Design and Implementation of the UsMSS : User-centric secure Multimedia Service System in Intelligent Home

Jong Hyuk Park\textsuperscript{1}, Sangjin Lee\textsuperscript{2}, Dong Hoon Lee\textsuperscript{2}, Jongin Lim\textsuperscript{2}, In-Hwa Hong\textsuperscript{3}, Laurence T. Yang\textsuperscript{4}

\textsuperscript{1}R\&D Institute, HANWHA S\&C Co. Ltd., \textsuperscript{2}CIST, Korea University, \textsuperscript{3}Korea Electronics Technology Institute, \textsuperscript{4}St. Francis Xavier University

parkjonghyuk@gmail.com, \{sangjin, donghlee, jilim\}@korea.ac.kr, hongih@keti.re.kr, ltyang@gmail.com

Abstract

In this paper, we propose UsMSS (User-centric secure Multimedia Service System) which provides interoperability of multimedia contents among incompatible devices in intelligent home. In addition, an authentication method suitable for the intelligent home is suggested. Furthermore, the proposed system provides intelligent services by reflecting context information (user preference, user location, device status information, etc.) through a sensor network module and home server, providing transparent and secure service.

1. Introduction

Thanks to Ubiquitous Computing, which was first introduced by Mark Weiser of XPARC, nearly all objects and spaces used in our daily lives have become ‘intelligent’. The intelligent environment offers useful services to users through Ubiquitous Computing, which offers unlimited access through interaction that takes place among computers without the recognition of the user [1]. This means that the creation of the Intelligent Home (IH) will be made possible through Ubiquitous Computing. In addition, the area of multimedia services is also likely to face increasing demands for automatic intelligent services that do not require manual commands from the user, customized services, user-friendliness, transparency of use, and interoperability of multimedia contents among incompatible devices. In order to create an environment that makes this possible, it is necessary to develop suitable multimedia security and management, authentication and copyright management measures [2].

In this paper, a UsMSS (User-centric secure Multimedia Service System) is proposed, which has the advantages of providing a suitable authentication method, multimedia interoperability among incompatible devices, transparent services, and security services.

This paper is organized as follows. In Section 2, system requirements for multimedia service of the IH are discussed. In Section 3, system design and implementation are discussed, including architecture, protocol, scenario, and analysis. A conclusion and discussions for future research direction are presented in Section 4.

2. System Requirements in the IH [3, 4]

To offer secure, user-centric multimedia service in the IH, the following requirements should be considered.

- User-friendliness and Transparency: In the IH, a user should be able to handle home devices without difficulty. The intervention of the user should be minimized, and transparency of use should be provided.

- Multimedia Interoperability: In general multimedia services, each device has a fixed resolution, hence requiring multi-formatted resources in order to offer services to incompatible devices. In the IH, however, the interoperability of multimedia contents should be ensured even among incompatible devices.

- Authentication: In the IH, flawless service should be provided by ensuring the reliability of public resources through device authentication, along with existing user authentication process. In order to
achieve this, authentication services such as intelligent device authentication carrying out synchronization, device loss, and robbery prevention are needed.

- **Confidentiality:** Areas that should be considered in order to provide confidentiality in the IH are the development of a low-energy encryption algorithm, key management, computable devices, appropriate use of a symmetric key cipher to reduce the amount of calculations, and the storage and transmission of important information within the IH after encryption, in consideration of the vulnerability of wireless communication network.

- **Integrity:** It is the general practice to verify any alteration of a message being transferred and the information in the receiving device in order to protect integrity of data. However, in the IH, the integrity of devices is more important than that of the message itself. In addition, it is important to prevent forged and counterfeited licences from being used in multimedia services provided in the IH.

- **Availability:** Some of the attacks against availability that should be considered in devices used in a wireless network environment such as the IH are signal disruption, Dos (Denial of Service) and malicious code attacks.

3. **UsMSS**

3.1 **System Architecture**

The proposed UsMSS consists of two parts, as depicted in Figure 1. The front area transmits multimedia contents to the IH, while the back area provides multimedia service using the contents that have been transmitted. In this section, the front area, which is constructed based on [5], is discussed briefly, after which the back section is discussed in detail.

The front area of UsMSS consists of CA, DII-Center, CP, MD and BS. Certificate Authority (CA) issues a certificate to a user. It provides system validation and authentication functions of the user or device. The DII (Digital Item Identifier)-Center generates an identifier, which enables the efficient and systematic management of multimedia contents. In the proposed system, DOI (Digital Object Identifier) is used as the DII. Contents Provider (CP) is a copyright holder that creates secure contents by downloading packager. CP creates digital items by adding metadata that describes the raw multimedia file in the process of packaging, and also establishes usage rules, which regulate the right of usage. Multimedia Distributor (MD) manages secure multimedia files which are distributed by the copyright holder, and provides an interface through which the user consumes the contents. MD consists of CMS and LMS. Contents Management System (CMS) manages multimedia that is safely packaged by the CP. It provides related information by using multimedia metadata. License Management System (LMS) manages licenses used to unlock the user's file lock system in order to play packaged multimedia, and gives a license to the End User when the right payment has been made. Billing System (BS) is a system that processes the payment charge for the acquisition of a license by the End User.

![Figure 1. UsMSS Model](image-url)
transparency of use for the user. The ICMS (Intelligent Context Management System) stores and controls context information collected through a wireless sensor network by the WSN Module into the database. In addition, the ICMS determines the type of multimedia service to be used by receiving the current user status. The HMMS enables interoperability of contents among incompatible multimedia devices by applying a MPEG-21 DIA and real-time video trans-coding in order to offer downloaded multimedia contents in a resolution that has been optimized to each IMCD. Table 1 shows a part of a license that is used to manage copyright by the MSMS, such as setting user rights and delegating authority. The license is shown in a XML format (Refer to Table 1).

Table 1. Part of license for usage rights management

- **End User**: The ‘end user’ refers to a user that has been authenticated through biometric recognition and granted access to the multimedia contents within the IH. An End User always carries a device (mobile phone, necklace, watch, etc.) in which the WSN Module is embedded, sending user context information in real-time to the IHCS.

- **User location recognition**: After the wireless sensor network randomly assigns nodes, the nodes must voluntarily transmit information in response to the user’s environment. In order to do this, it is important to ensure the reliability of location information and data transmission. Existing wireless networks, however, do not support the functionality of transmitting information regarding location recognition and active environments.

In this paper, a recognition algorithm for detecting the location of a moving node is proposed. A node is randomly assigned after measuring the RSSI (Received Signal Strength Indicator) based on a grid-type wireless network. The algorithm for location recognition consists of two parts. One is triangular measurement using RSSI measurements. The other part consists of distance measurements using triangular measurement and the average speed of a moving node. The user location recognition algorithm consists of the following steps: RSSI sampling → Location calculation → Error compensation → Estimation. The advantage of using the triangular measuring method in this process is that a formula regarding the relative distance of the RSSI can be used to convert the RSSI signal into distance measurements. If the distance between each node is identified, it is possible to obtain a relatively exact location with minimal operation by using the triangular measuring method. As a message formatting process consisting of RSSI Request Message and RSSI Reply Message is needed to measure the RSSI, the MAC of the Tiny OS developed by UC Berkeley was applied.

The RSSI is measured by repeatedly transmitting a **RSSI Request Message** and receiving a **RSSI Reply Message** and calculating the RSSI and error values obtained through ten repetitions of this cycle. A message formatting process is then carried out in order to transmit the date to the PC, and values that exceed the error are eliminated in the comparison process. The location of the node can be recognized by comparing converted average node speed and moving distance value in the estimation block.

### 3.3 System Operation Process (Protocol)
The operation process of the proposed system consists of 3 different protocols. The notations in Table 2 are used throughout this paper.

<table>
<thead>
<tr>
<th>Notations</th>
<th>Meanings</th>
</tr>
</thead>
<tbody>
<tr>
<td>E, E'</td>
<td>Distinctive symmetric key encryption algorithms</td>
</tr>
<tr>
<td>r1, r2, r3, r4</td>
<td>Random numbers</td>
</tr>
<tr>
<td>PK</td>
<td>Public key of IHCS</td>
</tr>
<tr>
<td>k</td>
<td>Symmetric key used between user and IHCS for each session</td>
</tr>
<tr>
<td>KEY</td>
<td>Symmetric key pre-shared between IHCS and IMCD</td>
</tr>
<tr>
<td>Cont_Req</td>
<td>Requests for new contents</td>
</tr>
<tr>
<td>Usr_Stat_Info</td>
<td>User context information (user location, contents starting /ending time, additional information on contents, etc.)</td>
</tr>
<tr>
<td>Updating_Cont_Adv</td>
<td>Advertising of newly added contents information</td>
</tr>
<tr>
<td>IMCD Des Info</td>
<td>Information on description of IMCD</td>
</tr>
<tr>
<td>Adapted Multi Service</td>
<td>Adapted multimedia service</td>
</tr>
<tr>
<td>BIO Info / CurrentTime.Date</td>
<td>Biometric information of user (fingerprints, iris, voice, etc.) / Current time and date</td>
</tr>
<tr>
<td>X.Auth / Y_Success</td>
<td>Authentication of X (User, device, etc.) / Success message of Y</td>
</tr>
</tbody>
</table>

### 3.3.1 Authentication Protocol between IHCS and End User / IMCD

Figure 2 represents an authentication process between the PCAS of the IHCS and End User / IMCD. The process consists of 12 steps as follows.

**STEP 1-3.** The user authenticates the IHCS using the IHCS Certificate.

**STEP 4-6.** A process of joint ownership is carried out between the User and IHCS after the session key is generated. This enables the user to use the symmetric key code in stages 7 ~ 9 of the user authentication process.

**STEP 7-9.** The user authentication process is carried out.

**STEP 10-12.** A process of mutual authentication is carried out, using a pre-shared symmetric key between the IHCS and IMCD.

### 3.3.2 Contents delivery Protocol between IHCS and End User

Figure 3 shows the contents delivery protocol between the IHCS and End User. The protocol is followed until the point when the End User downloads the desired contents through the IHCS, and uses the contents after user authentication. The process consists of 6 steps as follows.

**STEP 1.** An authentication method between the User and the IMCD in the IH is carried out, as described in 4.3.1

**STEP 2-3.** The authenticated user requests new multimedia contents through the IHCS. The contents are downloaded to the HMMS through an external line.

**STEP 4-5.** The MSMS of the IHCS manages the copyright of the contents by adjusting user rights such as settings, authorization and management, and the contents are allowed to be played when conditions have been satisfied.

**STEP 6.** In addition to playing contents, context information such as user location, status of the IMCD, information on the multimedia contents, and the starting and ending time of the contents are transmitted to the ICMS of the IHCS for future user-centric services.

### 3.3.3 Contents play Protocol between IHCS and IMCD (or WSN Module)

Figure 4 shows the protocol between the IHCS and IMCD (or WSN Module). The process consists of 6 steps as follows.
3.4 System Implementation and Analysis

In this subsection, the implemented system including environment settings is discussed. Then, the existing system is compared with the proposed UsMSS.

- **Intelligent home and components setting**: To structure an intelligent home, the space is divided into two zones (the size of the living room is set to 4m x 3m, while the bed room size is set to 3m x 2m). Each room is set up with a WSN Module, and the IHCS is installed in the living room. Furthermore, a WSN Module is attached to the IMCDs of each room (DTV with external STB and PDA). The user also carries a WSN Module for location recognition.

- **The implemented WSN Module**: The WSN Module is a communication module based on a 900MHz band to enable wireless communication, and is comprised of MCU Atmega 128 and RF module CC1000. The RF module CC1000 measures the RF signal strength, which it outputs to the RSSI port. The WSN Module also has self-organizing capability. In this experiment, the WSN Module is securely attached to the IMCD via USB (Universal Serial Bus). Figure 5 displays implemented the IHCS and the WSN Module to be attached to IMCD.

Next, the existing system is compared with the proposed UsMSS, followed by a discussion on security implications of the proposed system in case of potential attacks when offering multimedia service in the IH.

The ‘existing system’ refers to multimedia services provided by trial home network service systems provided by S-Com [6] or K-Com [7] consortiums of Korea, in aspiration of realizing the intelligent home.

- **User and device authentication method suitable for the IH**: The existing system uses an officially approved certificate method that employs PKI for user authentication, and the device authentication is carried out through a separate service provider acting as a CA, such as an ISP (Internet Service Provider). However, this method contains problems of decreased speed caused by an increased amount of operations as a result of using a public key method in each session of user authentication, and an additional authentication process executed through the CA whenever a new device is added. Whereas, in the proposed system, user and device authentication are assigned to the IHCS which acts as a subordinated private authentication body that has been authenticated by a preceding authentication body during the initial setting. Efficiency in speed is also enhanced by using a predefined symmetric key method instead of a public key during authentication.

- **User-centric multimedia service**: In the existing system, the user selects the contents to be viewed after downloading or streaming the contents using services provided by the CP to the home environment. Then, the user must command the device to play. Thus, the user’s manual command is required in each execution. However, the proposed system provides a user-centric multimedia service suitable for the IH by enabling automatic execution based on user context information, such as preference and status, without the manual intervention of the user. Of course, a few additional technologies are applied to enable these functionalities, such as context fusion (context DB handling) and data mining.
- **Interoperability among multimedia devices:** While the existing system does offer multimedia services to multiple devices, the contents must be formatted beforehand in order to meet the requirements of each device. In comparison, the proposed system offers multimedia interoperability among incompatible devices using uni-formatted contents, through the use of adapted DI and real-time video trans-coding.

- **Efficiency of user rights management of multimedia contents:** The existing system uses a license system based on XrML for user rights management, which focuses on the security of general online contents. This system has the inconvenience of having to reconnect the user to the main license server through an external line whenever they change user rights between user A and user B. Whereas, in the proposed system, the convenience of the user and as well as efficiency of user rights management can be enhanced by using the license system that is capable of reflecting changes to user rights through the MSMS of the IHCS.

    In the following, various attacks that can be anticipated when offering multimedia services in the IH are discussed, along with security implications of the proposed system against these attacks.

- **Forged and Counterfeited License File Attack:** It is important for the license file to be properly authorized before allowing access of its contents. The security of the system would be at risk if an attacker forges and counterfeits a license file that has been wrongfully acquired. The proposed system prevents forging and counterfeiting of the license file by including a digital signature that has a digest value in the license, as shown in Table 1.

- **IP Spoofing Attack:** W-LAN (Wireless Local Area Network) is generally used in home environments for centrally controlling various devices. The high frequency of the waves used in the W-LAN are a constant security hazard, as it allows access to outside attackers that can bug the system as the frequency travels outside of the walls. As seen in the 3.3 protocol, the proposed system can reduce the risk of spoofing attacks by means of applying an encrypted packet, thus utilizing a symmetric key algorithm for important information packets.

- **Denial of Service (DoS) Attack:** An attacker can send a large amount of useless traffics or transmit radio waves to interfere with the W-LAN connection between the IHCS and IMCD. The proposed system can limit the damage caused by these attacks by authenticating the user and devices on the IHCS, and assigning resources through the IMCD network.

4. **Conclusion**

In this paper, we proposed user-centric secure multimedia service system suitable for intelligent home. The system provides advanced multimedia services which improved from the general multimedia services currently provided in existing home network environments by utilizing context awareness in conjunction with WSN technology. In addition, by resolving the interoperability issue among incompatible multimedia devices within the home network, the new system can adaptively control and identify the suitable resolution for different devices, by using adapted DI and optimized video trans-coding on each device. Furthermore, a method of improving securities, user efficiency, and home device authentication are suggested, increasing the efficiency of user rights management in multimedia in the IH.

Future research should focus on methods to complement and improve the user-centric multimedia services proposed in this study by developing a conjunctive model to enhance protection of user privacy.

**References**


