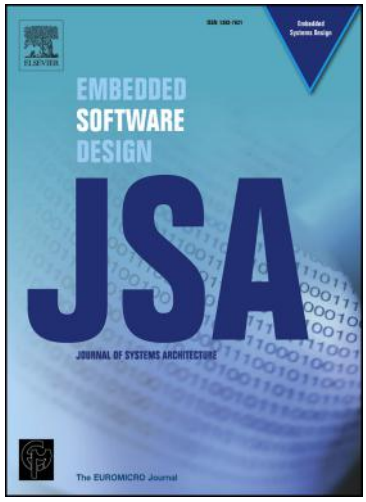


A Remote Control and Media-Sharing System Using Smart Devices

Shou-Chih Lo, Ti-Hsin Yu, Chih-Cheng Tseng

PII: S1383-7621(14)00067-8
DOI: http://dx.doi.org/10.1016/j.sysarc.2014.04.005
Reference: SYSARC 1238

To appear in: *Journal of Systems Architecture*

Received Date: 27 August 2013
Revised Date: 23 April 2014
Accepted Date: 29 April 2014

Please cite this article as: S-C. Lo, T-H. Yu, C-C. Tseng, A Remote Control and Media-Sharing System Using Smart Devices, *Journal of Systems Architecture* (2014), doi: http://dx.doi.org/10.1016/j.sysarc.2014.04.005

A Remote Control and Media-Sharing System Using Smart Devices

Shou-Chih Lo[1] Ti-Hsin Yu[1] Chih-Cheng Tseng[2]

[1]Department of Computer Science and Information Engineering
National Dong Hwa University, Hualien, Taiwan, ROC
[2]Department of Electrical Engineering
National Ilan University, I-Lan, Taiwan, ROC

sclo@mail.ndhu.edu.tw, bfl71109@hotmail.com, tsengcc@niu.edu.tw

Abstract — *The remote control and media sharing of electronic devices are key services in smart homes. The incorporation of mobile smart devices in these services has become a popular trend. Existing services require that these devices are located in the same local network. This paper presents the design and implementation of an integrated service architecture that supports the remote control of home appliances and the sharing of digital media between indoor and outdoor devices. The proposed design follows standards related to digital homes, and this study presents the details of its hardware and software components.*

Index Terms — Smart Home, Smart Devices, Media Sharing, Remote Control, DLNA/UPnP.

I. INTRODUCTION

With the popularity of various types of digital consumer products, digital content is becoming increasingly common. The sharing of various digital media, such as videos, photos, and music, between consumer products has become a popular trend. Some commercial solutions provide platforms to integrate home audiovisual devices. For example, a personal computer can control the playing and recording of TV programs or videos on a DVD player. A smart TV can integrate multimedia and Internet services together.

The Digital Living Network Alliance (DLNA) [1], which is responsible for defining interoperability guidelines between multimedia devices, was initiated in 2003. The underlying technology of DLNA is Universal Plug and Play (UPnP) [2] for media management, discovery, and control. The UPnP standard, which includes a set of standard network protocols such as TCP/IP, HTTP, and Simple Object Access Protocol (SOAP), enables digital devices with networking capability to connect to each other. Over two hundred member companies follow the DLNA guidelines in their products.

DLNA-compliant devices can seamlessly discover each other in the same home network, sharing services and media. The DLNA standard defines four types of devices: Digital Media Server (DMS), Digital Media Controller (DMC), Digital Media Player (DMP), and Digital Media Renderer (DMR). A DMS stores and provides media content to other devices. A DMC can discover media content and command a DMR to play the content. A DMP, which consists of a DMC and a DMR, can discover and play media content directly.

Digital media can be shared between DLNA devices for the users' convenience. However, users cannot benefit from such service when staying outdoors, since a remote device cannot directly join home DLNA networks. Thus, some solutions are required to extend the basic service model of DLNA. For example, a mobile user can retrieve and play media streams from an indoor DMS by connecting an

external device to a home network using the Session Initiation Protocol (SIP) [3]. However, this solution is only capable of one-way media sharing. Home-to-home media sharing can be achieved by setting up a DLNA proxy server in each home [4].

Making living environments smarter will require modern technologies other than DLNA/UPnP. For example, integrating sensor technology and automatic control in home appliances enables remote function control, power control, and remote surveillance [5-8]. A typical way to integrate different services and devices in heterogeneous home networks, including X10, wireless LAN, Bluetooth, and Ethernet, is to set up a residential gateway in the home based on the standards such as Open Service Gateway Initiative (OSGi) and Multimedia Home Platform (MHP) [9].

This paper presents a straightforward method of constructing a residential gateway using a popular smartphone to establish a service architecture that provides remote access and control to any home appliances. The powerful functions of smartphones enable several mobile personal services [10-12]. The home appliances in this system include any DLNA or UPnP devices and non-UPnP devices. The prototype system provides the functions of remotely monitoring and switching the power of a home device, and sharing media content between an indoor device and a remote device.

The proposed system is based on an open-source platform for easy deployment. Those traditional home devices without built-in UPnP functions are externally equipped with control boards, and hence these devices can be remotely controlled using an indirect method. The control board contains an open-source microcontroller that can be easily programmed to control robots, lighting, and other devices. Also, this control board provides a linkage to external modules, including sensor modules and wireless communication modules.

A previous conference paper [13] presented the initial concept of this prototype system. This study presents the system by introducing more implementation details and providing a performance evaluation. The remainder of this paper is organized as follows. Section II presents a brief introduction of the UPnP and DLNA standards. Section III presents the system design. Section IV presents system operations. Section V presents the developed system. Finally, Section VI provides concluding remarks.

II. Background Knowledge

The UPnP standard is an open and point-to-point protocol that enables the plug-and-play of a device in IP networks. The UPnP protocol specifies the communication between control points (or controllers) and devices. A device is any instrument that provides services. A service provides a list of executable actions and a list of state variables. For example, a time service contains a state variable that records the current time and two actions that set and get the current time, respectively. A control point can discover the presence of other devices to run the services of these devices.

The UPnP operations include six steps: addressing, discovery, description, control, event notification, and presentation. A device gets an IP address from a Dynamic Host Configuration Protocol (DHCP) server in the addressing step. A control point discovers other devices in the same network by sending a search request in the discovery step. This search request is a multicast message made using the M-Search method in HTTP. This search request also contains an ssdp:discover method in the Simple Service Discovery Protocol (SSDP). A device responds to the search request by sending a unicast message with the ssdp:alive method to the control point. The search response contains information such as the device type, a device identifier (or Unique Service Name, USN), and a Uniform Resource Locator (URL) to the device profile or description. The device profile is a description file in eXtensible Markup Language (XML) format that primarily consists of a list of URLs for accessing the services of

the device.

A device that has just joined the network can send a multicast message with the ssdp:alive method to show its presence to all control points. When a device wants to leave the network, it sends a multicast message with the ssdp:byebye method to inform all control points of its departure. In the description step, a control point obtains a device profile by sending an HTTP request with the GET method to the profile's URL. In the control step, a control point can remotely invoke a service function by sending an HTTP request with the POST method to the service URL. The service invocation in this request message is specified using SOAP headers and elements. In the event notification step, a control point can subscribe to a certain event to learn the state change of a device. If a device contains a web page showing the device status, a control point can access this page in the presentation step.

The DLNA standard [14] is built over the UPnP device architecture and the UPnP AV standard (an audio and video extension of UPnP) (Fig. 1). The media format layer defines the supported media types, which primarily include music, videos, and pictures. The media management layer provides functions to DLNA devices in managing and publishing media content, and enables communication between a DMC and a DMR (or DMP). The device discovery and control layer provides the same six-step operations of UPnP, and a DMC acts as a control point. The media transport layer specifies HTTP as the basic transport protocol for media content. The network stack and network connectivity layers define the supported network types and protocols.

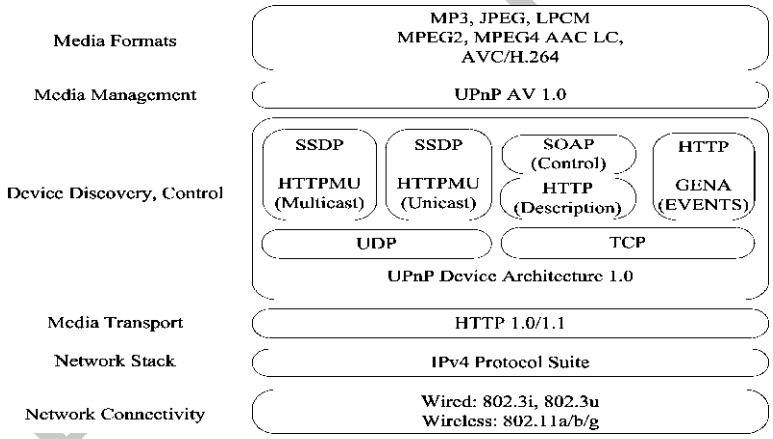


Fig. 1. DLNA layered architecture.

The DLNA service model is restricted to home networks for security reason. To extend this service to public networks, a secure residential gateway is needed to interwork with outdoor devices. The SIP server can be integrated into the gateway [3] such that an outdoor device acting as a SIP client can retrieve media registered by home DMSs. Another solution [4] is to let an outdoor device connect back to the home network using the Virtual Private Network (VPN) technology. Our solution is also based on the VPN, but our system has two distinguishing features against the above two solutions. First, both outdoor DMPs and outdoor DMSs are available. Second, remote control functions to traditional non-UPnP appliances are supported.

One important issue not widely addressed in this paper is about security. Certain prevention technologies from security threats are necessary. For example, digital content needs to be protected by using Digital Rights Management (DRM) technology. Unauthorized users can not access some home appliances or some media files. Secure networking solutions can be applied such as the link-layer solution: WPA (Wi-Fi Protected Access), the network-layer solution: IPsec (IP Security), the transport-

layer solution: SSL (Secure Socket Layer), and the application-layer solution: PGP (Pretty Good Privacy). The interested reader is referred to [15-17] for details.

III. System Design

This section presents the details of the system design, and Fig. 2 shows the service architecture. This system can extend smart living services from an indoor environment to an outdoor one. This architecture provides the following services:

- A user in the home or out of the home can monitor and control home appliances and share digital content with home DLNA-compliant devices through a mobile phone. For example, remote device A turns off the desk lamp and downloads a music file from an indoor DLNA device in Fig. 2.
- Two outdoor users can share digital content as if they were on the same home network. For example, remote device B can access image files from remote device A in Fig. 2.
- An outdoor user can redirect the play of digital content to a local DMR. For example, remote device C can command a local DMR to retrieve and play a video from an indoor DLNA device in Fig. 2.

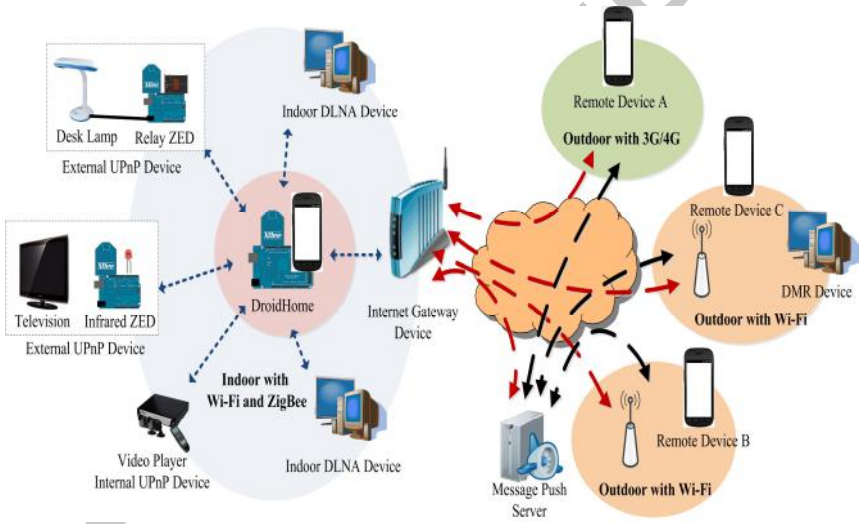


Fig. 2. Service architecture with main components in the proposed system.

The system contains two types of home devices DLNA devices and UPnP devices. DLNA devices provide or play media content and UPnP devices provide remote control services. To enable traditional devices, such as desk lamps and air conditioners, to support UPnP functions, each of these devices must be equipped with a control broad. Consequently, these traditional home devices become external UPnP devices (in contrast to internal UPnP devices, which have built-in UPnP functions). Each control board works as a ZigBee End Device (ZED) that can be controlled by a ZigBee Coordinator (ZC) through ZigBee wireless communication.

The core component of the system is the DroidHome component, which discovers and maintains DLNA and UPnP devices. DroidHome plays the role of a proxy server for remote devices and informs these remote devices about the state change of an indoor device through a message push mechanism. The message push mechanism is based on an existing push service on the cloud [18]. A mobile device can be notified in the background by the message push server if the corresponding user has registered to the server.

A. *Challenges and Solutions*

Service discovery and invocation in DLNA and UPnP networks use the same methods of SSDP. However, integrating non-UPnP devices and remote devices into this service architecture causes some problems. The following paragraphs present these challenges and the proposed solutions.

(1) **Remote DMS**: If an indoor DLNA device is allowed to directly access any digital content from a remote device configured as a DMS, this remote DMS should join the same home network as indoor devices. One simple way is to connect this remote device back to the home network using the Point-to-Point Tunneling Protocol (PPTP) that enables a VPN. However, this remote device cannot show its presence by simply multicasting an ssdp:alive message to the home network because of a different setting of the subnet mask. The subnet mask of the home network is 255.255.255.0, whereas that of the remote device is 255.255.255.255 by default. The proposed solution is that this remote device should unicast the message to DroidHome first, which in turns multicasts the message to the home network.

(2) **Remote DMP**: If a remote device configured as a DMP connects to the home network using the PPTP, this remote DMP can directly play the digital content of an indoor DMS. However, the drawback of this approach is that the remote DMP must stay connected to the home network. DroidHome can decouple this strong connection. DroidHome acts as a DMC and records the service state of each indoor DLNA or UPnP device. DroidHome also maintains a table recording the URLs to these device profiles. A remote DMP simply contacts DroidHome to retrieve this URL table to invoke a certain service. When DroidHome detects any state change (e.g., the joining or leaving of an indoor DMS), it notifies these remote devices using the message push service

(3) **Private home network**: Almost all home networks are configured as private networks in which all indoor devices use private IP addresses and an Internet Gateway Device (IGD) uses the only public IP address. This IGD provides the Network Address Translation (NAT) function to let all indoor devices share the same public IP address. The core technique is based on port mapping. However, most NAT devices maintain dynamic port mapping, which makes an indoor device unreachable from the Internet. The proposed system uses an UPnP-supported IGD that can be automatically discovered and remotely configured with static port mapping. DroidHome first registers a mapping port to this IGD to allow any remote devices to connect to DroidHome through the IGD's public IP address and the registered port number. DroidHome also translates all private addresses in the URL table to the IGD's public address to enable a remote device to directly access the profile of an indoor device. Each address translation requires DroidHome to register a new mapping port to the IGD.

(4) **External UPnP device**: In the proposed system, an external UPnP device actually refers to a non-UPnP device. These devices do not naturally have networking capability and service functions. Each of these devices is first equipped with a control board. This control board can switch the power or enable certain functions of the associated device through a programmable current relay unit or an infrared emitter. This control board communicates with DroidHome using ZigBee wireless communication. Second, DroidHome dynamically creates a software device object for each external UPnP device. A device object provides the corresponding service profile and service functions to the physical device. DroidHome records the access path to this device object in its URL table. Consequently, a remote device can look up the services provided by external UPnP devices and then invoke these functions through DroidHome.

B. Component Design

The following paragraphs present an explanation of the function and design of each hardware component in the system.

(1) **ZED**: The component is responsible for controlling the associated external UPnP device. Each ZED is implemented on a programmable control board and has the following types: infrared ZEDs and relay ZEDs. An infrared ZED can emit infrared signals to switch the power or perform a function of the associated device. The relay ZED can control the current to the power line of the associated device.

An infrared ZED contains the following hardware components. A current transformer (CT) sensor detects the current of a power line and detects the power status of a device. A ZigBee module provides wireless communication with DroidHome and is configured as a ZED mode. An infrared (IR) module sends and receives infrared signals. A button module sets the infrared signal in the IR module to the same frequency as the remote controller of a home device.

A relay ZED contains a CT sensor, a ZigBee module, and a current relay module that can turn the power on or off. In addition to these hardware components, each ZED maintains some data, such as the power status of the associated device, the ZED type, and the ZED identification number.

(2) **DroidHome**: This hardware component consists of a smartphone and a control board connected through USB communication. The former subcomponent discovers and maintains indoor DLNA devices and internal UPnP devices within the home network (a Wi-Fi networking environment in the system). The latter subcomponent discovers and controls indoor ZEDs through ZigBee networking.

Fig. 3 shows the internal software modules of DroidHome. The control board contains a ZigBee module that is configured in the ZC mode. This ZC periodically multicasts a discovery message (triggered by the ZED discovery module) such that all surrounding ZEDs respond to this message with their types and ID data. The ZED table records these response data. The ZED control module issues a control command (e.g., power switch) to each ZED.

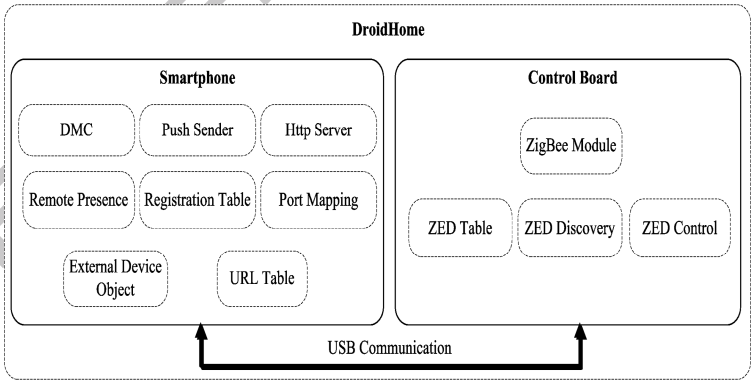


Fig. 3. Internal hardware and software components of DroidHome.

A registration table in the smartphone stores the identification information of each authorized remote device, including its USN, a push token (a certification code given by the message push server to identify a user), and a password. The DMC module is responsible for device discovery. The URL table stores the access path to the profile of a discovered device. This table keeps two versions of URLs (private URL and public URL) with the primitive and the translated IP addresses and port numbers, respectively, for each access path. A remote DMS (configured with a private IP address) and a remote DMP (configured with a public IP address) use these private and public URLs, respectively, to access the profiles of indoor devices.

The external device object table stores the basic information of all discovered ZEDs. Each device object maintains the status and profile of the associated device. A port mapping module handles the request and response messages to and from the IGD for port mapping. The remote presence module notifies indoor devices about the joining and leaving of a remote DMS by multicasting messages into the home network. The server push module handles the contact to the message push server to push a notification to a remote device. The HTTP server module handles the downloading request of a device profile and the request of service invocation from a remote device.

(3) **Remote device**: Fig. 4 shows the software modules in a smartphone that are necessary for the system operation. The register module processes the registration to the message push server and DroidHome. The DMP module discovers any DMSs and renders the service content. If a remote device is out of the home network, this device can discover indoor services by retrieving device profiles according to the access paths listed in the URL table of DroidHome. The import devices module performs this task. However, the URLs to the services listed in a device profile still include private IP addresses. Before a service function can be correctly invoked, the port mapping module requests that DroidHome adds a new mapping port for this service. The push receiver module listens to the notification of the state change of any indoor device. The DMS module is activated when a remote device wants to share digital content with other devices. In this situation, the remote device waits for incoming requests to access its profile or services through the HTTP server module.

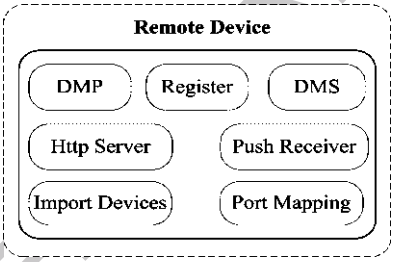


Fig. 4. Internal software components of a smartphone as a remote device.

IV. SYSTEM OPERATION

Any remote device in the system can configure itself as a DMP or DMS. The remote device may be in the home or out of the home. For the various combinations of working modes, the following paragraphs present the related operation of each service function. When a remote device is in the home, it operates as a typical indoor DLNA/UPnP device.

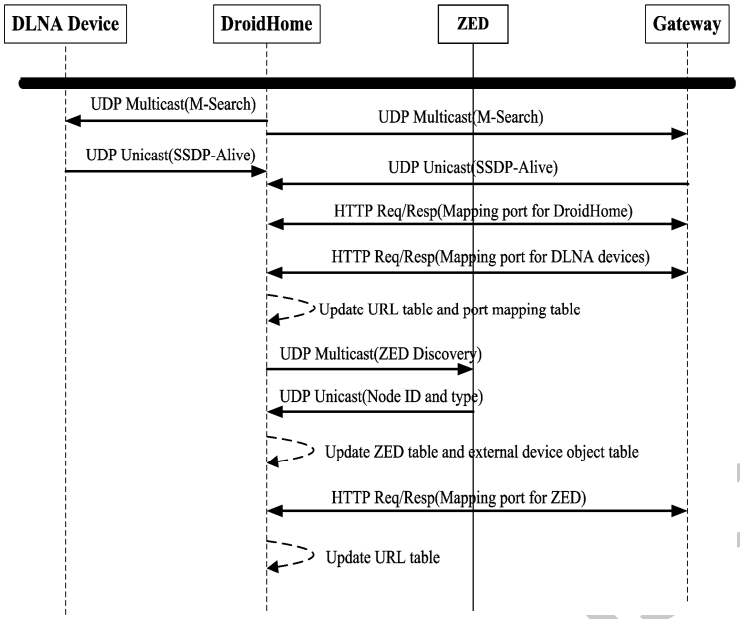


Fig. 5. Processing steps to initialize the DroidHome.

A. Indoor Operation

(1) **DroidHome initialization**: When starting, DroidHome first discovers indoor DLNA and UPnP devices (Fig. 5).

1. DroidHome sends a search request to the home network to discover the DMSs and the IGD. These discovered devices reply with search responses.
2. DroidHome records the access path to the device profile of each discovered device in the URL table.
3. DroidHome registers the mapping ports for itself and all discovered devices to the IGD.
4. DroidHome broadcasts a ZED discover message into the network and then records the types and IDs of the discovered ZEDs in the ZED table.
5. DroidHome creates the external device objects corresponding to the discovered ZEDs and generates both private and public URLs for these devices.

(2) **Remote device registration**: Each remote device registers itself with DroidHome within the home network one time (Fig. 6).

1. A remote device sends a registration message to DroidHome using a preconfigured multicast address.
2. DroidHome verifies the password and then records the USN and push token of the registered device. The server push service is initially disabled for a remote device.
3. DroidHome replies to the registered device with its private and public addresses.

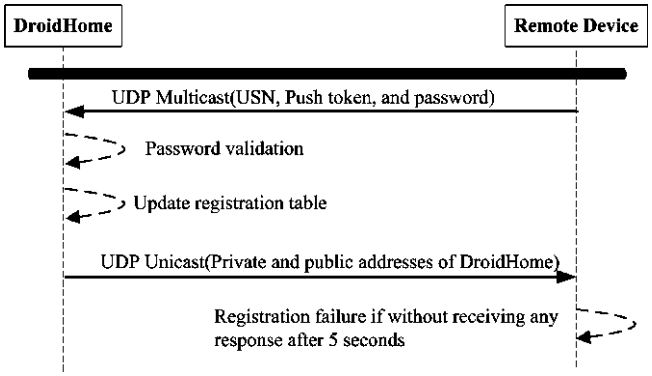


Fig. 6. Processing steps of remote device registration.

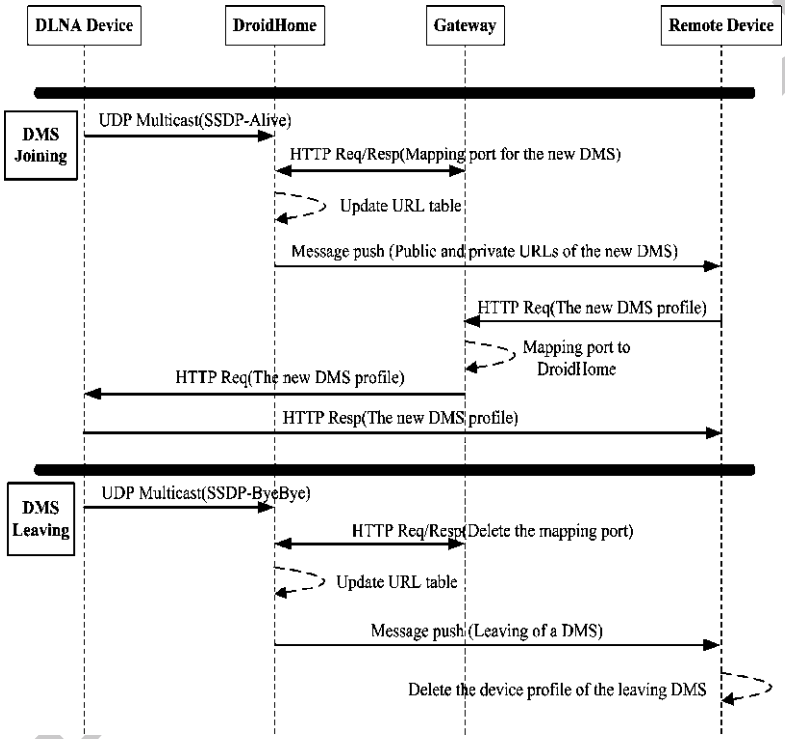


Fig. 7. Processing steps of the joining and leaving of an indoor DMS.

(3) **Indoor DMS joining**: DroidHome monitors the joining event and explicitly notifies this event to all remote devices that have registered (Fig. 7).

1. A new indoor DMS broadcasts an ssdp:alive message into the home network.
2. DroidHome records the private URL to the device profile of this new DMS.
3. DroidHome registers a mapping port for this DMS and records the public URL.
4. DroidHome sends a push message to each registered remote device. This message includes the access path to the device profile of this DMS.
5. A remote device retrieves the device profile of the DMS through the provided URL.

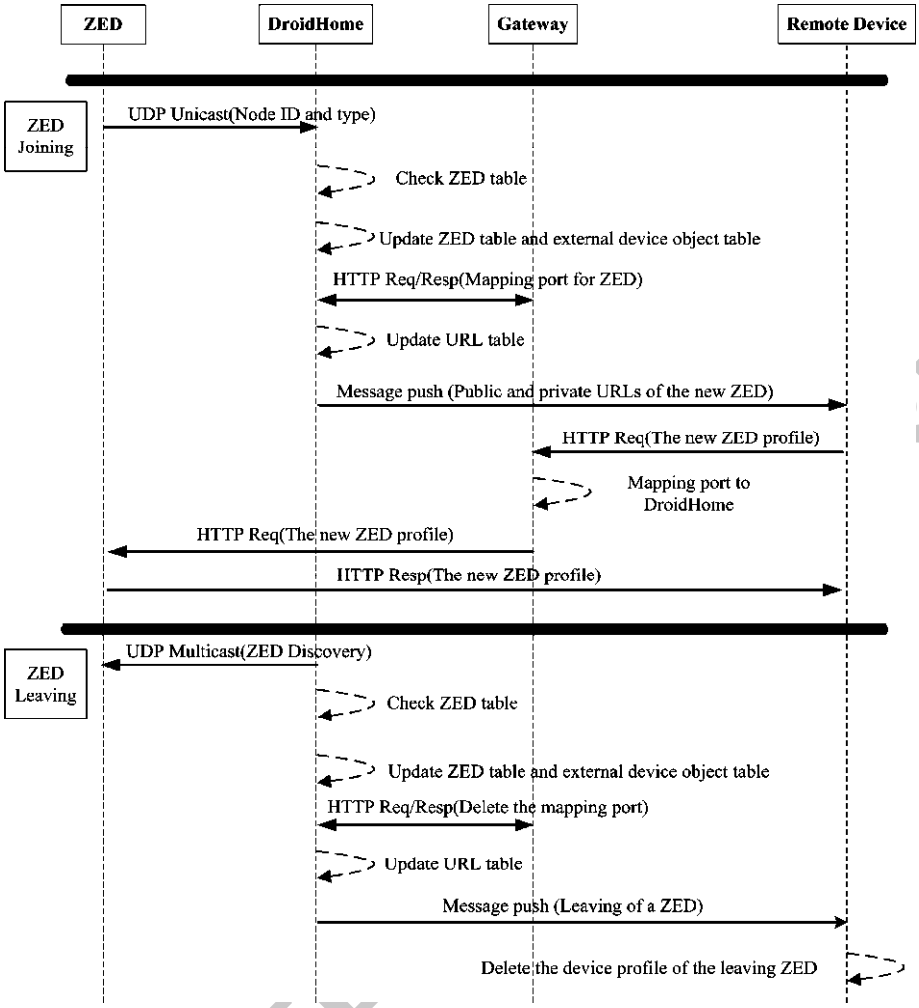


Fig. 8. Processing steps of the joining and leaving of an external UPnP device.

(4) **Indoor DMS leaving**: DroidHome monitors leaving events and explicitly notifies these events to all remote devices that have registered (Fig. 7).

1. A leaving indoor DMS broadcasts an ssdp:byebye message into the home network.
2. DroidHome deletes the access path information of this DMS from the URL table.
3. DroidHome removes the corresponding mapping port to this DMS from the IGD.
4. DroidHome notifies each registered remote device of a leaving DMS.

(5) **External UPnP device joining**: This process flow is similar to the joining of a new DMS, but is handled by the control board in DroidHome (Fig. 8).

1. The ZED corresponding to a joining device sends a joining message to DroidHome.
2. DroidHome retrieves the type and ID information from the joining message and checks whether this device has been recorded in the ZED table. If it is not, DroidHome updates the ZED table and proceeds to the next step. Otherwise, DroidHome ignores the joining message.
3. DroidHome creates a device object that provides the device profile and service functions of the joining device.
4. DroidHome sends a push message to each registered remote device. This message includes the access path information.
5. A remote device retrieves the device profile through the provided URL.

(6) **External UPnP device leaving**: This process flow is similar to that of DMS departure (Fig. 8).

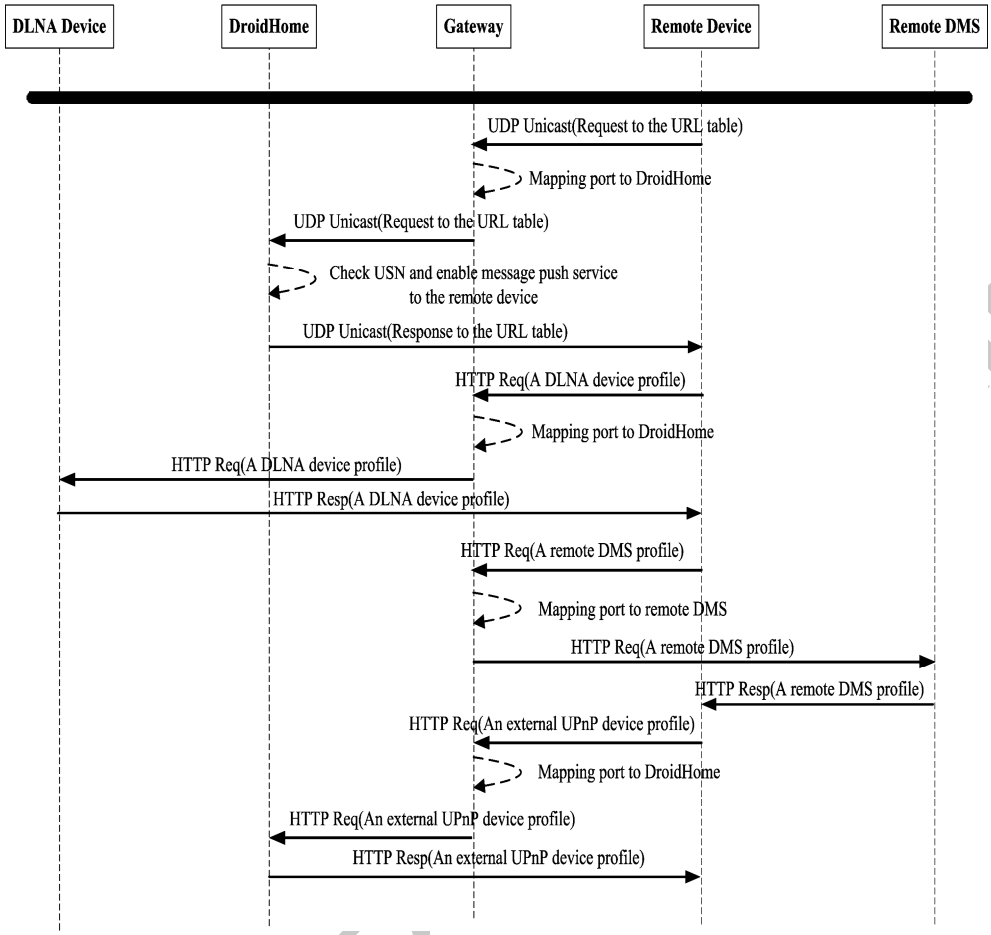


Fig. 9. Processing steps to get a device profile.

B. Outdoor Operation

(1) **Get a device profile**: A remote device connects to DroidHome and retrieves the URL table, which contains access paths to the device profiles of all indoor DLNA/UPnP devices and remote DMSs (Fig. 9).

1. A remote device sends a request message to DroidHome to download the URL table.
2. DroidHome authenticates this remote device and enables the server push service to this remote device.
3. DroidHome replies to the request by sending all entries in the URL table to the remote device.
4. The remote device then uses the provided URL address to retrieve a device profile.
5. The IGD redirects the profile retrieval request to the correct device by mapping ports. Remote DMSs and indoor DLNA devices hold device profiles for themselves, but DroidHome holds the device profiles of external UPnP devices.

(2) **Enable a remote DMS**: A remote device can configure itself as a DMS and connect to DroidHome using a VPN tunnel (Fig. 10).

1. A remote device connects to the IGD by initiating a VPN tunnel.
2. The IGD allocates a private IP to this remote device.
3. The remote device shows it service presence to the home network by sending its private URL and USN to DroidHome.
4. DroidHome records both the private and public URLs after registering a mapping port for this remote

DMS.

5. DroidHome broadcasts an ssdp:alive message into the home network for this remote DMS and then notifies remote devices of a joining DMS.

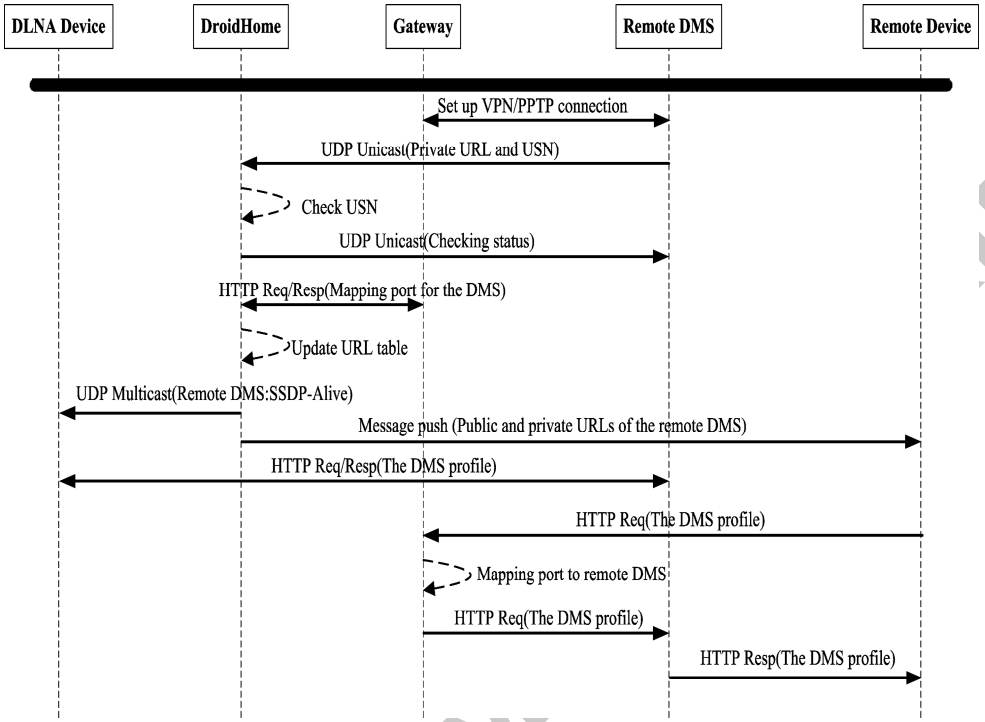


Fig. 10. Processing steps to enable a remote DMS.

(3) **Disable a remote DMS**: This process flow is similar to the departure of an indoor DMS, but is mainly handled by DroidHome.

(4) **Invoke a service function**: A remote device should configure itself as a DMP and then invoke a service function. Fig. 11 shows the steps involved in playing a media file located in different places. Fig. 12 shows the steps involved in turning on an external UPnP device.

1. A remote device sends a SOAP message to the service URL.
2. The IGD redirects this request to the correct device. An indoor DLNA or internal UPnP device receives this request. DroidHome receives this request if the invoked service function is provided by an external UPnP device.
3. The service device returns the execution result to the remote device. If an external UPnP device is involved, DroidHome communicates with the corresponding ZED to execute services.

(5) **Render output to a remote DMR**: A remote device discovers any DMRs in its current network using the standard DLNA service discovery. This remote device can render the digital content of an indoor or remote DMS to a locally discovered DMR (Fig. 13).

1. A remote device first invokes a browsing service to a DMS to retrieve the directory of media contents.
2. The remote device configures a public URL for the selected media file.
3. The remote device commands a local DMR to play the media by telling it the access path of the media file.
4. The local DMR then retrieves and plays the media stream.

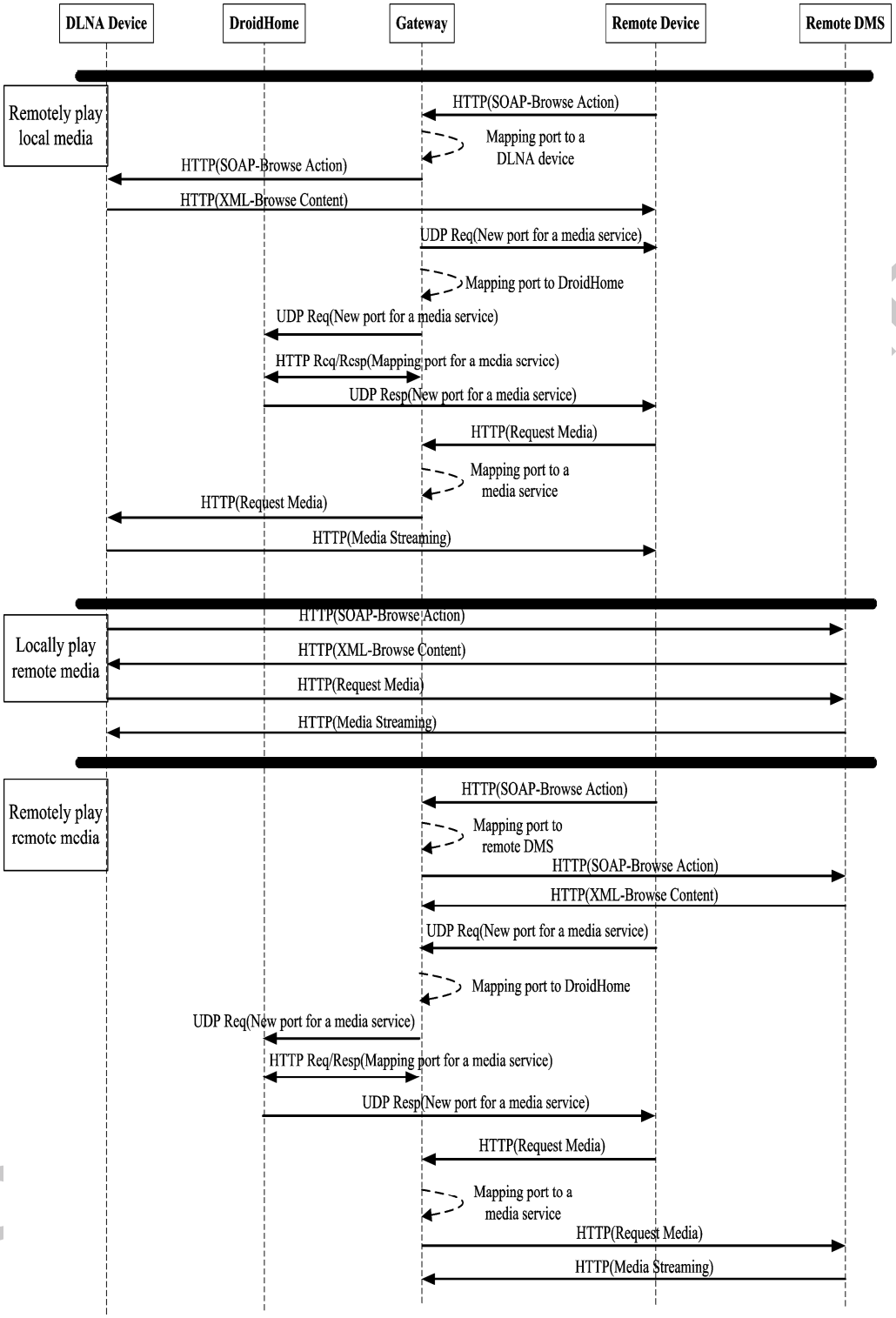


Fig. 11. Processing steps to play a media stream.

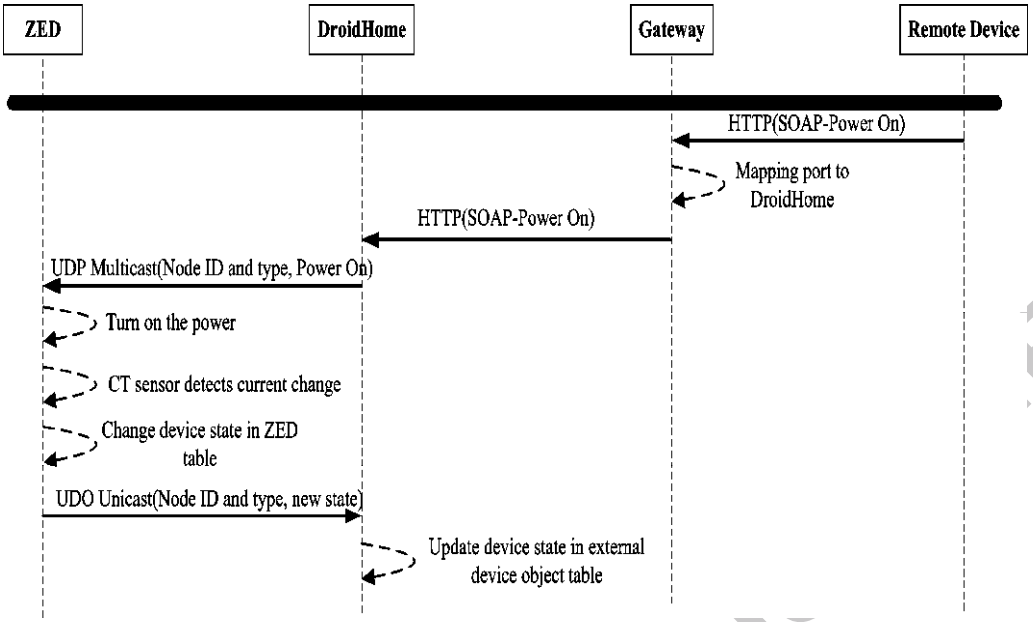


Fig. 12. Processing steps to turn on an external UPnP device.

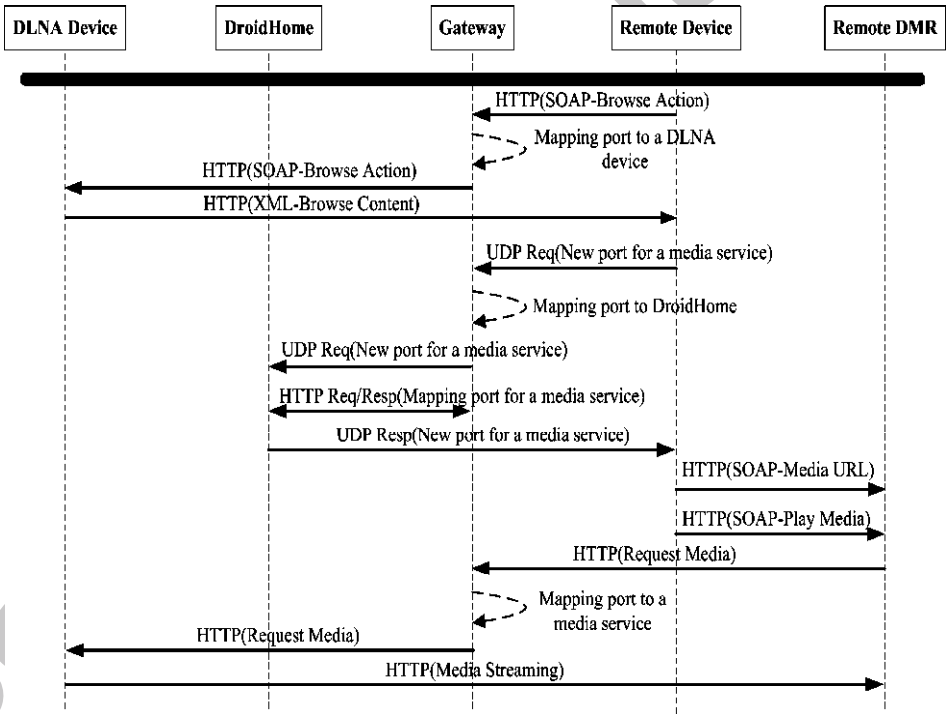


Fig. 13. Processing steps to redirect the play of a media stream to a DMR.

V. DEMONSTRATION AND EVALUATION

This section provides a demonstration of the prototype system and its performance evaluation. Table I lists the hardware specifications. The testbed in Fig. 14 is built over a campus-wide local area network which consists of one DroidHome, one remote DMS, one remote DMP, one remote DMR (colocated with the remote DMP), one indoor DMS, one relay ZED (controlling an indoor lamp), one infrared ZED (controlling an indoor TV), and one IGD. The coverage area of an access point is considered as an indoor or outdoor networking area. The leftmost two coverage areas are considered as remote

networks and the rightmost coverage area is considered as a home network.

TABLE I
HARDWARE SPECIFICATIONS IN THE TESTBED

NAME	SPECIFICATION
DroidHome	Smartphone + Control Board
Remote DMS	Smartphone
Remote DMP	Smartphone
Remote DMR	Notebook Computer (Media Player)
Indoor DMS	Personal Computer (Serviio Media Server)
ZED	Control Board
IGD	Access Point

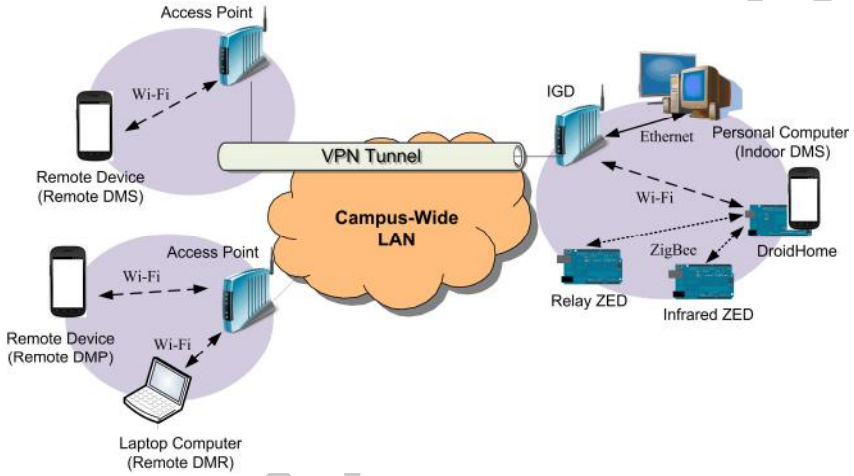
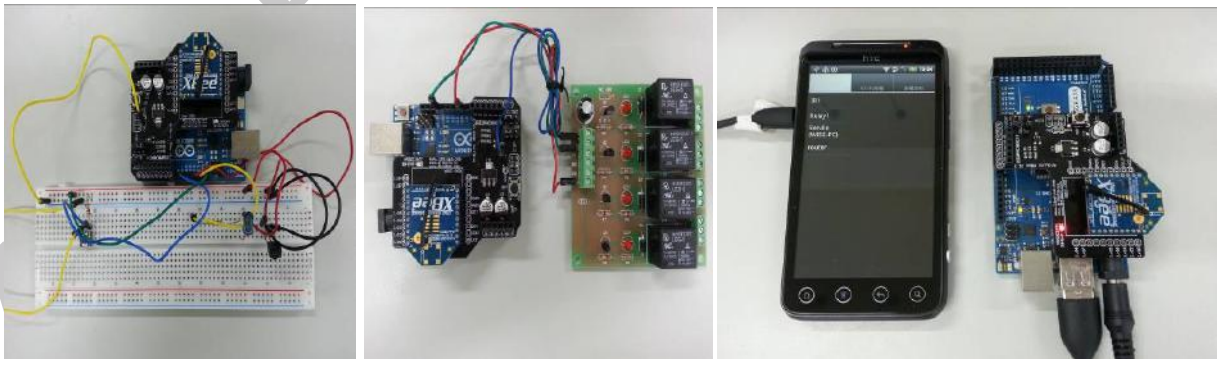


Fig. 14. Testbed environment setting.

Fig. 15 shows the prototypes of DroidHome (including one smartphone and one control broad), relay ZED, and infrared ZED. The DLNA/UPnP service programming in this system is based on an open software stack [19] providing Java-based application programming interfaces.



(a) **(b)** **(c)**

Fig. 15. Hardware design of core components: (a) infrared ZED, (b) relay ZED, and (c) DroidHome.

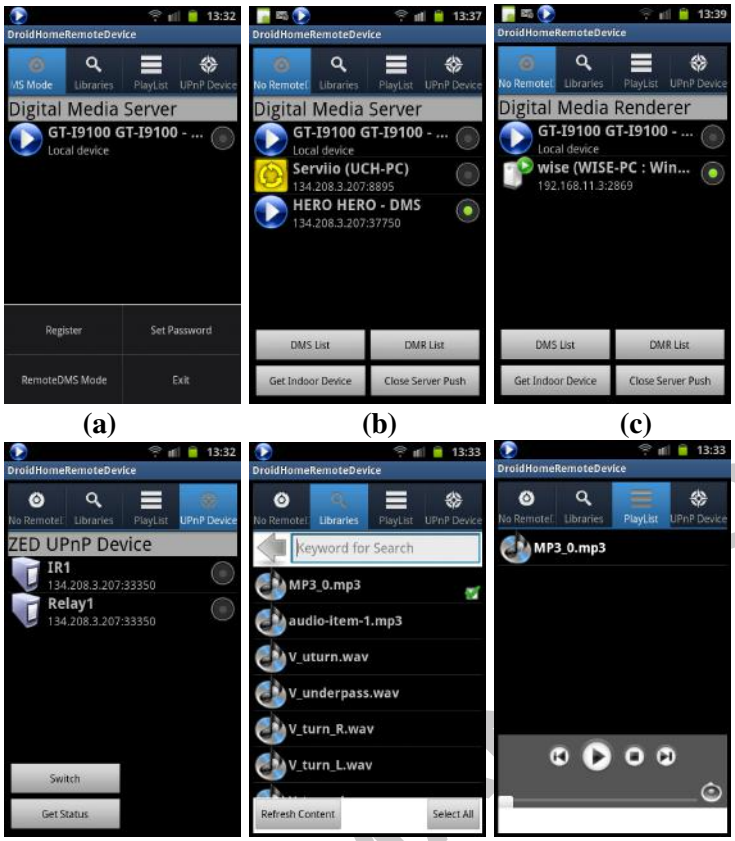


Fig. 16. Remote DMP interfaces: (a) setting menu, (b) discovered DMSs, (c) discovered DMRs, (d) discovered ZEDs, (e) media directory, and (f) media play.

Next, consider the operations of the remote DMP. On the main interface of Fig. 16a, a user can set a password, register with the message push server and DroidHome, and switch the remote device to the DMS mode. Device discovery is performed by clicking the Get Indoor Device button (Fig. 16b). All discovered DLNA devices are separately displayed by clicking the DMS List and DMR List buttons (Fig. 16b and Fig. 16c).

Fig. 16d shows all external UPnP devices, where two buttons are available for switching the device power and getting the device power status. After selecting a DMS (Fig. 16b), its media directory can be retrieved and browsed (Fig. 16e). Users can search the media directory using keywords. Fig. 16f shows the control panel of playing a selected music file. If a DMR is specified in the page of Fig. 16c, the media play is redirected to the selected DMR.

The remote power controls to the indoor lamp and TV are generally executed within 1 s to 2 s. The following discussion presents the performance of media streaming services under different simulated networking environments (e.g., xDSL, Wi-Fi, and 3G). The downlink and uplink data rates of the home network are configured with three settings: (8 Mb/s, 640 Kb/s), (20 Mb/s, 4 Mb/s), and (50 Mb/s, 5 Mb/s). The downlink and uplink data rates of the remote network have four settings: (2 Mb/s, 400 Kb/s), (1.2 Mb/s, 700 Kb/s), (1.5 Mb/s, 1.5 Mb/s), and (10 Mb/s, 10 Mb/s). The experiments reported in this study involve two media streaming services with a 7 MB MP3 file and a 159 MB MP4 file, respectively.

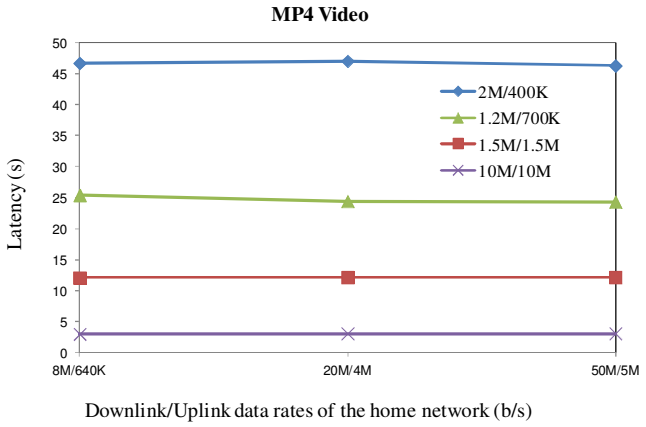


Fig. 17. Access latency of playing a remote video stream.

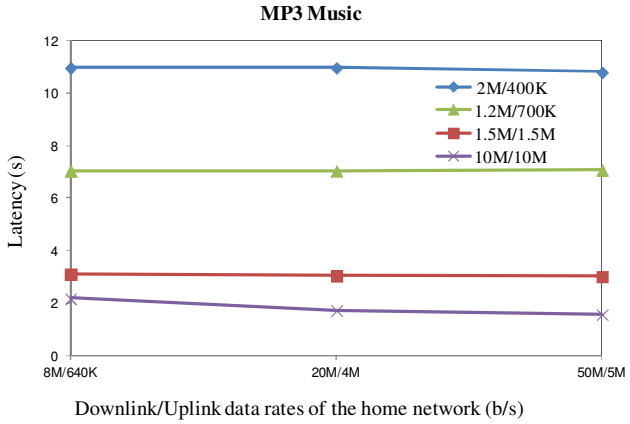


Fig. 18. Access latency of playing a remote music stream.

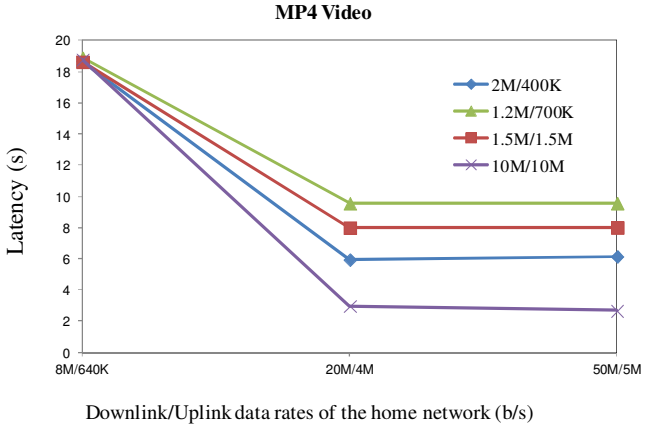


Fig. 19. Access latency of playing an indoor video stream.

The first experiment shows the access latency for an indoor device accessing a media stream from a remote DMS. The latency is the time period from the moment the user pushes the play button to the moment the media is actually played. Figs. 17 and 18 show the experimental results where each curve shows the case with the specified downlink/uplink data rates (b/s) of the remote network. Because the downlink data rate in the home network is sufficient large (i.e., greater than 8 Mb/s), the access latency is primarily dominated by the uplink data rate of the remote network. When the uplink data rate is large,

the latency becomes small. The latency of playing a video stream is greater than that of playing a music stream.

The second experiment shows the access latency for a remote device to access a media stream from an indoor device. Figs. 19 and 20 show that the access latency is primarily dominated by the small uplink data rate of the home network at 640 Kb/s. With sufficient uplink data rates, the latency is mainly affected by the downlink data rate of the remote network.

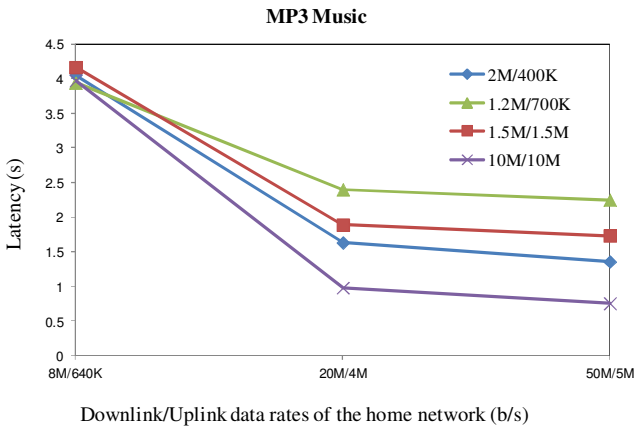


Fig. 20. Access latency of playing an indoor music stream.

VI. CONCLUSION

This study presents a home service platform that provides media sharing and power control to home appliances. The proposed system has four distinguishing features. First, it removes the restriction of media sharing among only indoor DLNA devices. The proposed system allows mobile phones to access this service regardless of whether they are in the home. Second, traditional home appliances without automatic control and networking capability can also be integrated with this platform when they are equipped with a simple control board. Third, the proposed system is based on an open-source software stack, existing equipment, and inexpensive hardware. Fourth, various home services, such as temperature sensing and video surveillance, can be easily integrated into the proposed service platform. In the future, a cloud computing platform and more home automatic functions will be involved into this system.

REFERENCES

[1] E. A. Heredia, *An Introduction to the DLNA Architecture: Networking Technologies for Media Devices*, John Wiley & Sons Ltd.: New Jersey, 2011, pp.1-6.

[2] UPnP Device Architecture, *International Standard*, ISO/IEC 29341-x, 2011.

[3] 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, pp. 542-547, May 2007.

[4] J. T. Kim, Y. J. Oh, H. K Lee, E. H. Paik, and K. R. Park, "Implementation of the DLNA proxy system for sharing home media contents," *IEEE Transactions on Consumer Electronics*, vol. 53, no. 1, pp. 139-144, Feb. 2007.

[5] M. F. Horng, B. C. Chang, and B. H. Su, "An intelligent intrusion detection system based on UPnP technology for smart living," *International Conference on Intelligent Systems Design and Applications*, pp. 14-18, Nov. 2008.

[6] J. S. Leu, W. H. Lin, and H. J. Tzeng, "Design and implementation of an OSGi-centric remote mobile surveillance system," *IEEE International Conference on Systems, Man and Cybernetics*, pp. 2498-2502, Oct. 2009.

[7] Y. S. Chen, I. C. Chen, and W. H. Chang, "Context-aware services based on OSGi for smart homes," *IEEE International Conference on Ubi-media Computing*, pp. 38-43, Jul. 2010.
[8] T. Yamazaki, "The ubiquitous home," *International Journal of Smart Home*, vol. 1, no. 1, pp. 17-22, Jan. 2007.
[9] D. Valtchev and I. Frankov, "Service gateway architecture for a smart home," *IEEE Communications Magazine*, vol. 40, no. 4, pp. 126-132, Apr. 2002.
[10] J. Ahn and R. Han, "An indoor augmented-reality evacuation system for the smartphone using personalized pedometry," *Human-centric Computing and Information Sciences*, 2:18, Nov. 2012.
[11] J. K. Y. Ng, "Ubiquitous healthcare: healthcare systems and applications enabled by mobile and wireless technologies," *Journal of Convergence*, vol. 3, no. 2, pp. 15-20, Jun. 2012.
[12] K. S. Chung and J. E. Lee, "Design and development of m-learning service based on 3G cellular phones," *Journal of Information Processing Systems*, vol. 8, no. 3, pp. 521-538, Sept. 2012.
[13] T. H. Yu and S. C. Lo, "A remote control and media sharing system based on DLNA/UPnP technology for smart home," *International Conference on Multimedia and Ubiquitous Engineering*, pp. 329-335, May 2013.
[14] Digital Living Network Alliance, "DLNA networked device interoperability guidelines", v1.5, Mar. 2006.
[15] P. A. Nixon, W. Wagealla, C. English, and S. Terzis, *Smart Environments: Technologies, Protocols and Applications*, Wiley-Interscience: Hoboken, NJ, 2005.
[16] H. Nakakita, K. Yamaguchi, M. Hashimoto, T. Saito, and M. Sakurai, "A study on secure wireless networks consisting of home appliances," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, pp. 375–381, May 2003.
[17] D. Diaz-Sanchez, F. Sanvido, D. Proserpio, and A. Marin, "Extended DLNA protocol: Sharing protected pay TV contents," *International Conference on Consumer Electronics*, pp. 321-322, Jan. 2010.
[18] J. Hansen, T. M. Gronli, and G. Ghinea, "Cloud to device push messaging on Android: a case study," *International Conference on Advanced Information Networking and Applications Workshops*, pp. 1298-1303, Mar. 2012.
[19] Cling, http://4thline.org/projects/cling.

BIOGRAPHIES

Shou-Chih Lo received the B.S. degree in computer science from National Chiao Tung University, Taiwan, in 1993, and the Ph.D. degree in computer science from National Tsing Hua University, Taiwan, in 2000. He joined the Computer & Communication Research Center at National Tsing Hua University in 2000 as a Postdoctoral Fellow. Since 2004, he has been with the Department of Computer Science and Information Engineering of the National Dong Hwa University in Taiwan, where he is currently an Associate Professor. His current research interests are in the area of mobile and wireless networks.

Ti-Hsin Yu received the B.S. degree in information engineering and computer science from Feng Chia University, Taiwan, in 2008, and the M.S. degree in computer science and information engineering from National Dong Hwa University, Taiwan, in 2012. His research interests include software programming on smart phones and RFIDs.

Chih-Cheng Tseng received his B.S. and M.S. from the National Taiwan University of Science and Technology, Taipei, Taiwan, Republic of China, in 1994 and 1997 respectively, all in electronic engineering. He received his Ph. D. from the Graduate Institute of Communications Engineering, National Taiwan University, Taipei, Taiwan, Republic of China, in 2007. Dr. Tseng is currently an associate professor of the Department of Electrical Engineering, National Ilan University, I-Lan, Taiwan, Republic of China. Dr. Tseng was a visiting researcher at the Center for TeleInFrastruktur (CTIF), Aalborg University, Denmark on 2007 summer. Dr. Tseng's research interests include the design and performance evaluation of protocols for the 4G mobile communications and wireless ad hoc/sensor networks.