[ ICCCI 2010 ] 학회 확인서

개최일자: 2010년 11월 10일
개최장소: 대만 Kaohsiung

- 주관기관: TACE
- 참 가 국: 5개국 이상 참여
- 총 발표논문: 155 건
- 발표자중 외국기관 소속 외국인: 50% 이상

2단계 두뇌한국(BK)21사업 참여대학원생 학술대회 실적 인정기준
[ 과학기술(융합 및 학계간 융합)분야]에 의거 해당 학회는 위와
같음을 확인합니다.

---국제학술대회 실적인정기준---

▶ 해외지명학회 주관(국내학회와 공동주관 포함)한 4개국 이상(한국포함)이 참여한 학술
대회도시. 총 발표논문이 50건 이상이어야 하며 전체 발표논문 중 외국인(외국기관 소속)
논문이 50% 이상

2011. 4.
사업팀장 홍중선

2단계 BK21 미래 커버전스 서비스 플랫폼 연구 사업팀
### ARToolkit-Based Augmented Reality System with Integrated 1-D Barcode: Combining Colorful Markers with Remote Servers of 3D Data for Product Promotion Purposes

*Jong-Chih Chien, Hoang-Yang Lu, Yi-Sheng Wu, and Li-Chang Liu*

**Table of Contents – Part III**

**Innovative Information System and Application**

- ARToolkit-Based Augmented Reality System with Integrated 1-D Barcode: Combining Colorful Markers with Remote Servers of 3D Data for Product Promotion Purposes
  
  Jong-Chih Chien, Hoang-Yang Lu, Yi-Sheng Wu, and Li-Chang Liu
  
  Design and Implementation of e-Journal Review System Using Text-Mining Technology
  
  Chun-Wei Tseng, Feng-Jung Liu, Wan-Chin Lu, and Shih-Hao Huang
  
  Study on Architecture-Oriented Information Security Risk Assessment Model
  
  Wei-Ming Ma
  
  Constructing Problem-Based Learning Activities Using Self-assessment System
  
  Feng-Jung Liu, Chun-Wei Tseng, and Wen-Chang Tseng
  
  Conducted EMI Analysis of a Three-Phase PWM Rectifier
  
  Kezxin Wei, Bin Liang, and Youjun Yue
  
  Synchronization of Duffing-Holmes Oscillators Using Stable Neural Network Controller
  
  Suwat Kuntanapreeda
  
  Codes Base on Unambiguous Products
  
  Ho Ngoc Vinh, Vu Thanh Nam, and Phan Trung Huy

### Intelligent Computing for Networks

- A Study on the Topology Control Method for Bluetooth Scatternet Formation
  
  Chih-Min Yu
  
  A Study on the Global Configured Method of Blueweb Routing Protocol
  
  Chih-Min Yu
  
  Energy Efficient Framework for Mobility Supported Smart IP-WSN
  
  Md. Motaharul Islam, Nguyen Tien Dung, Aymen Abdullah Al Saffar, Sang-Ho Na, and Eui-Nam Huh
  
  An Efficient Migration Framework for Mobile IPTV
  
  Aymen Abdullah Alsaffar, Tien-Dung Nguyen, Md. Motaharul Islam, Young-Rok Shin, and Eui-Nam Huh
An Efficient Migration Framework for Mobile IPTV

Aymen Abdullah Alsaffar, Tien-Dung Nguyen, Md. Motaharul Islam, Young-Rok Shin, and Eui-Nam Huh

Department of Computer Engineering
Kyung Hee University, Suwon, Korea
{aymen,ntiendung,shinyr,johnhuh}@khu.ac.kr,
motahar@icns.khu.ac.kr

Abstract. In this paper we present an efficient migration framework for mobile IPTV services. We present a secure migration for their devices when user migrates to receive MIPTV services for the first time, indoor and outdoor migration. In addition we use Conditional Access System (CAS) and Digital Right Management (DRM) to protect MIPTV service and digital content.

Keywords: MIPTV Services, CAS, DRM, Framework, Migration, Digital multimedia.

1 Introduction

In the progressive development of super-high speed broadband network and advancing of mobile devices capabilities, consumers are capable of connecting to the internet through Wifi Access Point or 3G to receive multimedia content and services. Mobile Internet Protocol TV (MIPTV) one of the services that are receiving tremendous demand by user in these days. MIPTV is technology that enables users to transmit and receive multimedia traffic including television signal, video, audio, text and graphic services through IP-based wired and wireless network [1]. MIPTV service providers are increasing their effort to provide diversity of services to user at home and to mobile devices while they are on the move. The recent development of STB that include wifi capability, make it possible for MIPTV provider to provide services [2]. However, wireless network environment has threats such as denial-of-service attack (DoS attack), replay attack, and man-in-the middle attack. Therefore, we proposed an efficient migration framework for mobile IPTV services to provide consumer with secure connection when migrating to MIPTV services. In addition, we explain the role of Conditional Access system (CAS) and Digital Right Management (DRM) in the MIPTV services. The rest of this paper is organized as follows. Section 2 related work. Section 3 proposed efficient migration framework for mobile IPTV services. Section 4 performance evaluation and lastly, section 5 the conclusion.

2 Related Work

2.1 CAS and DRM Role in MIPTV Security System

In present, multimedia such as video, data or voice have been digitalized and uploaded to the internet so consumer can have access to it anywhere anytime. One of this digital
content that has a demand is known as MIPTV content. In order to protect unauthorized access of MIPTV services and digital content, Conditional Access System is used to ensure only subscribed member can receive services. And digital right management (DRM) will ensure the right of digital content is not been violated in anyway.

Conditional access system (CAS) is used to preventing non-subscriber from receiving the services [3]. There are three main functions: scrambling and descrambling, Entitlement Control Message (ECM), and Entitlement Management Message (EMM). There are two main concepts to be considered. The first one is entitlement which known as authorization. In scrambling, the information is transformed to make it unreadable to anyone except the one who possess away of descrambling it by a given key [3]. In this way, CAS will protect the business and the profit of charge broadcasting services provider. Several researchers proposed many techniques of CAS which are suitable to protect their business.

DRM is used to protect and manage the user right of digital content such as editing, copying or reproducing. The implementation of DRM will establish a protocol between user and service provider in how the content can be used. However, a variety of standardization efforts associated with certain aspects of DRM have been recently initiated including the Open Mobile Alliance (OMA), Open Digital Rights language (ODRL), MPEG-21, and Coral Consortium [12]. Yet, these efforts and the field of DRM itself are at an early stage of development, therefore a viable open DRM architecture has yet to emerge.

2.2 Authentication Mechanisms for User Mobile Devices

Here we will describe recently used user authentication mechanisms such as Kerberos, EAP-TLS and their advantages and disadvantages. Furthermore, we compare them to our proposed authentication mechanism.

2.2.1 Kerberos Authentication Mechanism
Kerberos is an authentication mechanism that is used in a distributed environment. It uses a third party authentication server that allow users and servers to trust each other and therefore securely establish communication. Kerberos works by encrypting data by using symmetric encryption for the authentication [4, 5].

For instant, when a user needs to access a service server (SS), he/she need two tickets to get authenticated to SS. A ticket granting ticket (TGT) received from authentication server (AS). The user will send TGT to ticket granting server (TGS) to prove identity. A user will receive second ticket from TGS and therefore access SS. The disadvantage is the user may have access to workstation and pretend to be someone else [5]. For its weakness in security issues, it is vulnerable against above mentioned security issues.

2.2.2 Authentication Mechanism for Anonymity and Privacy Assurance
The authentication mechanism uses Extensible Authentication Protocol Transport Layer Security (EAP-TLS) authentication and Symmetric key (PKI). It provide feature such as single sign on (SSO), privacy, and user anonymity as the content provider affiliated to the authentication server can use service without the need for a separate sign on process when the user get authenticated by Authentication, Authorization and Counting (AAA) server [4]. Using the services through anonymity
will secure the user anonymity and provide easy way to exchange session key to obtain secure data transportation between user and service provider. However, the overhead of client side certificate is it deadly weakness [4].

3 Proposed Migration Mechanism of Secure MIPTV Services

In this section, we provide mobile user with three methods of a fast and secure migration of their mobile devices to receive MIPTV services through STB with wifi access point or 3G. In the process of migrating user mobile devices we securely authenticating consumer to receive MIPTV services. Table 1 gives description of system parameters used in this scheme.

Table 1. The System Parameters

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDM</td>
<td>Mobile ID.</td>
</tr>
<tr>
<td>ID_PW</td>
<td>Mobile ID password.</td>
</tr>
<tr>
<td>LicM</td>
<td>Mobile generated license.</td>
</tr>
<tr>
<td>STB_N</td>
<td>Set-top box number.</td>
</tr>
<tr>
<td>STB_ID</td>
<td>Set-top box id.</td>
</tr>
<tr>
<td>STB_PW</td>
<td>Set-top box password.</td>
</tr>
<tr>
<td>STB_Lic</td>
<td>Set-top box generated license.</td>
</tr>
<tr>
<td>Nonce_M</td>
<td>Random number of user mobile.</td>
</tr>
<tr>
<td>Nonce_STB</td>
<td>Random number of user STB.</td>
</tr>
<tr>
<td>Nonce_SP</td>
<td>Random number of service provider.</td>
</tr>
<tr>
<td>D_Nonce</td>
<td>Random number of Kerberos server.</td>
</tr>
<tr>
<td>Nonce</td>
<td>Random number of Kerberos client.</td>
</tr>
<tr>
<td>E_CT</td>
<td>Digital content encrypted.</td>
</tr>
</tbody>
</table>

3.1 Initial Phase to Migrate Mobile Devices to STB through Wifi Access Point

In this initial phase we assume the user did not register to receive MIPTV services through their mobile devices. The user only has the services to be watch through STB at home. Therefore, we will use initial phase to register and authenticate user mobile for the first time through wifi access point to home STB which store user STB license that they receive from license provider when they applied for MIPTV services. By connecting their mobile devices to their STB through wifi access point or STB with built-in wifi technology [2] and providing their STB license, they are securely authenticated by service provider. See figure 1 for a brief explanation. This basic architecture was introduce in our previous work [13].

Fig. 1. Initial phase process to migrate mobile devices to STB through wifi access point
The following components of this system architecture are defined in this paper:

- **User Mobile Devices**: will have a USIM that contain information about the user such as identification, password, and user content license, etc.
- **Wifi Access Point (AP)**: provide wifi access point between STB and users devices at home.
- **Set-top box (STB)**: will have USIM that contains information about STB such as id, password, license and other information.
- **Service Provider (SP)**: provide MIPTV services to user mobile devices base station or to home STB through wifi access point.
- **Database (DB)**: Will store all consumers received information& update them.
- **License Provider (LP)**: Generate a license for home STB or mobile devices user. The license will identify user and provide user with MIPTV services.
- **Content Provider (CP)**: The content provider will prepare the requested digital content based in the agreed license between mobile user and content provider.

![Diagram](image_url)

**Fig. 2. Initial phase process of migrating mobile devices to STB though wifi access point**

When the mobile user request MIPTV services through the user devices such as mobile device, the process is as follow (see figure 2):

**Authentication Process**: to watch MIPTV programs using mobile device, a request send through wifi access point to STB at home to migrate their devices to STB followed by mobile generated random number (NonceM). User STB request from mobile devices the following information such as \{ID_M \mid STB_N \mid STB_ID \mid STB_PW\} followed by mobile and STB received random number (NonceM, NonceSTB) to authenticate the user mobile device to access user STB at home.

- Mobile user send request \{Req \mid Nonce_M\}.
- STB request \{ID_M \mid STB_N \mid STB_ID \mid STB_PW \mid Nonce_M \mid Nonce_{STB}\}.
- Mobile user send \{ID_M \mid STB_N \mid STB_ID \mid STB_PW \mid Nonce_M \mid Nonce_{STB}\}

The STB received the requested information and compare it with the one stored in STB smart card (USIM). If it is valid, then transmit it to service provider. Otherwise, send an error message to mobile device through STB or base station.

**Registration Process**: When the STB complete mobile user authentication and migration to STB, it transmits \{ID_M \mid STB_N \mid STB_{Lic}\} to service provider. The service
provider processes the registration and a request will be forward to database and to the license provider to generate a new user mobile license.

- \{ID_{M} \mid STB_{N} \mid STBLic\}.

License Generation Process: When a license provider receives \{ID_{M} \mid STB_{N} \mid STBLic\} from service provider, it will generates another license for \{Lic_{M}\} and forward one copy to content provider and user STB and then to user mobile.

- \{ID_{M} \mid Lic_{M}\}.

Content Transmit Process: The content provider receives a license from license provider for mobile device (Lic_{M}). Then prepare the digital content, encrypt it (ECT) and transmit the requested program to user mobile through STB or base station.

### 3.2 Indoor Phase to Migrate Mobile Devices to STB through Wifi Access Point

In the indoor phase, we assume the user is at home watching program, but he/she want to suddenly go out but still want keep watching their program. The process of migrate devices to STB through wifi access point is less than before. We assume that the mobile user already have a mobile license in their mobile device.

Migrate to STB Process: Mobile user connect to STB through wifi access point. User send request to STB to watch the program through mobile device followed with mobile user random number (Nonce_{M}). The STB request \{ID_{M} \mid Lic_{M}\} followed with random number (Nonce_{STB}). The mobile user forwards the requested information to STB and compares \{ID_{M} \mid Lic_{M}\} and forward request to content provider.

- Mobile user send request \{Req \mid Nonce_{M}\}.
- STB request \{ID_{M} \mid Lic_{M} \mid Nonce_{M} \mid Nonce_{STB}\}.
- Mobile user send \{ID_{M} \mid Lic_{M} \mid Nonce_{M} \mid Nonce_{STB}\}.

Content Transmit Process: The content provider request a copy of user mobile information from user STB such as \{ID_{M} \mid Lic_{M}\}. If they are valid then prepare and encrypt content to provide services to user mobile. Therefore, the mobile user receives digital content and enjoy while they are indoor. If not valid, an error message will be send through STB or base station to user mobile.

### 3.3 Outdoor Phase to Migrate Mobile Devices through Base Station

In the outdoor phase, the MIPTV user want to receive the MIPTV services without connect their devices to STB at home. We assume that the mobile user already has a mobile license that allow user to receive MIPTV services through base station. When user comes home and still wants to watch MIPTV services privately, depending in how close they are to STB or base station they will receive MIPTV services. Therefore, users will have flexible methods to switch their devices indoor to outdoor and vice versa.

Authentication Process: Outdoor user request MIPTV services followed by mobile generated random number (Nonce_{M}) to service provider through base station. Service provider requests \{ID_{M} \mid Lic_{M}\} followed by generated random number from user
mobile and compare them. If valid, content provider sends MIPTV services to user mobile devices. Otherwise mobile user receive error message through base station.

- Mobile user send request \{Req | \text{Nonce}_M\}.
- Service provider request \{ID_M | \text{Lic}_M | \text{Nonce}_M | \text{Nonce}_SP\}.
- Mobile user send \{ID_M | \text{Lic}_M | \text{Nonce}_M | \text{Nonce}_SP\}.

Content Transmit Process: The content provider receives a request from service provider includes \{ID_M | \text{Lic}_M\}. Then the contents are prepared and encrypt. Finally, transmit it to user mobile to be watching it.

4 Performance Evaluation

4.1 Security Evaluation

The system performance evaluation is based on security aspects, communication cost and handover latency. In the process of migrating mobile devices with other devices through wireless communication, a secure authentication and authorization is essential security issue. In the process of authenticating the user, a security threat might occur such as; Denial-of-service attack: occurs when the server is cheated by an attacker to update the false verification information for the next login phase [6]. Man-in-the middle: is a form of active eavesdropping where the attacker becomes the middle man in the communication between two users A and B [6].

Most of these security threats try to access user computers while users are communicating with each other. As a result, the privacy and security is compromised. A cryptographic Nonce is used between consumer mobile devices and STB to prevent threats. It is a pseudo-random or random number issued in an authentication protocol to make sure that old communication cannot be used in above mentioned security threats [8][9]. The nonces are different every time that 401 authentication challenge response code is presented, and client request has a unique number, therefore preventing other attacks from occurring [8].

4.2 Communication Cost Evaluation

To evaluate the cost of our proposed authentication mechanism, we will compare it with previously proposed authentications mechanism such as Kerberos and EAP-TLS. Therefore, we will calculate the number of message exchange between entities in each authentication mechanism to get the cost efficiency.

4.2.1 Kerberos Authentication Mechanism

First, we will calculate the number of exchange message between entities in order to compute the cost of authentication mechanism [11].

\[
C_{\text{aut,Msg}} = 2C_{M,\text{STB}} + 2C_{M,\text{LP}} + 4C_{M,\text{CP}}
\]  

(1)

We will calculate the cost of exchanged messages between Mobile user and STB, Mobile user and License provider, and Mobile user and Content provider. We would like to mention that \(C_{M,\text{LP}}\) and \(C_{M,\text{SP}}\) have same value of 3.
4.2.2 Extensible Authentication Protocol Transport Layer Security Mechanism (EAP-TLS)

Here we will be using the same method that we used in previous mechanism in order to calculate the cost of exchange messages [10]. In EAP-TLS authentication mechanism the user mobile will request service from STB. The STB will request user mobile id to get authenticated to STB. The user mobile sends id to content provider and to license provider through STB or base station. The license provider receives the client certificate from user mobile. In return the user mobile will receive service certificate from license provider. Then user mobile send session key to license provider and the licenser provider send session key to user mobile. Finally user mobile receive broadcast key and session key from STB.

\[ C_{\text{aut,Msg}} = 3\text{CM}_{\text{STB}} + 1\text{CM}_{\text{CP}} + 5\text{CM}_{\text{LP}} \]  

Here also we will calculate the cost of exchange message between Mobile user and STB, Mobile user and Content Provider and Mobile user and license provider.

4.2.3 Our Proposed Authentication Mechanism

In our proposed authentication mechanism we will calculate the cost of exchange messages between all entities from figure 2.

\[ C_{\text{aut,Msg}} = 3\text{CM}_{\text{STB}} + 1\text{CSTB}_{\text{SP}} + 1\text{CSP}_{\text{LP}} + 1\text{CLP}_{\text{CP}} + 2\text{CM}_{\text{LP}} + 1\text{CM}_{\text{CP}} \]  

In our proposed authentication mechanism, we will calculate the cost of exchange messages between Mobile user and STB, STB and Service provider, Service provider and License provider, License provider and Content provider, Mobile user and License provider and Mobile user and Content Provider (see figure 2).

Using the cost values we can calculate the authentication cost of Kerberos authentication mechanism, EAP-TLS authentication mechanism and proposed authentication mechanism by computing the partial costs of each step of the authentication mechanism. The execution of the authentication mechanism involves the exchange of messages between the entities. For example, the number of messages exchange between mobile users, STB and so on. The same calculation applies for other entities in other authentication mechanism (See table 2). Therefore, based in these values we compute authentication cost in all mentioned mechanisms [10].

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM_{STB}</td>
<td>Mobile to STB</td>
<td>1</td>
</tr>
<tr>
<td>CSTB_{SP}</td>
<td>STB to Service Provider</td>
<td>2</td>
</tr>
<tr>
<td>CSP_{LP}</td>
<td>Service Provider to License Provider.</td>
<td>3</td>
</tr>
<tr>
<td>CLP_{CP}</td>
<td>License Provider to Content Provider</td>
<td>4</td>
</tr>
<tr>
<td>CM_{LP}</td>
<td>Mobile to License Provider.</td>
<td>4.5</td>
</tr>
<tr>
<td>CM_{CP}</td>
<td>Mobile to Content Provider</td>
<td>5</td>
</tr>
</tbody>
</table>

In table 3, we are comparing the authentication cost of exchanged messages between existing authentication mechanism and proposed one. Our proposed authentication mechanism exhibits greater performance in terms of authentication cost, compared to the Kerberos and EAP-TLS authentication procedure. This because
Table 3. Estimation of the Authentication Cost of Kerberos, EAP-TLS and Proposed Authentication Mechanism

<table>
<thead>
<tr>
<th>Kerberos Mechanism</th>
<th>EAP-TLS Mechanism</th>
<th>Proposed Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>2CM_{STB} + 2CM_{LP} + 4CM_{CP} = 31</td>
<td>3CM_{STB} + 1CM_{CP} + 5CM_{LP} = 30.5</td>
<td>3CM_{STB} + 1CM_{STB_{SP}} + 1CM_{SP_{LP}} + 1CM_{LP_{CP}} + 2CM_{LP} + 1CM_{CP} = 26</td>
</tr>
</tbody>
</table>

It includes less security operations and message that are exchanged between the involved entities, compared to Kerberos and EAP-TLS.

5 Numerical Results

Here, we will show the numerical results. First we will show the cost of authentication when we exchange message in the three authentication mechanism. Then we will show the impact of handover latency in Kerberos, EAP-TLS and Proposed authentication mechanism. We define latency as the time it takes a packet to travel from source to destination.

![Fig. 3. Accumulated authentication cost vs. no. of time mobile user access the services](image)

The figure 3 presents the accumulate authentication cost of the exchange messages Kerberos, EAP-TLS and Proposed authentication mechanism when user get authenticated to MIPTV services. We assume that the user is authenticated every time consumer gets access to restart MIPTV services after turn TV off. Therefore, we will use the number of access the user attempt and the cost of each authentication mechanism to show the different of authentication cost.

A side of reducing the authentication cost, our proposed authentication mechanism reduces the computational processing and energy cost at the level of mobile devices. For example, we will assume that number of access time the mobile user attempted was 5 times for proposed authentication mechanism and other authentication mechanism. The accumulated authentication cost for proposed authentication mechanism is 70 and for others 90. As a result our proposed authentication mechanism reduces the computational processing and energy cost by 70% compares to others authentication mechanism. Moreover, the reduced number of messages exchange optimizes the usage of the radio resources enhancing the efficiency of user authentication (see figure 3).
6 Conclusions

In this paper, we have presented an efficient migration framework for Mobile IPTV services. The main challenges facing the migration of MIPTV services from a STB or base station to mobile devices are providing mobile user with a fast, secure authentication and a convenient way of accessing, sharing, communicating and receiving MIPTV services. Our proposed mechanism eliminates the number of repeated authentication steps occurred in migration process. This will enhance the performance of user authentication, since proposed mechanism includes less number of security operation and message that are exchange in between entities in each authentication mechanism. We used cryptographic nonce between mobile devices and STB to prevent threats. A CAS used to protect and allow only charged subscriber to view the services. In addition, DRM was used to protect the digital content rights. In the numerical as a result, we compared our mechanism with other based on messages exchange and handover latency. In our proposed mechanism, cost efficiently and handover latency were less than other mechanism which enhances the service quality of real-time applications of mobile users.

Acknowledgment

This work was supported by the IT R&D program of KCC/MKE/KEIT [Contract number: Consolidation 5010-2010-0056-0058, Development of Open-IPTV Platform Technologies for IPTV Convergence Service and Content Sharing].

References

