Inf Syst Front (2009) 11:483–490
DOI 10.1007/s10796-008-9122-3

Service integration with UPnP agent for an ubiquitous home environment

Wally Chen · Sy-Yen Kuo · Han-Chieh Chao

Published online: 17 June 2008

Abstract Consumer electronics and intelligent appliances can be successful and widely used in a smart or ubiquitous home environment. Service integration had become an important issue for system development. In this paper, we present an approach for UPnP devices connecting to outer networks via UPnP aware gateway. We develop service on a smart campus network based on enhanced UPnP technologies as an example. Under such framework, intelligent system provides users individual information at the right place and the right time.

Keywords Information technology · UPnP · Ubiquitous computing

1 Introduction

In recent years, various consumer electronic products are actively developed and promoted by vendors. Almost every home has the consumer electronic products such as a videocassette recorder (VCR), a compact disk player (CDP), or a digital videodisk (DVD) player. Consumer electronics and intelligent appliances can be successful and widely used in home networks.

For today's rapidly growing mobile environments, information technology's research is providing middleware for the development of networked health-care systems, and some other applications for various end-user devices (PDAs, mobile phones for instance) and wireless networks (WLAN, Bluetooth for instance). Therefore, accessing electrical products is no longer a privilege for few people who are specialized on high technology. One of the key point for a widely deploy service (create business profit simultaneously, of course) is to lower the knowledge requirements of users. Once those annoying configurations could be omitted, everyone will be glad to enjoy the convenience which is brought by novel inventions.

Networks engineers had already contributed a lot to reduce the complexity of system configuration. One of the most popular examples is DHCP (dynamic host configuration protocol). Hosts (or devices) request and obtain an internet protocol (IP) address from a specific server which has a list of addresses available for assignment. Under present wireless technology, mobile system automatically selects and connects to the most preferred wireless network when it becomes available while the next generation Internet Protocol (IPv6) claims the auto-configuration procedure as its key features. To observe the progress of application services, above-mentioned facts are the best examples which show us that less manual operations brings more business.

Although the development of the communication infrastructure is working well, the application services still didn't keep up with it. One major reason is that those applications are

W. Chen
Department of Electrical Engineering,
National Taiwan University,
Taipei, Taiwan

S.-Y. Kuo (✉)
Department of Computer Science and Information Engineering,
National Taiwan University of Science and Technology,
Taipei, Taiwan
e-mail: sykuo@cc.ee.ntu.edu.tw

H.-C. Chao
Department of Electronic Engineering, National Ilan University,
I-lan, Taiwan

H.-C. Chao
Department of Electrical Engineering,
National Dong Hwa University (Jointly Appointed),
Hualien, Taiwan

developed by different vendors and each of them has their own protocol. Common users won't be comfortable before the compatibility problem had been resolved.

In order to solve above issues, it is necessary to build a framework for handling service discovery. Broadly, a service discovery framework is a collection of protocols which develops dynamic client/server applications (Richard 2000). A number of component protocols are typically included, which allow services to advertise their availability. Under those protocols, clients could search for needed services. In a service discovery-enabled network, devices once has been plugged in, become part of the community and may be discovered. User could access those services with minimum manual configuration.

For the past few years, competing groups have been pursuing automatic configuration, and those are several success models for service discovery, including Jini (Allard et al. 2003), Universal Plug and Play (UPnP), Salutation and so on.

They are designed to support zero-configuration, invisible networking, and automatic discovery for a breadth of device categories from a wide range of vendors. It is a pioneering work that users only need to know their own wanted services but without knowing about where those services are located (Coulouris et al. 2001).

Above mentioned protocols are different. Clients and services will not be able to cooperate in the naïve design even each protocol has similar high-level goals. However, a few engineers have proposed interoperability framework that allows heterogeneous protocols work together. Since it is no longer problem for users to access device in different resource discovery protocols, we won't discuss interoperability issue. In this paper, we only focus on network organizing in one carrier infrastructure-UPnP.

2 Background

The UPnP architecture offers pervasive peer-to-peer network connectivity of PCs, intelligent appliances, and wireless devices. It is well defined protocol targeting to home networks, and networks in small businesses. Following, we briefly illustrate UPnP behavior and discuss the relative performance if we extend its working scale (http://en.wikipedia.org/Universal_Plug_and_Play).

2.1 UPnP

UPnP aims to enable the resource discovery, service control, and consumer electronics. In UPnP, a device can dynamically join a network, obtain an IP address, convey its capabilities upon requests, and get the presence and capabilities of other devices. A device can also leave the network without configurations.

UPnP leverages current networking technologies. It uses the protocol stack in Fig. 1 for service discovery, advertisement, description, and event notification.

GENA (general event notification architecture) was defined to provide the ability to send and receive notifications using HTTP over TCP/IP and multicast UDP.

SSDP (simple object access protocol) defines how network services can be discovered as the name implies. It defines methods both for control point to locate resource of interest on the network, and for devices to announce their availability.

SOAP (simple object access protocol) defines the use of XML and HTTP to execute remote procedure calls. Above protocols enable automatic discovery and description. UDP is used for discovery and events control.

2.2 UPnP networking

Basically, the UPnP framework behaves as following steps:

2.2.1 Discovery

The first step in UPnP networking is discovery. While an UPnP device appears in the network, it advertises its presence to control points via SSDP which provides basic information about the devices and their services. Similarly, when a control point is added to the network, the UPnP discovery protocol allows that control point to search for devices of interest on the network.

2.2.2 Description

After a control point has discovered an UPnP device, the control point must retrieve the device's description from the URL provided by the device in the discovery message. It receives XML message from the UPnP device and get information, such as manufacturer information, serial number, URLs to vendor-specific web sites, and so on. For each

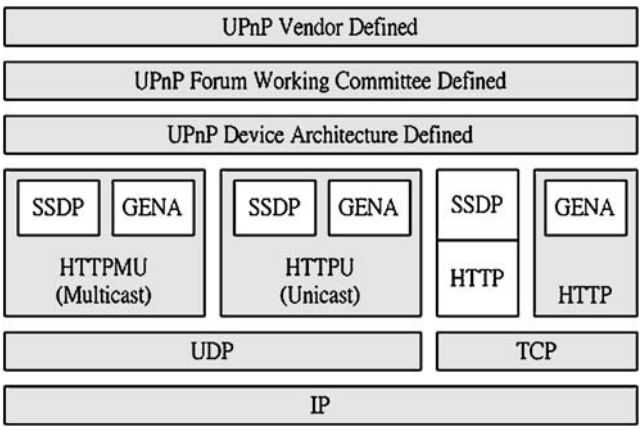

Fig. 1 UPnP protocol stack

service, the description includes a list of the commands or action, to which the service responds, and parameters or arguments for each action.

2.2.3 Control

After a control point has retrieved a description of the device, the control point can send actions to a device's service according to the description information.

2.2.4 Event notification

An UPnP description for a service includes a list of actions the service responds to and a list of variables that model the state of the service at run time. The service publishes updates when these variables change, and a control point may subscribe to receive this information. The service publishes updates by sending event messages.

2.2.5 Presentation

After all, if a device has an URL for presentation, then the control point can allow users to both control the device and monitor device status.

2.3 Extend the UPnP networking

The paper, which we are currently working on, is related to create an intelligent living space on campus. Smart information system provides quality life for both students and administrative staffs. In the past few months, a framework and several services have been established according to the UPnP protocol stack.

At first, we are happy that UPnP shows many advantageous properties and it helps system organizing itself with very little manual operation. Administrators feel good in adding device (or service sites) into the networks with very little configurations. However, we hit difficult point while we try to increase the application domain into a large scale network.

The control point must receive SSDP message in Discovery stage while an UPnP device added into networks. In the system view, if the device and control point are located inside the same LAN, it is fine. The added UPnP device could either multicast or broadcast its presence to control points. Otherwise, the Discovery procedure may not always work since the multicast infrastructure isn't complete everywhere and gateway won't broadcast SSDP message as well. The message dies right away once it reach boundary of LAN (Universal Plug and Play Specification, v1.0).

It is necessary for our paper to break the restriction since we may simultaneously access several devices located in different LAN. For such a purpose, the gateway couldn't be unaware of UPnP protocol. In (Kim et al. 2006), authors propose Internet Gateway that consists of UPnP IGD (internet gateway device), DCP (device control protocol) and the UPnP Bridge for control electrical appliance of Internet home network. Their work is successful and users can have the same control environment in Internet network as at home. Such idea is quite useful for our project and we plan to expand our framework for device cooperation on campus networks.

2.4 Secure UPnP network

Resource discovery and communication are fundamental problems in the networking of devices and services. UPnP is a widely accepted solution for discovering, controlling and monitoring networked appliances. Network installation becomes easy; furthermore, networks can be built in which one terminal controls all appliances and each appliance can be controlled by many different control points. However,

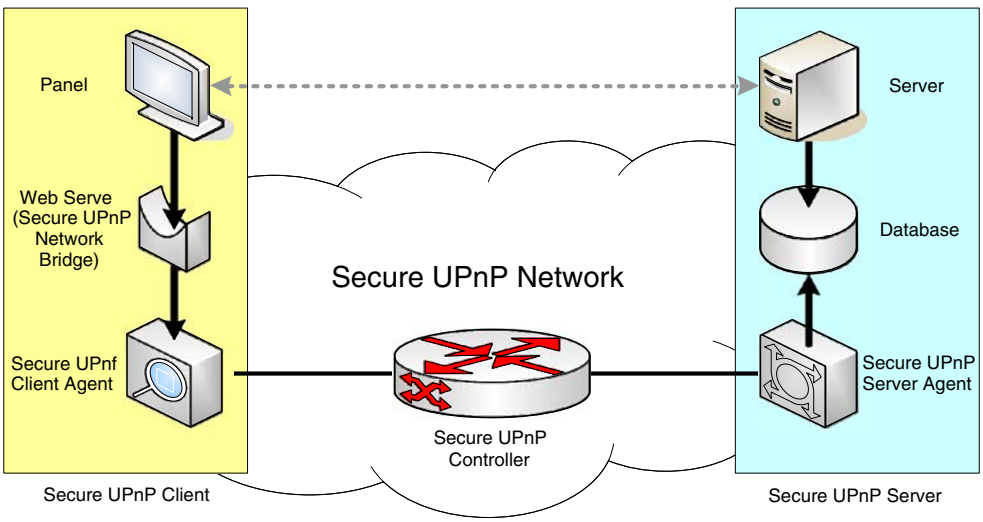

Fig. 2 Secure UPnP network architecture