices to STB via Access Point (AP) by sending $\{M_{ID}|STB_{ID}|STB_{PW}|Nonce_M\}$.

The STB will forward the same information to Service Provider where user registration will be established. Then, Service Provider send $\{M_{ID}|U_{INFO}\}$ to Trust Authority (AT) to be registered, authenticated and stored. TA send $\{M_{ID}|U_{INFO}\}$ to DCAS in Service Provider. Here the DCAS will issue a mobile license, generate DCAS code encryption key, Encrypted DCAS code and send $\{M_{LIC}|E(DCAS_{CODE}|DCAS_{CEK})\}$ them to user mobile. The mobile license will state that this user have this privilege to receive this services. The DCAS code key encryption will be generated between DCAS and user mobile where it will be used by user mobile to decrypt DCAS code when it is received. The DCAS code and key will be stored in user mobile memory. Base in DCAS, the user mobile will receive DCAS code whenever it is needed for the user mobile. Furthermore, user mobile will receive Entitlement Management Message (EMM) and Entitlement Control Message (ECM) from DCAS. EMM will have Key of Entitlement will be used by user mobile to decrypt ECM which will have a Control Word (CW). CW is used to scramble the descrambled video and view it. In this way, the mobile user is not only securely authenticated but also the content is protected from compromised or misused by unsubscribed user (Fig. 2).

Second phase (request services at home): We are assuming that mobile user is at home, already have a mobile license, DCAS code encryption key and previously installed DCAS code stored in their mobile.

System sequence diagram: Here, we will briefly describe the system sequence diagram in Fig. 3. To receive Mobile IPTV services, the user send request to DCAS in Service Provider where user received information will be compared to the one stored in TA and validated. Upon the validation, DCAS will send DCAS code to user mobile and the mobile id with user information to Session Manager. Session Manager will send mobile id and user session information to Content Server where requested content are prepared, encrypted and forwarded to Streaming Server. Streaming Server will stream the content to user mobile via STB or 3G where it will be decrypted and viewed.

In details, mobile user send the following request $\{M_{ID}|M_{LIC}|Nonce_M\}$ to DCAS in Service Provider. DCAS will compare it with the one stored in TA and then validate it integrity. If it is valid, DCAS sends the DCAS code to user mobile $\{DCAS_{CODE}\}$. In the same time DCAS send the following information $\{M_{ID}|U_{INFO}\}$ to Session Manager. Session Manager will have current session information of the program or show the user were viewing and send $\{M_{ID}|U_{SI}\}$ to Content Server where the contents

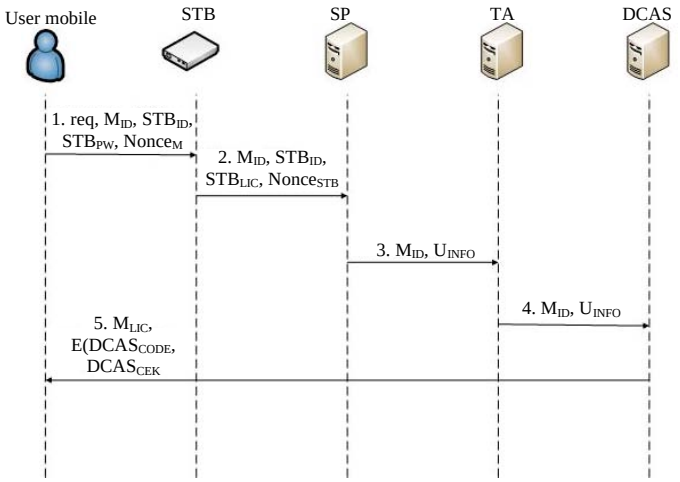

Fig. 2: Secure migration services for mobile IPTV using DCAS procedure

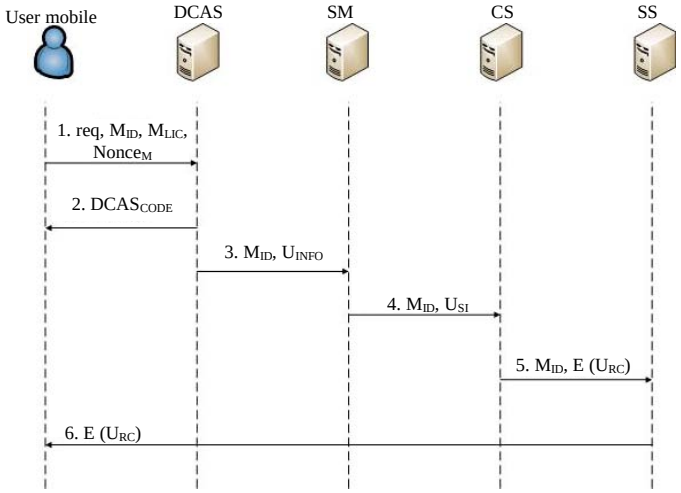

Fig. 3: Second phase of secure migration services for mobile IPTV using DCAS

are prepared, encrypted and then send to Streaming Server $\{M_{ID}|E(U_{RC})\}$. Streaming Server will send the encrypted content to user mobile $\{E(U_{RC})\}$ via STB or 3G where it will be decrypted and viewed.

Third phase (request services at outdoor): We are assuming that mobile user is outside, already have a mobile license, DCAS code encryption key and previously installed DCAS code stored in their mobile.

System sequence diagram: Here, we will briefly describe the system sequence diagram in Fig. 4. To receive Mobile IPTV services, the user send request to DCAS in Service Provider where user received information will be compared to the one stored in TA and validated. Upon the validation, DCAS will send DCAS code to user mobile and the mobile id with user information to Session Manager. Session Manager will send mobile id and user session information to Content Server where requested content are prepared, encrypted and forwarded to Streaming Server. Streaming Server will stream encrypted content to user mobile via STB or 3G where it will be decrypted and viewed. Note that at home the user will have the option to switching or not between different terminals. The closer you are to STB the more likely that you are going to use that method and vice versa.

In details; user send the following request $\{M_{ID}|M_{LIC}|Nonce_M\}$ to DCAS in Service Provider. DCAS will validate the receive information with the stored one in TA. If it is valid, DCAS sends the DCAS code to user

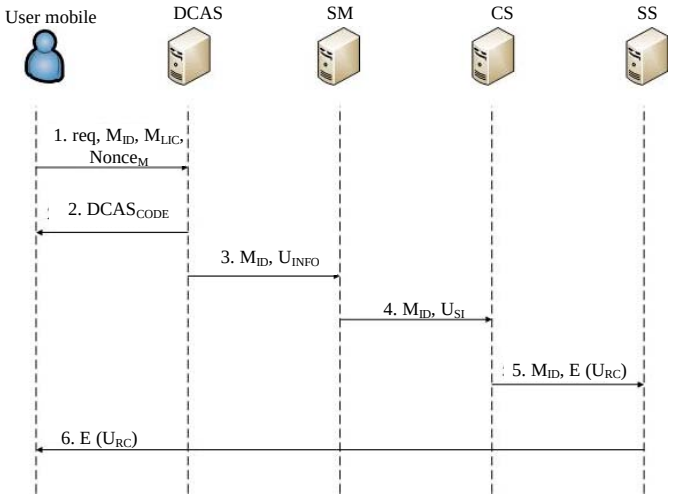

Fig. 4: Second phase of secure migration services for mobile IPTV using DCAS

mobile {$DCAS_{CODE}$}. In the same time DCAS send the following information {$M_{ID}|U_{INFO}$} to Session Manager. Session Manager sends {$M_{ID}|U_{SI}$} to Content Server where the contents are prepared, encrypted and then send to Stream Server {$M_{ID}|E(U_{RC})$}. Streaming Server will send the encrypted content to user mobile {E (U_{RC})} via base station, mobile switch center and finally to user mobile where it will be decrypted and viewed. Note that the difference here is we are using 3G.

PERFORMANCE EVALUATION

Security analysis: Replay attack, Denial of service attack and Man in the middle attack are some of the continuously well known occurring dangerous threats to users and services when mobile user migrate their devices or re-authenticated again to the services. Most attacks against authentication and key distribution protocols are based in capturing messages and replay them in different context or format. These messages could be resend to other recipients than the intended one. Furthermore, they can be repeated in several different protocols or transmission processes. Replay attack and Man in the middle attack are most likely to occurred when user migrate their device to STB (endpoint). Here the mobile user provides user name and password to complete the migration to STB. One way to avoid replay attack is using Nonce which is a random number generated by user mobile and STB when they exchanges messages between each other in order to get authenticated. The random number will ensure that previous communication cannot be used again. It is different each time that the 401 authentication challenge response code is presented, thus making replay attacks virtually impossible. In this message {$M_{ID}|STB_{ID}|STB_{PW}|Nonce_M$}, we did not only use Nonce to prevent replay attack but also we required user to provide their Mobile id, STB id and STB password, therefore, insure the integrity of the message, strengthen authentication mechanism and detect the attack when it occurs where previously mentioned authentication mechanism only considered Nonce or token or time stamp. Denial of service is likely to occur when mobile user try to connect to DCAS in order to receive the DCAS code from DCAS in service provider.

In this message {$M_{ID}|M_{LIC}|Nonce_M$}, we also required the user to provide Mobile id and Mobile License along with the Mobile Nonce, therefore, increasing the possibility of detecting the attack, providing a strong authentication and message integrity. With the combination of Nonce and user information such as (Mobile id, Mobile License, STB id, STB password), it will be very difficult for attack to occur without being detected. Furthermore, DCAS have a system to update mobile user code and to challenge the authentication anytime it is necessary in case an attacker could recover the DCAS code from mobile user and change it to use it in different devices. Thus, the authentication and authorization of user and service is protected.

Communication cost analysis: Here, we will analyze the cost of communication which we obtained when user register and authenticate their devices for the first time and for every time the user completely turn off their devices and then turn it on again. We will compare our communication cost with previous mentioned authentication such as Kerberos and EAP-TLS where we

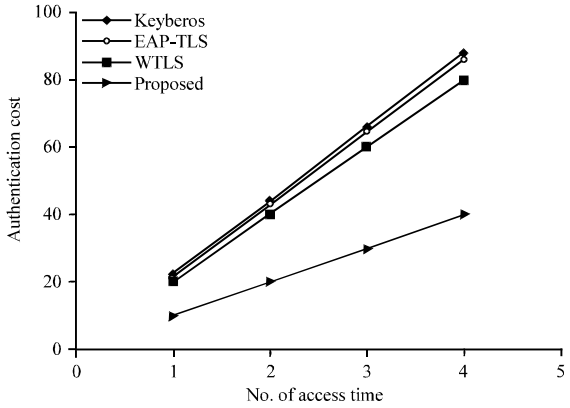

Fig. 5: Accumulated authentication cost vs. Access time of the user

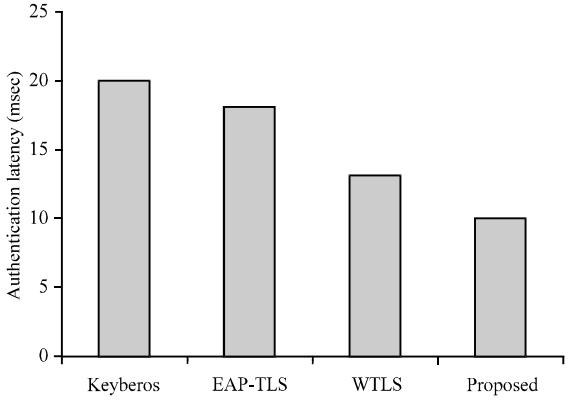

Fig. 6: Authentication latency for each mechanism (msec)

will use the same cost value calculated previously (Alsaffar *et al*., 2010). As for WTLS (He and Lee, 2008) and our proposed scheme we will compute a new cost value for them. Here will calculate the cost by taking the number of message that is necessary for user to register their devices. In each flow chart, we will calculate the cost of exchanges messages. For easy understanding, we substituted the following symbols C_{SP_LP}, C_{LP_CP}, C_{M_SP} and C_{M_CP} with C_{SP_TA}, C_{TA_DCAS}, C_{M_S}, (Mobile to Server) and C_{DCAS_U}, respectively. Table 2 illustrates the estimation cost of each authentication mechanism based on the number of messages exchanged in each authentication process and finally comparing them to each other.

As you can see, there is increased improvement in our proposed authentication process when we compared with other. This can be explained by the number of fewer messages that are exchanged in our proposed.

Numerical result: In the numerical result, our evaluation will be based on the analysis which we mentioned in previous section. Based on the number of messages that

Table 2: The estimation cost of authentication process

Kerberos	EAP-TLS	WTLS	Proposed scheme
22	21.5	$C_{M\_S}(8) = 20$	$C_{U\_STB}(1)+C_{STB\_SP}(1)+C_{SP\_TA}(1)+C_{TA\_DCAS}(1)+C_{DCAS-U}(1) = 10$

exchanged in each authentication process, we produce an accumulated estimation cost. In Fig. 5, we are assuming that the number of time user is going to switch between different networks, the user will have to turn off one device completely and then turn it on again. As a result, the numbers of times the user access the system multiply by the cost of authentication for each time the user authenticated. This calculation will be done as well as for other authentication process in order to compare with our proposed mechanism.

In Fig. 5 the number of messages that are exchange in our proposed is less than others and in Fig. 6. our proposed show lowest delay (10 msec) when it comes to user authentication than Kerberos (22), EAP-TLS (21.5) and WTLS (20). As a result, it did not only reduce the cost of user authentication but also decrease the delay time which result from number of exchange messages when user get authenticated or switch between different networks where they needed to re-authenticate again. Furthermore, the less number of messages are exchange in authentication, the better optimize the usage of radio resources which enhance the efficiency of user authentication. Figure 6 represent a bar graph that shows the delay comparison for Kerberos, EAP-TLS, WTLS and our proposed mechanism. As you can see our proposed shows better performance and less delay compared to other.

CONCLUSION

In this study, we proposed a secure migration services for mobile IPTV using DCAS. To ensure a secure migration services from mobile IPV using DCAS, our proposal was designed to consider the following process in order to provide strong security against the security threats we mentioned earlier. Also provide the user with convenient methods to switch between terminals without the trouble of turn off one device and then turn on another device. Furthermore, to provide security to protect the content and the services, a DCAS code is downloaded from DCAS to user mobile after generating a secure key between DCAS and user mobile. This process will be considered as a way of authentication user devices after decrypting the code with the generated key. Our mechanism decreases the user authentication cost and reduce the delay which occur in the process. Therefore, meeting the security requirements mentioned previously.

ACKNOWLEDGMENT

This research was supported by the MKE (The Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National IT Industry Promotion Agency)" (NIPA-2011-(C1090-1111-0001)).

REFERENCES

Alsaffar, A.A., T.D. Nguyen, Y.R. Shin and E.N. Huh, 2010. Secure migration of IPTV services from a STB to mobile devices for pay per view video. Proceedings of the 6th International Conference on Digital Content, Multimedia Technology and its Application, Aug. 16-18, IEEE Computer Society, Seoul, pp: 91-97.

Borza, M. and Al-Hawtin, 2008. The future of open cable systems: Conditional access migrates to DCAS. Information Quarterly, Vol. 7. http://www.iqmagazineonline.com/IQ/IQ23/pdfs/IQ23_pgs60-63.pdf

Foster, I. and C. Kesselman, 1999. The Grid: Blueprint for a New Computing Infrastructure. 1st Edn., Morgan Kaufmann Publisher, San Fransisco, ISBN-10: 1558604758, pp: 675.

Glass, S., T. Hiller, S. Jacobs and C. Perkins, 2003. Mobile IP authentication, authorization and accounting requirements. IETF. http://www.ietf.org/rfc/rfc2977.txt

Guyot, V., N. Boukhatem and G. Pujolle, 2005. Smart card performances to handle session mobility. Proceedings of the 1st IEEE and IFIP International Conference in Central Asia on Internet, Sept. 26-29, IEEE Press, Central Asia, pp: 5-5.

He, Y.J. and M.C. Lee, 2008. Improving WTLS security for WAP based mobile e-commerce. Wireless Pers. Commun., 51: 17-29.

Kwak, D.J., J.C. Ha, H.J. Lee, H.K. Kim and S.J. Moon, 2002. A WTLS handshake protocol with user anonymity and forward secrecy. Proceedings of the 7th CDMA International Conference on Mobile Communication, Oct. 29-Nov. 1, Seoul, Korea, pp: 219-230.

Riede, C., A. Al-Hezmi and T. Magedanz, 2007. Quadruple play-session management enabler for multimedia streaming. Proceedings of the 16th Mobile and Wireless Communication Sunmit, July 1-5, Budapest, pp: 1-5.