

# Open Service Platform Providing Services for Home Appliances

Tomohiro Ishihara and Naoki Matsuoka

FUJITSU LABORATORIES LTD., JAPAN

**Abstract**—New network services targeting home appliances (e.g. TV, DVR, network camera and sensors) are attracting great attentions. However, these services are provided by appliance vendors for their own appliances. An open platform on which third-parties can provide services to any home appliances is not yet available. We propose an open service platform where a home gateway and center-located servers cooperate. To achieve the open platform, our home gateway can add its software functions and be managed remotely. Remote access service to control home appliances is one of the key services over this platform. We propose a remote access method which provides highly secured and scalable access from the Internet into home. This paper also shows a prototype system with which we have demonstrated our proposed architecture.

## I. INTRODUCTION

Broadband access including ADSL (Asynchronous Digital Subscriber line) and FTTH (Fiber To The Home) have been spreading rapidly. Most popular services over these broadband accesses are called triple play which includes Internet access, telephone and video services. Service providers are also trying to create new services coming after the triple play.

Network services for home appliances are attracting a lot of attentions because the number of network-attached home appliances is increasing, and some services have already begun. These services are dedicated ones that are provided by appliance vendors for their own products. Therefore it's hard to do that third parties develop their services for home appliances. We believe this situation must be solved because opening the window to third parties is very important in order to create new attractive services.

In this paper, we propose an open service platform that connects home appliances and third parties. The platform consists of a home gateway, home gateway manager and service portal. Our home gateway takes a software architecture that enables the providers to add functions for new services.

This paper also shows a practical service on this platform. We believe remote access service is one of the key services. The service enables user to control his/her home appliances from outside. We propose a remote access method which provides highly secured and scalable access from the Internet into home.

In this paper, our proposed service platform is described in section II, and remote access method is described in section III. Finally, our developed prototype system is described in section IV.

## II. PROPOSED SERVICE PLATFORM

### A. Architecture

The proposed service platform is composed of a home gateway, home gateway manager, and service portal, as shown in Fig. 1.

The home gateway is located between home appliances and the Internet. The home gateway performs not only home router's functions but service support functions including protocol conversions between home appliances and Internet-based services. These service support functions are done by software in the home gateway. These functions can be added as "service module" from the home gateway manager.

The home gateway manager monitors home gateway's running status and controls service module download. The home gateway manager has a bank of service modules that are used to support network services. A service module is sent to a home gateway when a new network service needs it and the home gateway does not have it yet. To perform this operation, the home gateway manager holds internal state of each home gateway that shows what service module has been downloaded and is ready to run.

The service portal is the first access site for user. When a user wants to subscribe a new service, the user firstly accesses to the service menu of the portal through his/her home appliances or PC. Then the user chooses one of the services to subscribe. The portal checks the service profiles that describe required service modules to support the service. The portal requests the home gateway manager to send the service module to home gateways.

Taking this architecture, the service portal can be operated by third parties like application service providers (ASPs). This is because that an ASP only needs to know the service module's name which required for the service. The ASP neither needs to know home appliance's dedicated protocols because service modules convert them to ASP-favorite protocols, nor manage service module download because the home gateway manager takes this role.

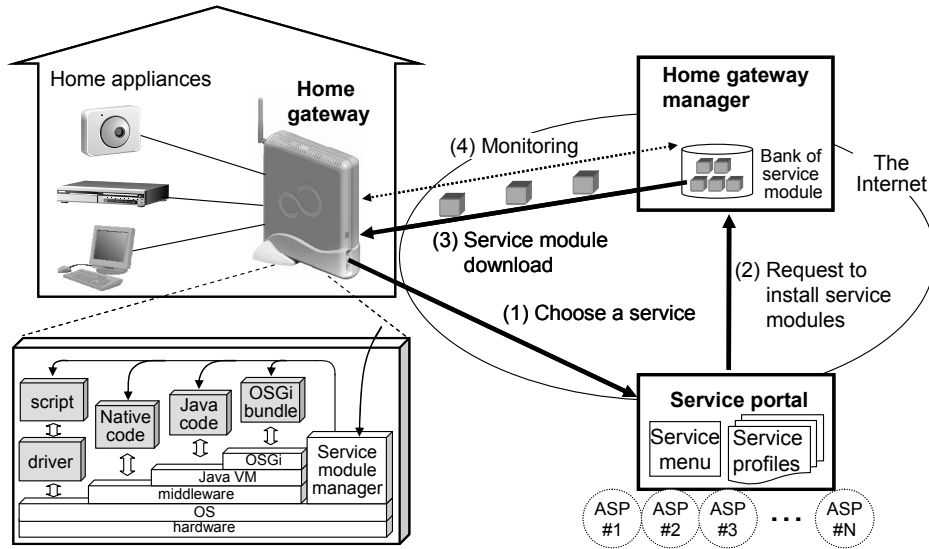


Fig. 1. Architecture of proposed service platform.

### B. Service module

The service module sent from the home gateway management server contains various kinds of software, such as a native application code, Java application code, OSGi bundle [1], script, driver. Comparing to the OSGi based on Java, our architecture handles wide range of software layers of the home gateway. We defined a metadata forming a service module as shown in Fig. 2. The metadata contains a module identifier, module type, installation path, and start/stop profiles. Using this metadata, various types of service modules can be uniformly handled in the home gateway.

### C. Security

To prevent an illegal installation of service modules by unauthorized users, the service platform authenticates home gateway, home gateway manager and service portal based on a digital certificate before they begin to communicate. Also the communication data between each device are encrypted by SSL or IPsec.

```
#MODULE_INFO
moduleID: F001-G002-X500-W030
version: 1.25
moduleName: Security service module
moduleFileName: security.tar.gz
moduleLang: Native code
:
#INSTALL_PATH
path: /service/security/manager
path: /service/security/security.conf
#START_PROCESS
startCmd: /service/security/manager -start
#STOP_PROCESS
stopCmd: /service/security/manager -stop
#END_OF_FILE
```

Fig. 2. Metadata of service module.

### D. Sequence to use a new service

There are five steps to provide a new service to a new user as shown in Fig. 3 and described as follows.

#### (1) Registration of home gateway

When the home gateway is attached to the Internet, the home gateway sends a registration message with its IP address to the home gateway manager. As a result, the manager starts to monitor and control the home gateway.

#### (2) Notification of home appliance's profile

The home gateway finds home appliances attached to the home network automatically using the device discovery protocol of UPnP [2]. Then the home gateway notifies the appliances' profiles including appliance type, model number and capability to the service portal. If there is a home appliance which does not support the device discovery protocol, the user manually registers the appliance's profile to the service portal.

#### (3) Choosing a service

The user accesses the service portal through a web browser of a home appliance, such as an intelligent TV or PC. The service portal provides the list of services available for the user referring the appliance profiles sent from the home gateway. Then the user chooses one of the services.

#### (4) Service module download

The service portal requests the home gateway manager to install service modules needed for the new service. The manager sends service modules to the home gateway if needed. Then a new capability is added to home gateway, and ready to provide the new service.

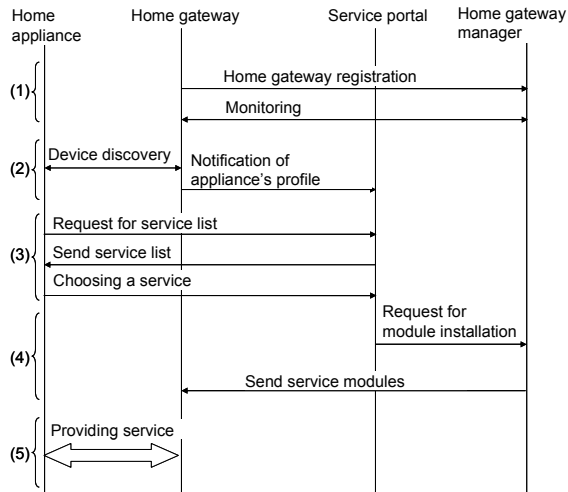


Fig. 3. Flow sequence to start new service.

(5) Use of service

The home gateway setups its internal functions of firewall, routing, QoS based on provided parameters via downloaded service module. Also the home gateway provides device drivers for home appliances, protocol conversions for dedicated appliances if they are needed.

III. REMOTE ACCESS SERVICE

We believe remote access service is one of the key services on this platform. The service enables user to control his/her home appliances from outside. For instance, the service provides door-lock control, surveillance camera viewing, and timer setting of a DVR (Digital Video Recorder) through a mobile phone. To achieve this kind of service, a technology of secure and scalable remote access from the Internet to home is very important.

A. Conventional method

Figure 4 illustrates two conventional remote access methods. The peer-to-peer method has been installed onto some off-the-shelf home router. This method uses source IP address filter of the home gateway to reject illegal access. However this filter is not effective for remote access from mobile terminals because a PC in a hot spot uses a dynamically assigned IP address which cannot be known in advance. Moreover, some cellular phones don't have its IP address. Therefore the IP address filter cannot reject IP spoofing attack.

Another conventional method is gateway relay method. Here, the gateway authenticates user and relay user data to the home gateway over secured path (e.g. IPsec). In this method, the gateway can reject attacks using application-layer filter. Also the home gateway can reject attacks using the IP address filter because the home gateway rejects all incoming session except from the gateway. This method is securer than the peer-to-peer method, but is not

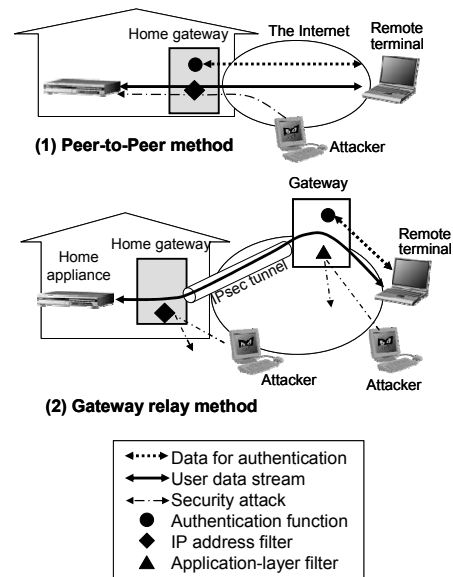


Fig. 4. Conventional remote access methods.

scalable. Because all user data go through the gateway, increasing the number of users and data volume makes the gateway be a bottleneck.

B. Proposed remote access method

In order to solve these issues of conventional methods, we have been proposing a new method of remote access [3]. Figure 5 shows our architecture achieving secure and scalable remote access to home. We place a home gateway and authentication server. The first key of this architecture is that the authentication server assigns an access permission code (a generated random number used as a one time pass word) to each session. The server sends the code to both the remote terminal and the home gateway. The home gateway distinguishes an authorized access using the code. The second key is that the data stream between the appliance and remote terminal doesn't pass through the server. Thus this architecture is scalable from the view point of user count and data volume increase.

The sequence of remote access is as follows;

- (1) First, the user logs in the authentication server with a user ID and password using the web browser of a remote terminal (e.g. mobile phone, PDA or PC).
- (2) After the user authentication, the server generates an access permission code for this session and notifies both the remote terminal and the home gateway. The permission code is generated every access and used as a one-time password in this system.
- (3) The remote terminal user can reach the home gateway with the permission code by just clicking a link sent from the authentication server. The link is a URL of HTTP redirect message to home gateway including the permission code.

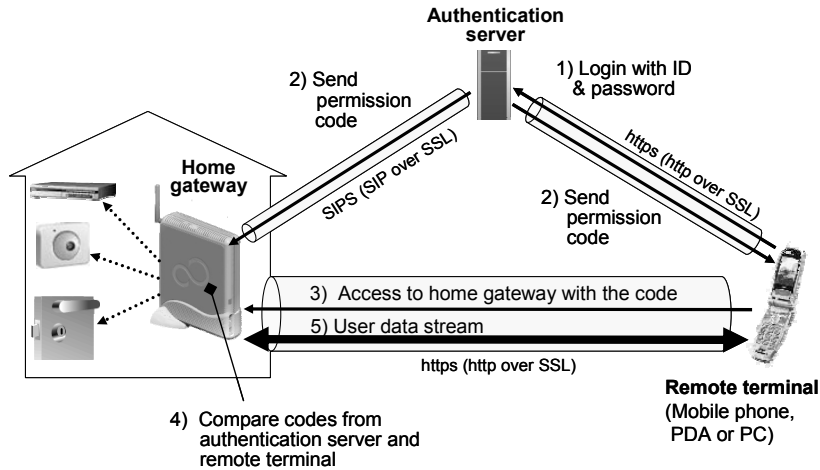


Fig. 5. Proposed architecture and sequence for remote access

- (4) The home gateway compares the permission code received from the center server and the one from the remote terminal. Only when the codes match exactly, the access from the remote terminal is accepted.
- (5) The home gateway sends a web-page-based menu to the remote terminal where the menu is used to control home appliances.

#### IV. PROTOTYPE SYSTEM

To confirm our concept, we have developed a prototype system including home gateway, home gateway manager, service portal, and authentication server.

We have also developed two service modules. One is a module for remote access service that performs our proposed remote access method described in section 3.2. The other one is a module for appliance

control service that enables to control door lock, light, surveillance camera, DVR, and Web server through a web browser running on a remote terminal.

Figure 6 illustrates the prototype system and its service. Firstly user chooses the remote access service by accessing the service portal from her home. Then the portal requests the home gateway manager to install the two service modules. The home gateway manager sends the modules and the modules are installed onto the home gateway. Thus preparation is completed.

The user logs in to the authentication server from her mobile phone. After authentication, she reaches the home gateway securely. Now she can control the door lock through her mobile phone as shown in Fig. 6.

We've confirmed that our prototype system operates appropriately, provides the service examples, and rejects IP spoofing attacks.

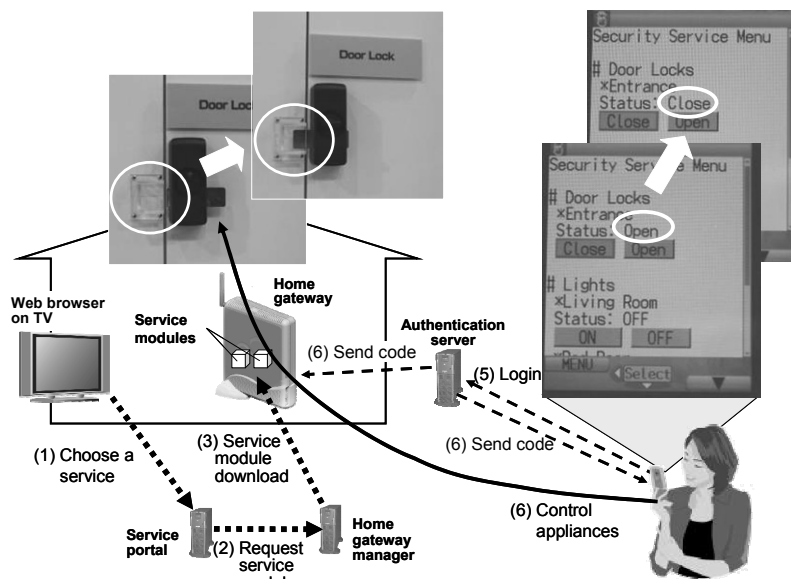


Fig. 6. Prototype system and service.

## V. CONCLUSION

In this paper, we proposed an open platform that enables third parties to provide new network services for home appliances. The platform consists of home gateway, home gateway manager and service portal.

We also proposed a secure and scalable remote access method that will be a key for home appliance control services.

A prototype system has been developed, and we confirmed the proposed architecture is performs appropriately.

## ACKNOWLEDGMENT

A part this work was supported by the National Institute of Information and Communications Technology (NICT), Japan.

## REFERENCES

- [1] OSGi Alliance, “OSGi Service Platform Release 2”, p 16, Oct 2002.
- [2] UPnP Forum, “UPnP Device Architecture”, version 1.01, pp.10-21, May 2003.
- [3] T. Ishihara, et. al., “Home Gateway Architecture Enabling Secure Appliance Control Services”, ICIN 2006, pp 329 – 332, May 29, 2006.