Mechanism for Sharing Media Content in Multiple Home Network Environments

Jing-Yuan Wu † Daigo Muto ‡ Takumi Koyama ‡ and Tsutomu Yosinaga ‡
Graduate School of Information Systems,University of Electro-Communications
E-mail: {†go, ‡muto, ‡koyama}@sowa.is.uec.ac.jp; ‡yosinaga@is.uec.ac.jp

Abstract: Recently, many DLNA [1] products have entered the market. However, both the UPnP architecture [2] and DLNA guidelines for these products are only applicable to single home networks. We propose a new mechanism for sharing media content in multiple home network environments. We present a Wormhole Device (WD) system based on DLNA and SIP [5] and a Digital Media Controller (DMC) system based on DLNA and implemented on a mobile device. In correspondence with the WD, the DMC locates Digital Media Servers (DMS), Digital Media Renderers (DMR) on multiple home networks, and rends single media content on two DMRs that are deployed in two different home networks synchronously.

Keyword: DLNA , UPnP , SIP , IPsec , Mobile , Synchronous

1. Introduction

we propose a new mechanism for sharing media content in multiple home network environments based on DLNA and SIP. In order to integrate seamlessly with the existing DLNA-based devices in home network environments, we separated the Wormhole Device from the Internet Gateway Device.Wormhole Devices assume the role of SIP user agents and are able to exchange messages through an SIP proxy server. In order to reduce the latency, necessary communications, that is, user authentication and root device summary, are relayed by the SIP proxy server. Considering that high-quality communication cannot be ensured when the status of the network is not stable, we employ a buffer in order to stream the contents in the Wormhole Device. Because communication through the Internet is not protected, it is not very safe to share media content among multiple home networks. In order to resolve the issues involving safety of the media content, the IPsec technique was adopted to encrypt the UPnP data packets; further, the out-of-band transfer among multiple home networks. Our proposed system is shown in Figure 1. In addition, we also developed a DMC on a mobile device that is based on the Linux operating system. It focuses on controlling the DMS and the DMR on home networks. By cooperating with the Wormhole Device, our mobile DMC can browse the contents in the DMS of a remote home network, and playback the selected contents on any DMR of the local home network. Furthermore, we also present a solution based on Wormhole Devices to render single digital media on two DMRs synchronously. And these two DMRsare deployed in two different home networks.

2. Related work

Many researches have been carried out in related areas. W.-S. Liao et al. [7] developed a mobile media server based on a mobile phone platform, which allowed users to render their preferred contents from their mobile devices with small panels to other player devices with large panels in a home network environment. The drawback of their research is that it focused on a single home network.

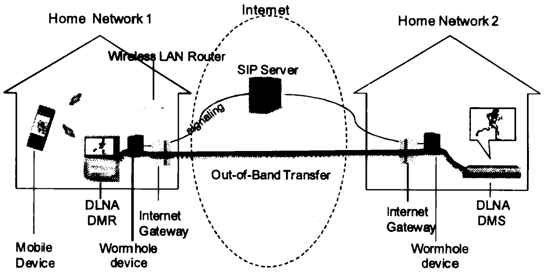

Figure 1. Concept Graphic

Y.-J. Oh et al. [8] developed "DLNA-ALG" on an Internet Gateway Device. It acts as an SIP proxy server and manages the DMS devices. The selected media contents are relayed by the server and can be rendered on the devices that act as the SIP user agent on a public IP network. Their research was focused on accessing DLNA compliant home media from outside the home, but the situation of multiple home networks was not considered. Because determining an SIP server from an SIP user agent in a practical application is impossible. Another drawback is that the DLNA-ALG is only compatible with an Internet Gateway Device with a static global IP address.

A. Vilei et al. [9] developed a VVoIP device, which is a SIP user agent and is able to interoperate with the standard DMS and DMR. The VVoIP device makes it feasible to display the image of the caller on the desired DMR. Users can also send a set of still images or video contents acquired from a DMS in a local area network to their respective conversation partners. However, the VVOIP device did not complicate the NAT traversal. As a result, the VVoIP is only compatible with an Internet Gateway Device; thus, this architecture results in limited flexibility.

S. Motegi et al. [10] developed the W-DLNA, which is based on the SIP and UPnP technique, as an extension of the DLNA for sharing media contents in multiple home network environments.

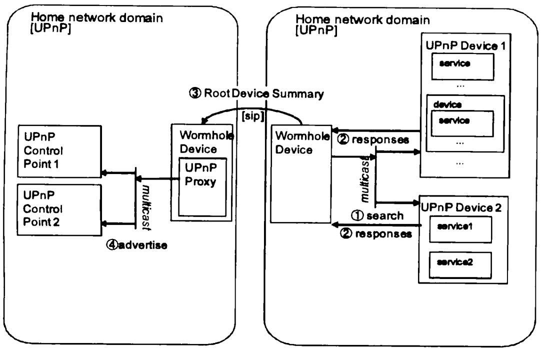

Figure 2. SSDP Packet Transmission

Because W-DLNA is embedded in the Internet Gateway Device, it is difficult to interoperate with the existing Internet Gateway Devices. Another drawback is that the UPnP SOAP actions are forwarded via SIP signaling. As a result, it will enhance the latency in UPnP communication. In addition, as no buffer is used to stream the contents, high-quality communication cannot be ensured when the status of the network is not stable.

3. Background

3.1 DLNA

DLNA uses UPnP as its core technology. The main objective of DLNA is the establishment of a wired and wireless interoperable network of personal computers (PC), consumer electronics (CE), and mobile devices in the home and on the road, enabling a seamless environment for sharing new digital media and content services. DLNA is focused on delivering an interoperability framework of design guidelines based on internationally recognized open industry standards along with a certification and logo program to officially verify and validate the conformance and interoperability of compliant products for the consumers. According to DLNA1.5, the following three Device classes were defined to support the 3-Box System Usage. A DMS assumes the role of exposing and distributing content. A DMR assumes the role of playing back the content it receives after it is setup by another network entity. A DMC assumes the role of finding content transmitted by the DMS and matching it to the rendering capacities of the DMR. Further, the DMC is responsible for setting up the connections between the DMS and the DMR. The 3-Box system usage uses a DMC to browse the content present on the DMS and to select a DMR in order to play-back the selected content. The DMC employs the UPnP to initialize and configure both devices, browses the contents by the media server, and triggers the flow of transmitting content. The media server and the media renderer do not control each other through UPnP actions. However, in order to transfer the content, the media server and media renderer use an out-of-band transfer protocol to directly transmit the content.

4. Design of WD

4.1 System outline

Usually, the UPnP devices can communicate with each other in the same home network environment. As shown in Figure 1, by assuming the role of an SIP user agent, the WD provides a media content sharing mechanism for UPnP devices in different home network environments by connecting to an SIP proxy server.

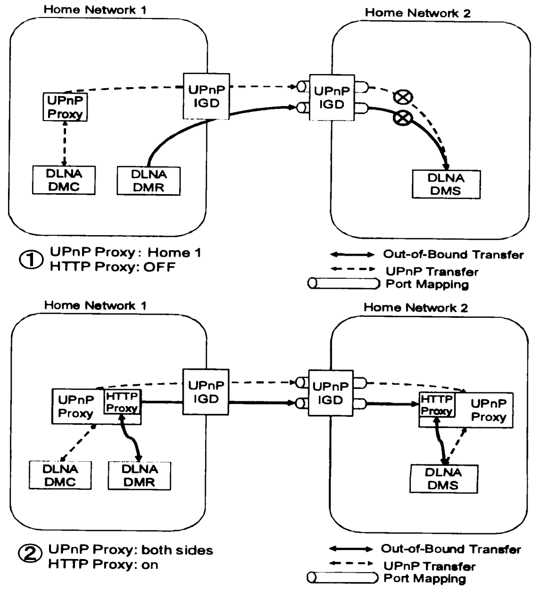

Figure 3. Route Path of UPnP & out-of-band Transfer

The WD provides user authentication and port mapping, manages the information of DLNA devices present in a local home network, and relays the messages among the DMS, DMR, and DMC.

4.2 Technical issue

4.2.1 NAT traversal

Most of the present day internet addresses are IPv4 addresses. Due to the shortage of IPv4 addresses, not all devices can have global IP addresses. The UPnP devices connect to the internet by using NAT traversal. There are two kinds of issues regarding NAT traversal.

a) As a source address, a global IP address cannot correspond with a private IP address; however, a private IP address can connect to the internet through an IGD.
b) When a node with a private IP address sends a packet to another node with a global IP address, the source IP address in the IP header should be considered to verify whether or not the source can be accessed from the global side.

It is possible to resolve the first issue by using port mapping wherein a TCP or UDP port number, which corresponds to the global IP address, is allocated to the device with a private address.

In case of the second issue, before the packet is sent to a global network, the device on the home network acquires a global address of the device with a private IP address. Therefore, the device on the global network side can respond with it by using the converted external IP address.

Adding port mappings and acquiring an external IP address can be performed semi-automatically by using a router supporting the UPnP-IGD. The WD connects with the UPnP-IGD and performs the operations mentioned above. In this way, the NAT issues can be effectively resolved.

4.2.2 Discovering the remote UPnP devices

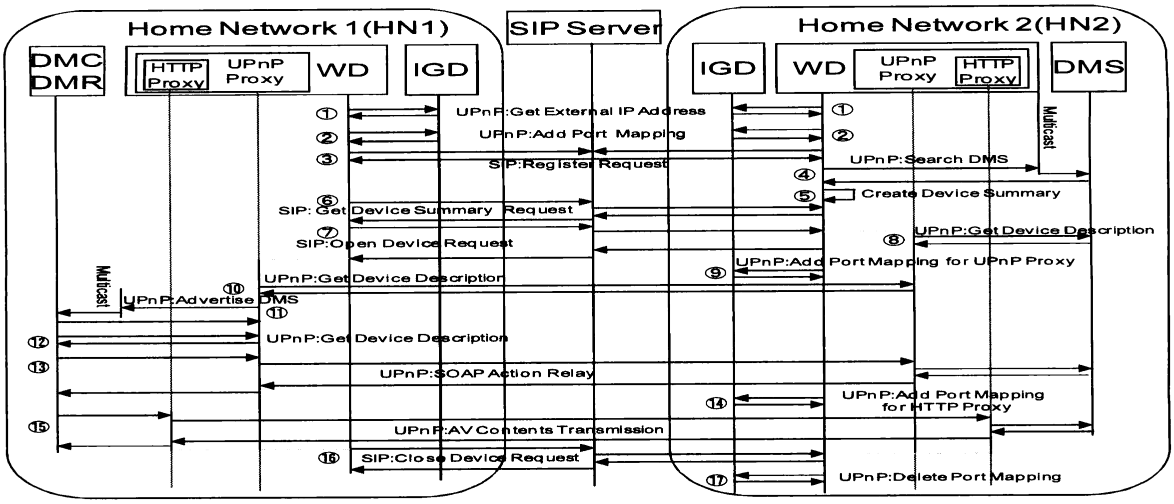

Figure 4. Handling Sequence

SSDP [2] is known as a method of discovering the UPnP devices that exist in the local area network domain. However, SSDP cannot forward a multicast packet to another network, except when the IGD is rebuilt to support that function. Moreover, even if an SSDP packet is forwarded to another network, it operates inefficiently. It should be noted that the private IP address is embedded in the SSDP packet (refer to 5.2.1 b)). Subsequently, it is necessary to find out some other methods besides SSDP. As shown in Figure 2, the WD resolves these issues by using the following methods.

Firstly, the WD in each domain discovers devices in the same domain by using the SSDP. Secondly, the summaries of those devices are created by the corresponding WD. Thirdly, the WDs in different home networks exchange summaries of their devices with each other. Finally, if users decide to access a remote device, a local WD sends a request to a remote WD. If that request is accepted, the UPnP Proxy Process will start up immediately and provide the UPnP device service on the local home network. As a result, the UPnP control points can discover devices mirrored in the local domain using SSDP. Refer to chapter 4.4.4 for a detailed description.

4.2.3 UPnP relay and out-of-band transfer relay

According to DLNA, the communication between the DMS and the DMC is the standard UPnP communication, and the communication between the DMS and the DMR is based on the out-of-band transfer protocol. There are various types of transfer protocols supporting the out-of-band transfer protocol, such as RTP, HTTP-GET, and HTTP-POST. HTTP-GET is adopted by DLNA as a default out-of-band transfer protocol. It should be noted that some DMS products provide security protection by refusing access to all devices from an external network. As shown in Figure 3: ①, neither UPnP nor out-of-band communication is rejected by the DMS. In order to resolve this problem, we develop the UPnP proxy service and the HTTP proxy service as a part of the WD's function to relay these two kinds of communication. As shown in Figure 3: ②, the communications are permitted by the DMS.

4.3 Communication handling sequence

We assume a situation where the users in home network 1 (HN1) wish to access the media contents present in home network 2 (HN2).

4.3.1 Initialization operations

As shown in Figure 4: (1)~(3), when the WDs boot up, they discover the UPnP-IGD and acquire mapped ports and external IP addresses. Then, registration will be successful. Refer to chapters 4.4.1 and 4.4.2 for a detailed description.

4.3.2 Device summary sharing

As shown in Figure 4: (4)~(6), the WD in HN2 creates root device summaries of the devices it discovers and shares these device summaries with the WD in HN1. Refer to chapter 4.4.3 for a detailed description.

4.3.3 Device virtualization

As shown in Figure 4: (7)~(13), the UPnP proxy process virtualizes the DMS's service in HN1. Refer to chapter 4.4.4 for a detailed description.

4.3.4 Out-of-band transfer relay

As shown in Figure 4: (14)~(15), the out-of-band transfer is relayed by HTTP-Proxy on both sides. Refer to chapter 4.4.5 for a detailed description.

4.3.5 End of sharing

As shown in Figure 4: (16)~(17), after the "Close Device" is accepted, the UPnP proxy servers on both sides end the sharing of the selected content immediately, and mapped ports for relaying the UPnP actions and out-of-band transfer are removed.

4.4 Prototype implementation

The WD is developed using ANSI C language on X86 PC-Linux (Fedora Core 6). The compiler is gcc-4.1.1. Portable UPnP SDK 1.4.6, The GNU oSIP library 2.2.2, the eXtended oSIP library 2.2.3, and the partysip SIP proxy server 2.2.3 are employed. There are about 9500 lines of code in the WD.

4.4.1 Communication implementation based on SIP

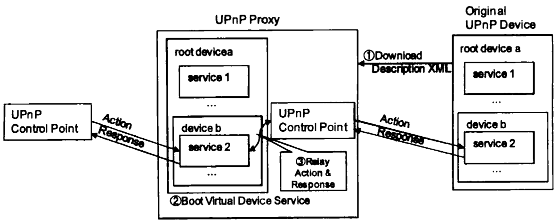

Figure 5. UPnP Proxy Anatomy

The WD transmits the register request to the SIP proxy server in order to communicate with the remote WD. When the SIP proxy server receives an SIP request message, it transmits an SIP response message back to that WD. At this time, the following information about that WD is required.

- Mapped port
- External IP Address

If this information is not provided, the WD cannot receive the response message. Therefore, the WD must send an "Add Port Map" action to the UPnP IGD first to add a new port mapping, following which it must and then send a "Get External IP Address" message to the UPnP-IGD to acquire an external IP address. In addition, during the period of registering to the SIP proxy server, digest authentication is required by the SIP proxy server. The WD uses an authentication name and an authentication password, which are saved in a configuration file, as authentication information.

4.4.2 Implementation of access signaling between the WDs

The SIP proxy server relays messages to the respective WDs in different home networks. The local WD inserts an RPC message in XML into the SIP request message body [6] and sends it to the SIP proxy server. When the remote WD receives the SIP request message relayed by the SIP proxy server, it inserts "200 OK" into the body of the SIP response and transmits it back to the SIP proxy server. The local WD will receive the SIP response message relayed by the SIP proxy server.

The RPC message contains the command name, parameter, return value, error code, and error message.

4.4.3 Implementation of the root device summary exchange

When the WD boots up, it first discovers the UPnP root devices on the local home network using SSDP, and creates root device summaries according to the discovered UPnP root devices. The root device summary includes the following information:

- Unique device name (UDN) of the UPnP Device
- Friend's names
- Device type

The WD packs the root device summary using XML. If WD receives the "GetDeviceSummary" RPC message, it transmits the root device summary back as a reply.

4.4.4 Implementation of the UPnP relay

The local WD transmits the "Open Device" RPC message for sharing a certain remote UPnP device on the local home network. If the local WD receives the "200 OK" response message relayed by the SIP proxy server from the remote WD, the local WD will initialize the UPnP proxy process immediately. The UPnP proxy process downloads the device description XML document, service description XML document, icon files, and so on, from the URL of the remote UPnP device (Figure 5: ①). Subsequently, the UPnP proxy process provides the UPnP device service on the local home network, i.e., the remote UPnP Device is replicated on the local home network (Figure 5: ②). Therefore, if the UPnP Proxy Process receives the UPnP actions from the UPnP control point, it will transmit the UPnP actions to the remote UPnP device keeping the actions intact. Similarly, the UPnP proxy process will transmit the response message received from the remote UPnP device to that UPnP control point keeping the actions intact (Figure 5: ③).

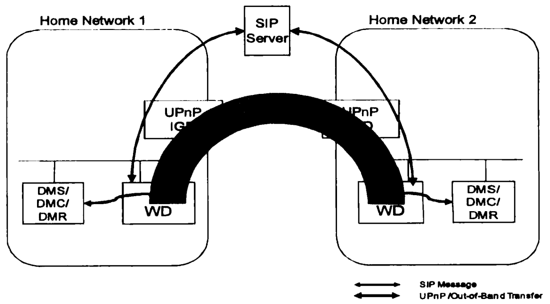

Figure 6. Security Assurance VPN Tunnel

4.4.5 Implementation of out-of-band transfer relay

The transmission of certain content from the remote DMS includes the following steps:

- Obtain the URL of the content
- Transmit that content by using the out-of-band protocol

The UPnP proxy service relays the UPnP communication by adding the operation into it. In particular, the DMC sends the "browse" UPnP action to a content directory service using SOAP. After the UPnP proxy relays the response of the "browse" UPnP action, it replaces the host name and the port number of the content's URL that is saved in the "res" tag. The route path of the out-of-band transfer can be varied by the HTTP proxy by varying the destination URL of the established connection of the HTTP communication.

4.5 Security assurance

4.5.1 Friends list

The WD contains an XML configuration file. This file includes the following content.

- An SIP UID assigned to the WD
- The URL of the SIP proxy server
- An authentication name for the SIP UID
- An authentication password for the SIP UID
- A friend list

When the WD is to be registered on the SIP proxy server, its authentication name and password are requested. In addition, the messages sent from a WD in the friend list will be accepted. Otherwise, the messages will be ignored.

4.5.2 IPsec

The data channel can be protected using IPsec. There are two modes of IPsec operation: transport and tunnel. The tunnel mode is implemented in the WD. As shown in Figure 6, the UPnP transfer and out-of-band transfer are protected by the VPN tunnel.

4.5.3 Contents access control

The WD defines two kinds of access rules, called "accept-based rule" and "deny-based rule". The accept-based rule allows all

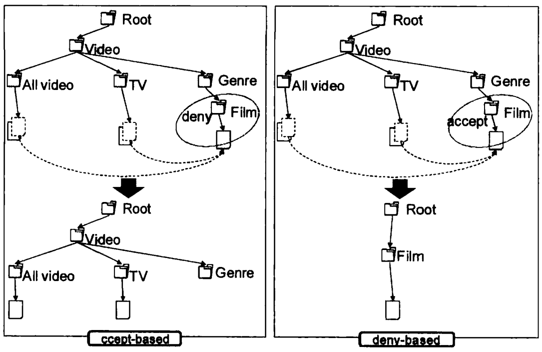

Figure 7. The Contents Access Control

remote WD to access the contents by default, but some containers are not allowed to access for the WD with the SIP UID marked in the rule. The deny-based rule rejects all remote WD to access the contents by default, but some containers are allowed to access only the WD with the SIP UID marked in the rule. The WD modifies the response message of "Browse" UPnP action based on those rules. Therefore, it is able to realize the provision of the contents according to the SIP UID. The image of contents access control is shown in Figure 7.

5. Design of mobile digital media controller

We aim to implement a DMC, which is based on the Linux operating system, on a mobile device. As shown in Figure 8, the mobile device is equipped with wireless LAN. Therefore, it can connect to a wireless LAN router. The DMC acts as a push controller with the role of pushing the URL of the content to a DMR, and then that DMR pulls the content and renders it. In addition, the device is equipped with a touch screen. Therefore, the DMC application can be easily used.

5.1 Design considerations

It should be noted that the target is a mobile device that has limited memory resources. Therefore, its code should be optimized.

Qt, as a C++ cross-platform fully object-oriented application framework, enables the rapid development of GUI applications for multiple embedded Linux platforms. Therefore, we use Qt to develop our DMC GUI application. As the DMC interacts with multiple DMSs and DMRs, it should provide a user-friendly interface. Additionally, in order to avoid confusion, the interface of the DMS should be separated from that of the DMR. Therefore, there are two specific interfaces— the DMS interface and the DMR interface. For the DMS interface, the users can follow the content directory structure of the DMS and browse the contents of a certain DMS.

5.2 Prototype implementation

The DMC is developed using the C++ language on an X86 PC-Linux (Fedora Core 6). The compiler is arm-linux-gcc. We use Qt/Embedded Free Edition 2.3.12 to develop the GUI of the DMC. Portable UPnP SDK 1.4.6 is employed. The target mobile phone is equipped with an ARM 266 MHZ CPU, 32 MB NOR-FLASH, 64 MB NAND-FLASH, 64 MB SDRAM, and CeLinux Kernel 2.4.20 OS. There are approximately 2500 lines of code in the DMC.

The following functions were implemented in the DMC application:

Application	DMC	
Middleware	Qt2.3	
Protocol	UPnP Protocol	
OS	CE-Linux 2.4	
Drivers	Wireless LAN	Touch Screen
CPU	ARM	
Hardware	Wireless LAN	Touch Panel

Figure 8. The Contents Access Control

① Discovering the UPnP devices, i.e., the DMS and the DMR, presenting in the network, and displaying the devices list on GUI of the DMC.

② Browsing the contents in a certain DMS, and displaying the directory structure on the GUI of the DMC.

③ Implementing basic functions for controlling contents, such as "play," "pause," and "stop."

④ The same content can be rendered on multiple DMRs. In addition, we make it flexible to switch the same content on the different DMRs.

⑤ Rending a single media content on two DMRs synchronously, And these two DMRs are deployed in two different home networks.

In order to realize function ⑤, we add new functions to the UPnP proxy of DMR. We designed a new UPnP service named "grouprendercontrol" and add it into the description XML file of DMR proxy. This description file is based on the original description XML file download from DMR. Then create the service description file and install it to the base directory. We call it method based on service. Any DMC in the same network of this proxy will fell that the DMR which is mapped to the local home network can offer a service named "grouprendercontrol". And the DMC can call the functions which are offered by this service through invoking general UPnP action.

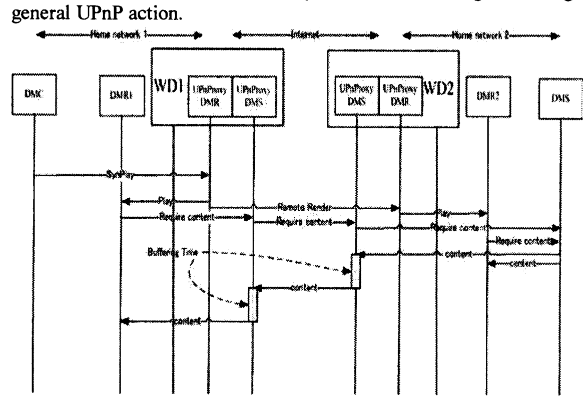

Figure 9. Working Flows of Synchronous Rending

5.3 Working flows of synchronous rending

Considering that high-quality communication cannot be ensured when the status of the network is not stable, we employ a buffer in order to stream the contents in the WD. Because of the buffering of remote media and the transmission of it through Internet, the remote rendering for a media content is a little later than the local rendering.

To overcome this drawback, we should not simply only invoke these two content flows at the same time. If we can calculate the prise time delay between these two flows, we could invoke the local

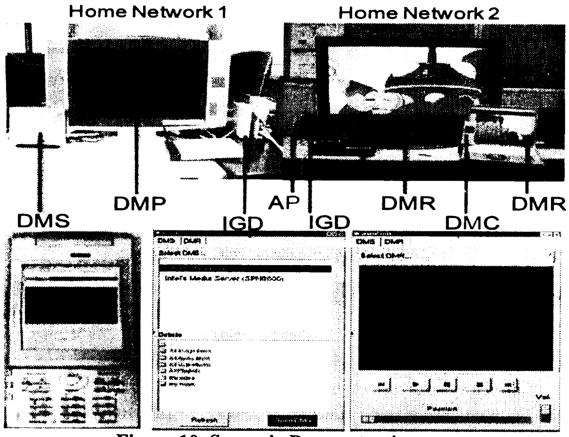

Figure 10. Scenario Demonstration

rendering according to the time delay later than the remote rendering. Because the measurement of time delay is difficult to be precise completely. Here we choose another method and it already be tested effective in our experimental environment. As shown in Figure 9, we can invoke the remote rendering first in the DMR process. The DMS proxy process involved in the remote rendering will send a signal to the DMR proxy process by IPC when the first time of content buffering finishes. Once the DMR proxy process receives this signal, it will invoke the local rendering right now.

6. Experimentation

In order to implement the WD, we constructed four home network environments. The Internet environments were set up as follows: FTTH B FLET's line was provided by NTT, FTTH HIKARI-one line provided by KDDI, the ADSL line was provided by Yahoo!BB, and the CATV line was provided by J:COM-NET. The DMS hardware and software were used as follows: Buffalo LinkStation, Sony X Video Station, Panasonic DMR-E500H, DIXIM 2. The following DMP were used, Funai TV & Sony Network Media Receiver, Toshiba 37LZ150, Funai TV & Sharp Network Media Player, and Sharp IT-32X2. The DMR hardware and software were as follows Funai SYLVANIA and Intel(R) Tools for UPnP(TM) Technology. Buffalo Airstation A&G was used as the Wireless LAN router.

As shown in Figure 10, the remote DMS was realized at the local domain in cooperation with the WDs. The DMC browses the contents on that DMS and renders the desired content on an arbitrary DMR located on the local home network. It also ensures flexibility in that the same content can be switched from one DMR to another.

Figure 11 illustrated the experimental results for the performance over the test environment shown in Figure 10. There are about 150 millisecond difference between on local domain and relayed by the WDs in multiple home networks. This is mainly due to the processing time consumed for the message encryption and decryption and relayed by the WDs. Because the delay for response time is steady and acceptable, our proposed system is feasible for sharing media content in multiple home network environments.

7. Conclusions and future work

In this paper, we proposed a new mechanism based on DLNA and SIP for sharing media contents among multiple home network environments. This mechanism can be integrated seamlessly with

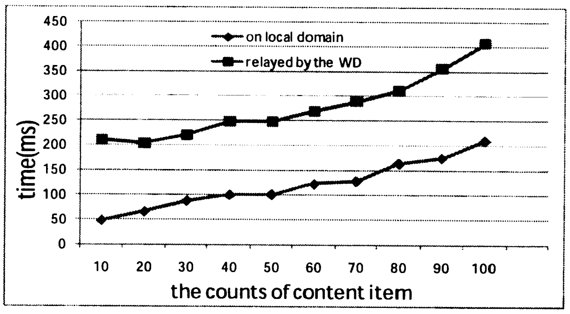

Figure 11. Processing Time for Obtaining the Content list

the existing DLNA-based devices in home network environment. In the process, these devices benefit from its excellent architecture. We also presented a mobile digital media controller with a user-friendly GUI. Users can select the desired DMS, either in the local home network or in a remote home network, and render the desired content on an arbitrary DMR in a local home network. Furthermore, *a single media content can be rendered on two DMRs that* are deployed in two different home networks *synchronously.* for example, in the case of the children who desire to share live video clips with their parents who are located on a remote network.

It is not safe to share media content with copyright protection among multiple home networks over the Internet. Recently, DTCP-IP— a digital transmission content protection specification over the IP network— was approved for use by the DLNA. Our future work, we will improve our WD to make it adaptable with DTCP-IP. In addition, we will also implement a DMR on a mobile device.

References

[1] Digital Living Network Alliance, "DLNA Network. Device Interoperability Guidelines", expanded: March 2006, pp 33-45.

[2] UPnP Forum, UPnP Device Architecture 1.0: Document Version 1.01, 20 July 2006, pp 4-76.

[3] UPnP Forum, UPnP AV Architecture: 1: Document Version 1.00, June 25, 2002, pp3–22.

[4] UPnP Forum, Internet Gateway Device: 1: Document Version 1.0, 2001, pp76.

[5] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnson, J. Peterson, R. Sparks, M Handley, and E. Schooler, "SIP : Session Initiation Protocol", RFC 3261, 2002.

[6] J. Rosenberg, dynamicsoft, H. Schulzrinne, Columbia University, C. Huitema, D. Gurle, Microsoft Corporation, "Session Initiation Protocol (SIP) Extension for Instant Messaging", RFC3428, 2002.

[7] W.-S. Liao, Y.-J. Huang, and C.-L. Hu, "Mobie Media Content Sharing in UPnP-Based Home Network Environment", Proceedings of the 2007 International Symposium on Applications and the Internet Workshops, SAINTW'07, pp.1-4.

[8] Y.-J. Oh, H.-K. Lee, J.-T. Kim, E.-H. Paik, and K.-R. Park, "Design of an Extended Architecture for Sharing DLNA Compliant Home Media from Outside the Home", IEEE Transactions on Consumer Electronics, Vol.53, No.2, MAY 2007, pp.1-6.

[9] A. Vilei, G. Convertino, F. Crudo,"A New UPnP Architecture for Distributed Video Voice over IP", MUM'06,pp.1-7.

[10] S. M., K. Tasaka, T. Niwat, H. Horiuchi, "Proposal on Wide Area DLNA Communication System", IEICE Technical Report, April, 2007, pp.1-6.