Pers Ubiquit Comput
DOI 10.1007/s00779-011-0484-z

ORIGINAL ARTICLE

A near field communication-driven home automation framework

Yue-Shan Chang · Wei-Jen Wang · Yung-Shuan Hung

Received: 25 March 2011 / Accepted: 27 October 2011

Abstract Rapid advances in the field of consumer electronic devices have made home automation a research issue of increasing importance. In recent years, one of the most popular and widely used devices in certain consumer electronic applications has been RFID (Radio Frequency Identification) and of particular interest here is Near Field Communication (NFC), a two-way communication technology based on RFID. A setup that has a NFC device embedded in a cellular phone has attracted growing attention for various business applications, among them payments and ticketing. In this paper, we propose a novel application and framework that uses a NFC phone to create a personalized digital home environment. With this proposed setup, by one touch the NFC phone is used to send a request that carries predefined personal preferences to control various home appliances. We present the system architecture and implement the prototype, employing such well-known standards as NFC, OSGi, and UPnP to demonstrate the feasibility of the framework. We then evaluate the performance for efficiency and discuss the merits of the approach.

Keywords Near field communication · RFID · Personalization · Home automation · Digital home · Smart space

1 Introduction

Automation [1] is a key factor in smart home environment and given the advances in many consumer electronic technologies, an increasingly important research issue. Emerging technologies, such as ZigBee [2], mobile phone [3], and IR [4] are making ever more information appliances capable of remote control and thus enhancing convenience in the lives of consumers.

In addition, the smart environment that assists people has acquired extra significance in these times of aging populations. Several such systems have been proposed [5–11, 35, 36], each exploiting advanced technologies to construct a context-aware [5, 9, 12] smart space. In general, they construct a public smart space by acquiring a public context. However, in the smart home environment, what the user prefers is very important, so personalization is certainly a further appropriate issue [13]. The need in the smart home context is to help users employ user preference accurately control their selected appliances and generally create a more comfortable domestic ambience. Additional and in time increasingly necessary considerations in the discussion of an advanced home automation platform are energy saving and carbon reduction, diversity, cost, convenience, and security. An easy-to-use framework especially designed for smart spaces with multiple devices and complex settings will attract and inspire more users.

Y.-S. Chang (✉)
Department of Computer Science and Information Engineering,
National Taipei University, 151, University Road,
Sanhsia, Taipei 237, Taiwan, ROC
e-mail: ysc@mail.ntpu.edu.tw

W.-J. Wang
Department of Computer Science and Information Engineering,
National Central University, 300, Jhongda Rd., Jhongli,
Taoyuan 32001, Taiwan, ROC

Y.-S. Hung
Institute of Communication Engineering,
National Taipei University, 151, University Road,
Sanhsia, Taipei 237, Taiwan, ROC

Published online: 19 November 2011

1.1 Problem and motivation

To illustrate the issue and explain the motivation for this paper, we present the following scenario and description of operations. A user arriving home at a residential community may well use RFID authentication to gain entry. It may then be necessary to go through a sequence of operations to reach the front door. For instance, if arriving after dark, there may be a poorly lit garden path to negotiate before reaching the lobby of a multi-storey building and before spending time waiting for an elevator. On reaching the right floor, it may be necessary to find another RFID key for the front door. Finally, there may be a number of home appliances to be switched on one-by-one: lights, air-conditioner, machine for making a much welcome cup of coffee, and so on.

At least two ways of simplifying such a train of operations has been proposed, namely, the Mobile-controlled Home Automation,[1,2] (MC) and the Web Services-based Home Automation (WS) [14, 15]. With MC, the user has a cellular communication channel via which to send control context and thus remotely control selected appliances. This approach provides control of home appliances anytime, anywhere, but it may incur extra communication cost and needs manual intervention for each configuration, and is not a simple matter if many appliances are involved. With WS, the Internet provides the means of control. Multiple appliances can be configured in each operation through a wired network, which means that extra connection cost is avoided. However, the issue of difficulty here is indeed the means itself, in that the user may need to access to the Internet and the Web point to do the configuring. In addition, with both MC and WS, manual operation is unavoidably necessary, even if the control context is the same for every required occasion.

As is well known, cryptography-embedded RFID inherently enjoys the characteristics of security and privacy [16]. Using RFID as a key implies that authentication and authorization will be checked. Both MC and WS need extra support to check authorization when the user enters the residential community or controls any appliances [17]. NFC[3] [18] is an extension of RFID technology and has an inherent two-way communication capability. NFC protocol distinguishes between two modes of operation: active and passive. With the first, one NFC peer can actively send a message to another, while the second only serves as a passive tag. The NFC phone embeds the NFC device in a cellular phone and can be employed in a growing number of applications [19–21], among them contactless transactions such as payment and transit ticketing. A device of this sort provides simple and fast data transfer including calendar synchronization or electronic business cards, as well as access to online digital content. Not many applications have been built with for control as their purpose [22]. It has also been shown that NFC allows some applications in a pervasive computing environment to be made more personalized, dynamic, and intelligent [34].

1.2 Objectives and contribution

It is possible to effect digital home control operations by an exchange of messages (tags) between a NFC phone and a NFC reader home located at the residential gateway. The control context is easily encapsulated in the message by the Generic Control Record Type Definition (GCRTD) [23] of NFC. The phone can switch operation modes. Therefore, it not only serves as the basic key for authenticating entry to the home environment, but also uses personal preference to control the information for all related, selected appliances. At the time where the phone is used to allow entry to the user, all other operations including authentication can be automatically executed with one touch, delivering home automation control via user preference with no complex interactions. So, any necessary lighting on the way to the lobby can be switched on in readiness, the elevator pre-called to wait, and any domestic appliance activated to a state predefined by the user.

The inherent characteristics of the NFC-embedded phone that demonstrate its suitability for home automation applications are as follows:

1. User preference for appliances: the NFC phone easily carries predefined and pre-stored user preference, with all control contexts automatically exchanged with one touch and no manual operation.
2. Security: the NFC phone serves as the key for checking authority and authentication before controlling appliances.
3. Scalability: the NFC phone has much more storage space than a general RFID [24] and can therefore carry and store multiple preference of a user.

This paper proposes a novel application framework for a NFC device, namely, a NFC-driven personalized digital home environment. The application allows a NFC phone user to deliver predefined personal preferences that will control home appliances in a smart home space, that is, the phone is not only the entry key to the space, but also the means of personalizing the context for control of selected appliances within the space. The framework has two important components, the first the Universal Service framework for an NFC phone (US-NFC), which is a negotiation mechanism between NFC devices, and the

[1] http://www.mobilecomms-technology.com/projects/foma/.

[2] http://blog.neonascent.net/archives/mobile-controlled-home-automation/.

[3] NFC Forum, http://www.nfc-forum.org/home.

second NFC-driven Home Automation Environment (HAE) architecture, which is to infer whether user preference regarding appliances in either space, communal or domestic. As it is based on US-NFC, the phone can automatically exchange key and user preference with the HAE without user intervention.

For greater convenience, a simple context orchestration tool for defining user preference for all appliances is also presented. In addition to the use of NFC, the environment also integrates a variety of digital home standards, such as OSGI[4] (Open Service Gateway Initiative), and UPnP[5] (Universal Plug and Play) to prototype the platform.

Finally, we implement an ARM-based embedded system in the prototype to demonstrate usability and conduct a performance evaluation of efficiency and effectiveness, followed by a discussion of the merits of the proposal.

The contribution of the paper can be summarized under three headings:

1. A novel application of NFC to home automation is proposed, with a design for an architecture that ties NFC to standards for that automation.
2. A Universal Service framework for the phone (US-NFC), designed as a negotiation mechanism between NFC devices, was used to construct a flexible NFC-driven Home Automation Environment (HAE) architecture that was suitable for inferring user preference for appliances both in communal and domestic spaces.
3. A simple authoring tool for creating user preference for all appliances was presented, as well as a prototype to demonstrate the feasibility of the architecture and evaluate the performance and efficiency of the system.

The remainder of the paper is organized as follows. Section 2 introduces the NFC and surveys related works. Section 3 presents the Universal Service Framework for NFC and depicts an application scenario. Section 4 has a detailed explanation of the HAE architecture, including the components and operating procedures. Section 5 depicts the system prototyping, followed in Sect. 6 by a performance evaluation. Finally, conclusions are presented and future work discussed in Sect. 7.

2 Background

2.1 Near field communication

NFC, based on RFID technology, is a short-range high-frequency wireless communication technology. It enables the exchange of data between devices over a distance of about 10 cm. The technology is a simple extension of the ISO 14443 proximity-card standard that combines the interface of a smartcard and a reader into a single device. A NFC device can communicate with both existing ISO 14443 smartcards and readers, as well as with other NFC devices, and is thereby compatible with contactless infrastructure already in use for public transportation and payment. Figure 1 shows a NFC reference implementation framework.[6] That device can be used either in Peer-to-Peer mode or in tag read/write mode. The device discovery can switch the mode: in our work, we mainly employ the Peer-to-Peer mode for exchanging control context.

As mentioned above, the NFC device can be utilized for peer-to-peer message exchanges, simply by bringing the devices close together. A protocol automatically enables this peer-to-peer communication. These communication modes can be found in [25]. The NFC chip embedded in the mobile device reads the information in the tag, thus emulating a smart card, so that the reader can access its data, or can communicates directly with another NFC device. Obviously, NFC technology combines two paradigms, the one being communication between devices, where both have active power supply and computing capabilities, and the other being communication between powered devices and passive tags. Such a mechanism is necessary for many applications, e.g., file transfer, authentication and authorization, smart poster, and control context.

Some NFC phone manufacturers have provided a proprietary Java 2 Micro Edition (J2ME) API for developing mobile applications that make use of NFC capabilities. Siemens has a NFC Service Platform [26] and Nokia a NFC and RFID API [27] to allow the development of such applications. Currently, many mobile phone vendors support the development of Java Specification Request (JSR) 257 Contactless Communication API[7] to define a standard API for contactless communication with RFID/NFC tags or bar codes.

The NFC forum has defined certain specifications for message exchange, such as NFC Data Exchange Format (NDEF),[8] NFC Record Type Definition (RTD),[9] and Type 1/2/3/4 Tag Operation Specification. The NFC Data Exchange Format (NDEF) specification has defined a message encapsulation format for exchanging information, e.g., between one NFC Forum Device and another, or an NFC Forum Tag.

[4] OSGi Alliance, http://www.osgi.org/Main/HomePage.

[5] UPnP FORUM, http://www.upnp.org/.

[6] NFC Forum, http://www.nfc-forum.org/home.

[7] JSR 257: Contactless Communication API, Version 0.85, Public Review Draft, October 5 2005, http://www.jcp.org/en/jsr/detail?id=257.

[8] NFC Forum, "NFC Data Exchange Format (NDEF 1.0)", NFCForum-TS-NDEF_1.0, 2006.7.24.

[9] NFC Forum, "NFC Record Type Definition (RTD 1.0)", NFCForum-TS-RTD_1.0, 2006.7.24.

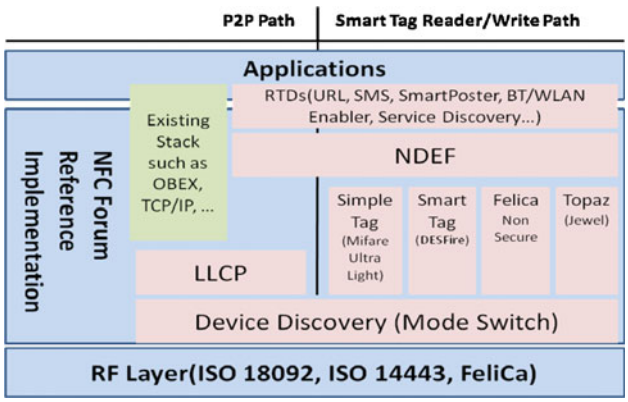

Fig. 1 NFC reference implementation framework

NDEF is a lightweight, binary message format that can be used to encapsulate one or more application-defined payloads of arbitrary type and size into a single message construct. Each payload is described by type, length, and optional identifier. In addition, the NFC forum also defines certain Record Type Definitions (RTD) that are intended to support NFC-specific applications and service frameworks by providing a means for reserving well-known record types, and third party extension types. Figure 2a shows the structure of the Generic Control Record Type Definition (GCRTD) [23], while Fig. 2b showing an example of message format. Based on GCRTD, the control context of a smart space can be easily exchanged between an NFC phone and reader.

Among the wireless communication technologies that have been developed for use in the home automation environment is Bluetooth, ZigBee [2]. In Table 1, we make a simple comparison between such technologies, concentrating on four main aspects; security, personalization, flexibility, and power consumption. Security in the home is obviously important [29]. NFC and RFID are short-range communication technologies (10–20 cm) and clearly offer higher security than the other two approaches shown. As for personalization, both NFC and RFID serve as keys, while also storing control context in their devices and offering greater personalization than the others. It is the case that that the Bluetooth does have medium personalization and has been widely used in handheld devices. The flexibility in the comparison mainly concerns the question of replacing the control context, which the RFID user will find is not easy. Concerning power, neither RFID nor NFC use power for their passive mode and for transmission only very low power is required for the short-range the device.

2.2 Related work

Much interesting research into related systems has taken place over recent years [2, 4, 7, 12, 28], but many of the proposals have either lacked sufficient attention to personalization or have needed complex operations on the part of the user. The following is a discussion of those works.

Georgia Tech's Aware Home [7] was a prototype for an intelligent space that constituted a living laboratory aware of itself and of the activities of people within the system. It combines the context-aware and ubiquitous sensing, computer vision-based monitoring, and acoustic tracking. Massachusetts Institute of Technology (MIT) and TIAX LLC[10] has been working on the PlaceLab initiative [6], which was a part of the House_n[11] project, the research mission for which is to design and build real living environments—"living labs"—that are used to study technology and design strategies in context, in this instance, a one-bedroom condominium with hundreds of sensors installed in nearly every part of it.

Kim and Lee [12] proposed a personal context-aware Universal Remote Controller (URC), a system that allows users connected to it to control home appliances in their own preferred manner. It is runs via a home server, which supports service discovery and user repositories and allows access to any public universal remote controller. Although personalized control is supported, it is not user-friendly control, seen in the fact that appliances in question require complex interaction, quite unlike one-touch NFC.

Han et al. [2] proposed remote-controllable and energy-saving room architecture with an automatic standby power cut off outlet and the ZigBee controller with IR (Infrared radiation) code-learning functionality to configure the architecture. The outlet monitors power consumption periodically, with the effect that when the power reads below threshold, it is automatically cut off at the outlet, thus reducing wastage during standby. What this system lacks, though, is sufficient consideration of personalization in the digital or smart home environment.

Park et al. [4] proposed a dynamic control scheme for multiple legacy IR-controllable consumer electronic devices based on IEEE802.15.4, especially on ZigBee protocol. Their scheme uses a URC unit based on ZigBee WPAN, termed Z-URC (ZigBee-based universal remote control), and a "Z2IR (ZigBee to infrared)" conversion module for converting control messages transferred through the ZigBee network into IR typed control signals. The list of devices to be controlled here by the Z-URC dynamically varies, that is, they are added or dropped depending on the location of the Z-URC unit carried by the user from place to place. A further disadvantage is that personalization for the smart environment has not been considered.

NTT DoCoMo has developed a controller that enables home appliances to be operated with 3G FOMA[12]

[10] http://www.tiaxllc.com/.

[11] http://architecture.mit.edu/house_n/placelab.html.

[12] http://www.mobilecomms-technology.com/projects/foma/.

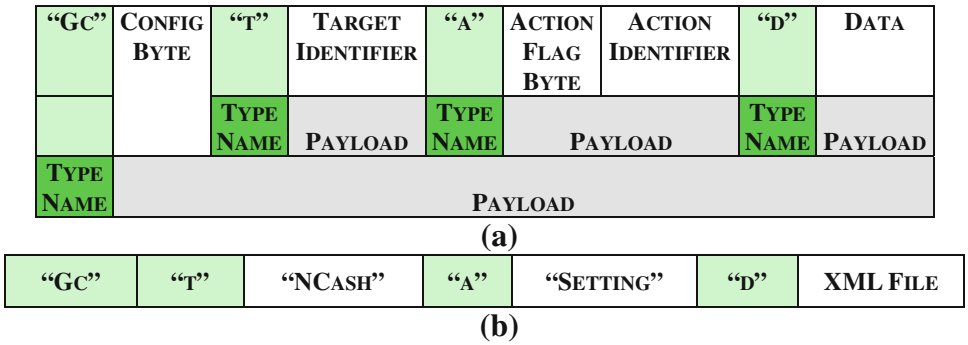

Fig. 2 **a** The structure of generic control record type definition (GCRTD), **b** Message format example

Table 1 Compare NFC with other wireless communication technologies

	RFID	Bluetooth	ZigBee	NFC
Security	High	Low	Low	High
Personalization	High	Medium	Low	High
Flexibility	Low	High	High	High
Power consumption	No	High	Low	Low

videophone handsets, enabling remote operations such as programming TV recordings and playback; switching lights and air-conditioning on and off and viewing live surveillance video of the user's home, sent automatically whenever sensors located there detect movement. The problem, though, is the same as with Kim's solution [12]. The system does support personalized control of appliances, but instead of it being a user-friendly operation, the control requires complex interaction on the part of the user.

Nichols and Myers [28] proposed a framework for automatically generating appliance interfaces from abstract specifications of appliance functions. The interfaces here give users full control of appliance functionality and are consistent with any other interface the phone has, which allows leverage of existing knowledge. Although supporting personalized control, their system does have problems with connection cost and security.

3 Universal service framework for near field communication

The proposed NFC development toolkits listed above in Sect. 2 all lack a negotiation protocol for interacting between NFC devices. Without this negotiation protocol, the user must manually select the tag that conveys user preference messages between reader and phone. The phone holds multiple keys and tags relating to a variety of operations in the smart space, and via the reader the user manually selects the relevant keys and associated tags to contact the NFC phone. It is our intention to short circuit such needlessly complex operations by proposing instead the modularized Universal Service Framework for an NFC platform that we term US-NFC. We here describe the architecture and components of the device.

To design an architecture to suit possible future applications also, we divide the US-NFC into three layers shown in Fig. 3, Application Layer, Core Layer, and NFC Interface Layer. The Application Layer includes all applications on the framework. These interact with the Core Layer via the Dispatcher module. The role of the Core layer, the main part of the device, is to manage, parse, and store all tags received from another peer with which it will negotiate. The Interface Layer, the hardware part of device, sends and receives the RF field. When a request sent by an application interacts with one peer, the Interface Layer initiates a RF field for sending it to another.

The Core Layer consists of Dispatcher (DP), Application Registry (AR), Record Manager (RM), Record Parser (RP), NFC Repository (NFCR), AppName Repository (ANR), NFC Controller, and Network Connector. Their functions are briefly described as follows:

- *DP* A bridging component between a NFC layer and applications. It is mainly responsible for parsing exchanged messages (or tags) and dispatching them to related components for further processing.
- *AR* A launched application needs to register itself before it can receive any message from a peer and the DP can deliver a related request or message to it. The AR is the place where information relating to registered applications is kept.
- *RM* A NFC device may hold multiple tags for various applications and the user might also receive tags from smart posters and keys (tags) for entering a smart space. The RM is designed for managing the tags stored in the NFC Repository.
- *RP* Responsible for encapsulating a request (tag) into a NDEF message and de-encapsulating a NDEF message into a request (tag).
- *NC* Offers a connection capability to wireless channels such as GPRS or Bluetooth for access to other networks.

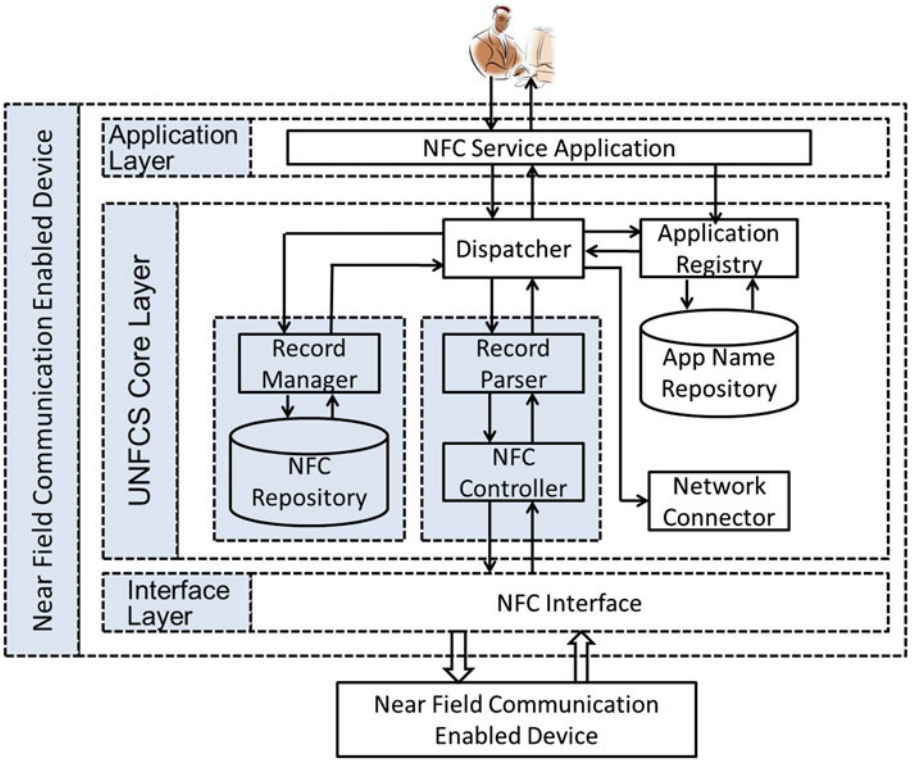

Fig. 3 The architecture of universal NFC service framework

- *NFC Controller* Monitors the state of NFC hardware and controls switching between communication (active/passive) modes.
- *NFC Repository (NFCR) and AppName Repository (ANR)* Both used for storing tags and application ID in the framework.

Possible applications of NFC [29] can be classified into the five categories of Authentication, Payment, Data Exchange, Device Setting, and Unknown, each with a different operation flow. Figure 4 shows the task of these modules and the flow for authentication using the US-NFC. (We do not refer in the following description to operation flows for any of the other categories.) First, the NFC phone is set to Receive Mode to deal with requests from the NFC reader, e.g., located at the entry to a residential building. Dispatcher calls NFC controller to set the mode. Then, the phone contacts the reader and receives a request (tag) for an authentication key via a message. NFC Interface delivers the request to Dispatcher via NFC Controller and Record Passer. On receiving the request, Dispatcher notifies the User and asks Record Manager for a properly authorized key. After calling Record Parser, the resulting authentication check is packed as a tag and sent to NFC Controller. Finally, the result is reported to the reader via NFC Interface. The detailed flow is shown in Fig. 4

The diverse applications highlight the necessity for an extensible and scalable message format between NFC peers, a need that we answer with our designed NDEF for the US-NFC. Although the GCRTD can be used to encapsulate a control message to initiate a desired action, it is difficult to verify what kind of registered application will be invoked. An example of message exchange is shown in Fig. 5. "AU" in "Service Type" means that the message has to do with checking authentication. "Application Name" field identifies the name of the application to which the request is addressed. "Decision Code" can be used for various applications, but here carries the requested gate ID. "Content" field can be used to deliver the content of the request. Here, the value "FFFFFFFFFFFFFF" means that it is a request message for authentication, while the other refers to the content of a tag. For example, the control context for a selected appliance will be encapsulated into the field. In addition, all fields are encapsulated into the GCRTD of the NFC.

The example shown in Fig. 5 is that of a user wishing entry to a residential building, where the NFC reader at the main entrance asks for the authentication key. When the NFC phone receives that request, it extracts Decision Code so as to ascertain the relevant authentication code, which it then packed into a tag before finally responding to the tag in the NFC reader.

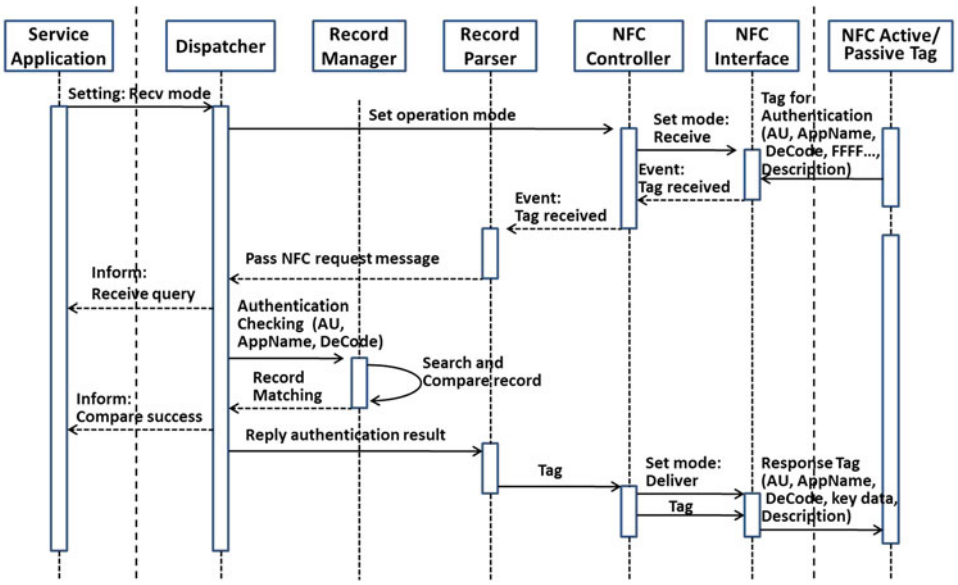

Fig. 4 The flow of authentication using the US-NFC

4 Home automation architecture

This section presents the architecture for constructing the NFC-driven home automation framework.

4.1 Architecture

The architecture shown in Fig. 6 comprises four parts: *Front End* (FE), *Community End* (CE), *Home End* (HE), and *Appliances End* (AE). FE involves a NFC phone and reader located at a residential community entrance, providing for general security control. CE controls communal appliances via the components of *Manager*, *Authentication Module* (AM), *Control Flow Processing Module* (CPM). *Manager* controls managing and dispatch operations in CE *and* also relays control context to the next CE or HE. AM checks authorization and authentication. CPM schedules the control of appliances according to control context. The functions of HE and HE are similar, with the first controlling appliances in the home and the second communal appliances.

If the home is a stand-alone building with no communal parts, the CE can be easily removed without modification. Similarly, if the home is part of a larger community, CEs can be easily added into the system in a parallel or serial manner to extend management to both kinds of appliances, as shown in Fig. 7. It may be the case that there are n CEs on the way to an HE; so that the path to HE may be FE $\rightarrow$ CE_1 $\rightarrow$ CE_2 $\rightarrow$ … $\rightarrow$ CE_n $\rightarrow$ HE. Each CE needs to relay remaining control context to the next CE or HE. For example, as in Fig. 7, if the user lives at residence number Room *3F25* of Building *A*, the control context will be relayed to the HE of Room *3F25* from the CE of the communal entrance and to the CE of Building *A*. Obviously, the design can gain system flexibility. AE is a set of home appliances that are UPnP-embedded and controlled by the OSGi-based Home gateway. Each part can be connected by existing network protocols, such as the Wi-Fi, HomeRF or Power Line Communication network.

Based on observation of Fig. 7, an overall tag for controlling all appliances is needed. The control context C for all appliances consists of n two-tuple elements, which is defined as follows:

$$C = \{ <Key_1, C_1> , <Key_2, C_2> , \ldots, <Key_n, C_n> \}$$

When n is equal to 1, it means that the user resides in a stand-alone building. Each tuple is a pair involving a Key_i for authentication and control context C_i of the layer i on the path to home. Each Key_i and Key_j, $1 <= i, j <= n$, can be the same or distinguishable, depending on the implementation. The ith CE will get the pair Key_i and C_i. When a NFC user employs a phone to contact a reader to gain entry to the community, the reader sends a request involving control context C. The NFC device initiates whole control context C delivery, and then the reader delivers context C to *Manager* of CE or HE. The first CE (CE_1) extracts Key_1 and C_1. If Key_1 is authorized, then C_1 will be delivered to CPM for further processing, and then to process control according to user preference. The remaining tuple of the control context, say $\{<Key_2, C_2>,\ldots,<Key_n, C_n>\}$, is forwarded to the next CE (CE_2). Control context C_i is an implementation issue that will be described in detail in Sect. 5.

4.2 Function and components of CE and HE

This section describes the function, components and application scenario of CE and HE. All these components

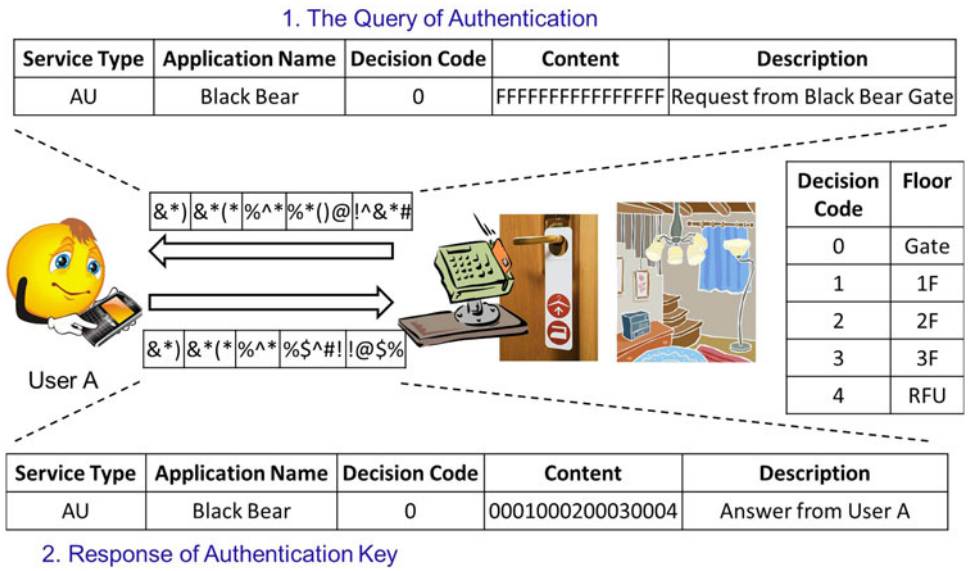

Fig. 5 Message format and exchange for authentication between NFC peers

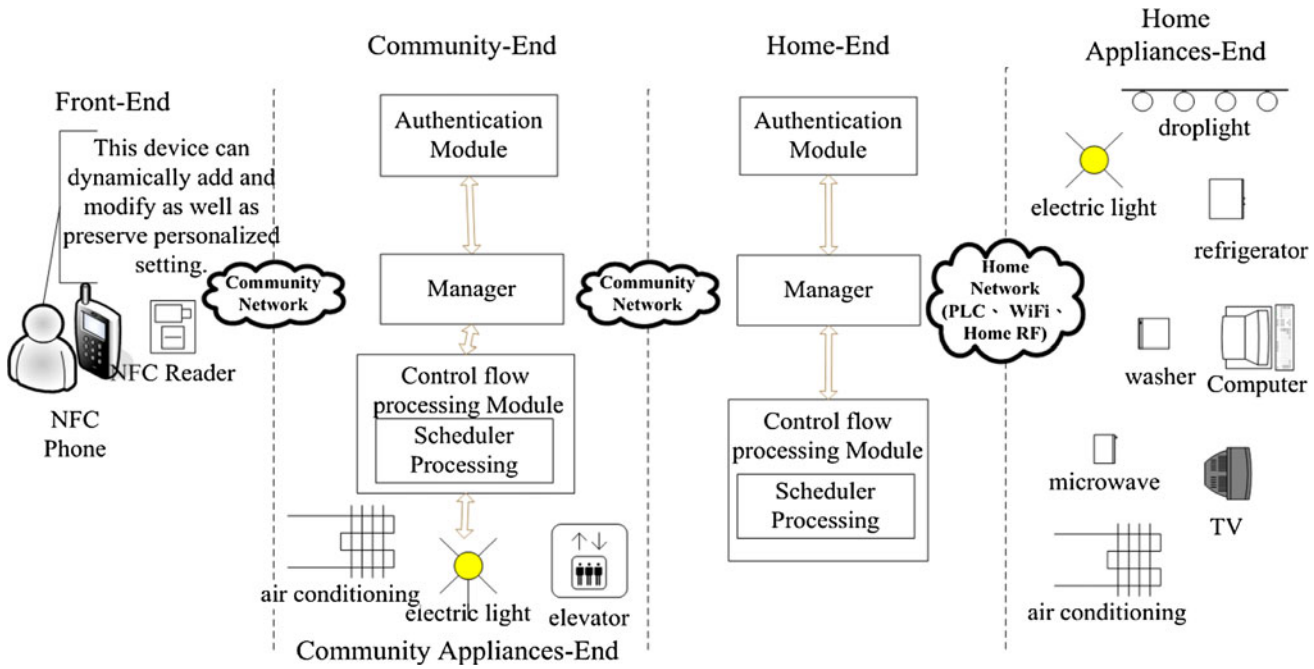

Fig. 6 System architecture

can be implemented as an OSGi bundle.[13] The main function of CE is as a control gateway to mediate the process and control the appliances in the community. As mentioned in the previous section, the CE consists of an *Authentication Module*, a *Control Processing Module* and a set of communal appliances. Here, we depict these components in details as shown in Fig. 8.

Manager This component can be implemented as a *Manager bundle*. When a control context is sent to Manager, it extracts *Key* and launches AM to check authentication and extracts and sends context to CPM for further processing.

Authentication Module (AM) AM involves *Member Database*, *Entry Record,* and *Authentication Bundle*. AM is mainly responsible for checking user authentication and recording user entrances for security. To improve security,

[13] A bundle is a group of Java classes and additional resources equipped with a detailed manifest file on all its contents, as well as additional services needed to give the included group of Java classes more sophisticated behaviors, to the extent of deeming the entire aggregate a component.

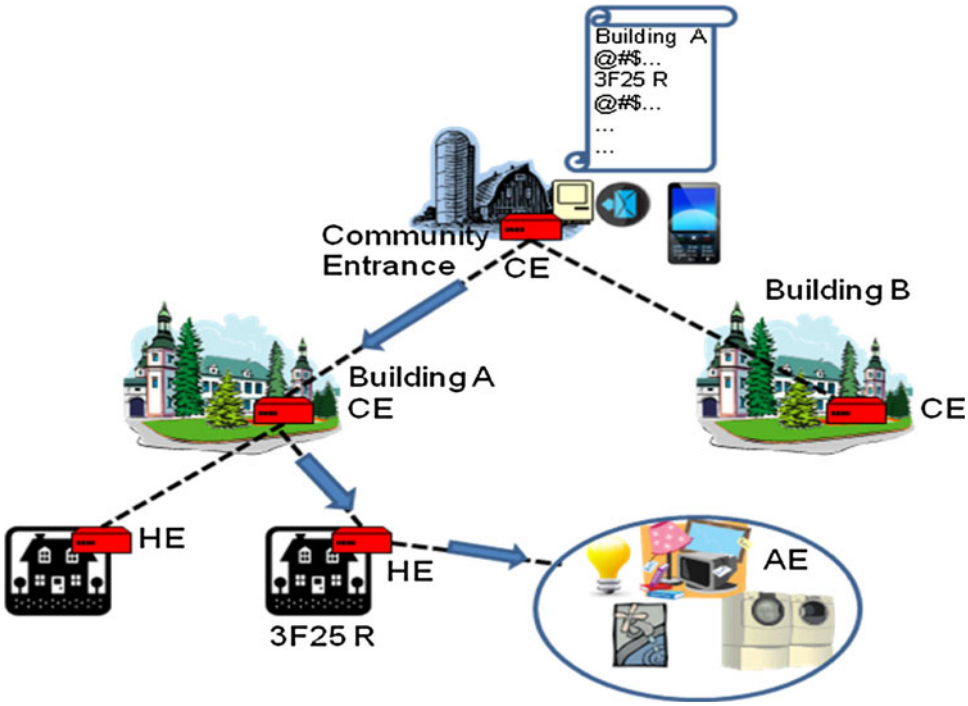

Fig. 7 A macro view of the architecture of home automation

a certain cryptography algorithm can be implemented in the *Authentication Bundle.*

Control flow Processing Module (CPM) CPM is responsible for retrieving control context (C_i), scheduling the operation of appliances and monitoring their states. CPM consists of *Control flow controller bundle (in short, Control Bundle,* CB*)*, and *Control Point bundle (in short,* CPB*)* of Appliances. When a user request sent by the NFC phone arrives, CB extracts the control context and schedules the initiation of appliances.

Services Each appliance is a kind of device. In the framework, we adopt UPnP, which is a set of networking protocols that allow devices to connect seamlessly, to simplify the implementation of networks in the home, and to emulate all the appliances. Each device may have one or many services to be invoked.

The main function of HE is as another control gateway for a home appliance. When Manager of CE receives a request from a user, it relays the control context of the appliance to HE. Similarly, the Manager of HE parses the request, extracts the control context, and schedules execution of the appliance. Most functions and components in HE and CE are almost the same, with the only difference being that while Manager of CE needs to relay any remaining context to the next CE or HE, HE does not, since it is at the end in the control path. Although the functions of HE and CE are almost the same, the reason for separating them is that HE is in general a private device and can only be accessed privately, while CE can be accessed publicly.

4.3 Execution flow

Figure 9 shows a partial execution flow, i.e., only that for controlling communal appliances, which is, however, the same as that for home appliances. First, a NFC phone contacts a NFC reader and sends a RTD message comprising a NFC tag of the request to the reader. Then, the reader delivers the RTD message related to the request to the *Manager bundle* of CE. Next, *Manager bundle* extracts *Key* from the RTD and checks user authorization and authentication. The process of authentication depends on the algorithm utilized in the module. In our prototyping, we only use a simple key matching process. If the user is authorized to enter the community and control appliances, *Manager* extracts the control context that is related to communal appliances and then invokes CB by sending a user request. CB then schedules execution of control of appliances according to the context. Lastly, CE relays any remaining control context to the next CE or HE. All control processes and monitoring are executed via CPB.

5 Implementation

In implementing the framework, to enhance the scalability of home automation, we adopt a variety of well-known standards, such as OSGi for gateway control, UPnP for servicing appliance, an embedded system for emulating appliances, and XML for formatting the control context. Most appliances are implemented with an embedded

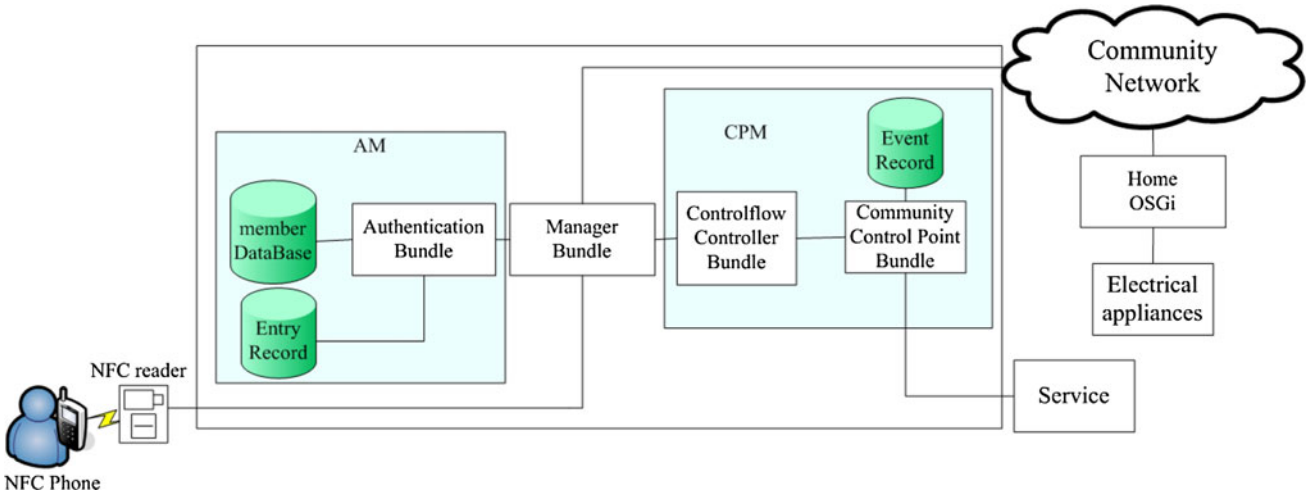

Fig. 8 Community control gateway architecture

system. In addition, to demonstrate the system and measure performance, we also design a control flow authoring tool and prototype the whole set-up.

5.1 Personal preference orchestration

In this system, the user needs to prior orchestrate personal preference and store it in the NFC phone. To offer a flexible environment, the preference can be presented in XML format and changed dynamically. To facilitate the pre-orchestration, we implement an authoring tool termed *Control Flow Designer* (CFD) for visually defining user preference, as shown in Fig. 10. The tool allows the control flow of appliances to be regulated, with each appliance viewed as a node in the flow. The nodes are so connected as to indicate that appliances can be activated sequentially. However, if required the nodes can be executed in parallel. A design for such operations has the following features:

- *Visualization* Devices can be individually configured visually with no technical labeling needed.
- *Initiation time presetting* Timing of activation of devices can be predefined individually.
- *Execution flow presetting* Activation of related appliances can be orchestrated in sequence.

For example, on arriving at the residential community and initiating the contact between the NFC phone and reader, the user may wish first to switch on *Hot-Water Heater* and set to 60°C. This operation will be activated 10 s after making the phone/reader contact. After 20 s, *Lights* and *Air-Conditioner* in the living room will switch on, and so on. The flow in Fig. 10 shows the generation of an XML-formatted control, orchestrated in *NCASHAction* language. Figure 11 shows the partial control context in *NCASHAction* language. The orchestration is easily stored in the phone and encapsulated in a tag of RFID for delivery

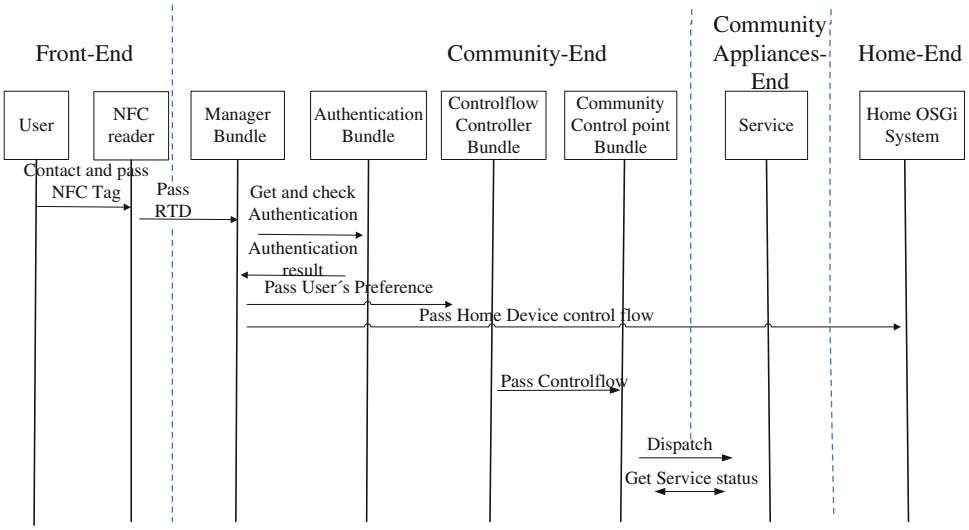

Fig. 9 The execution flow in CE

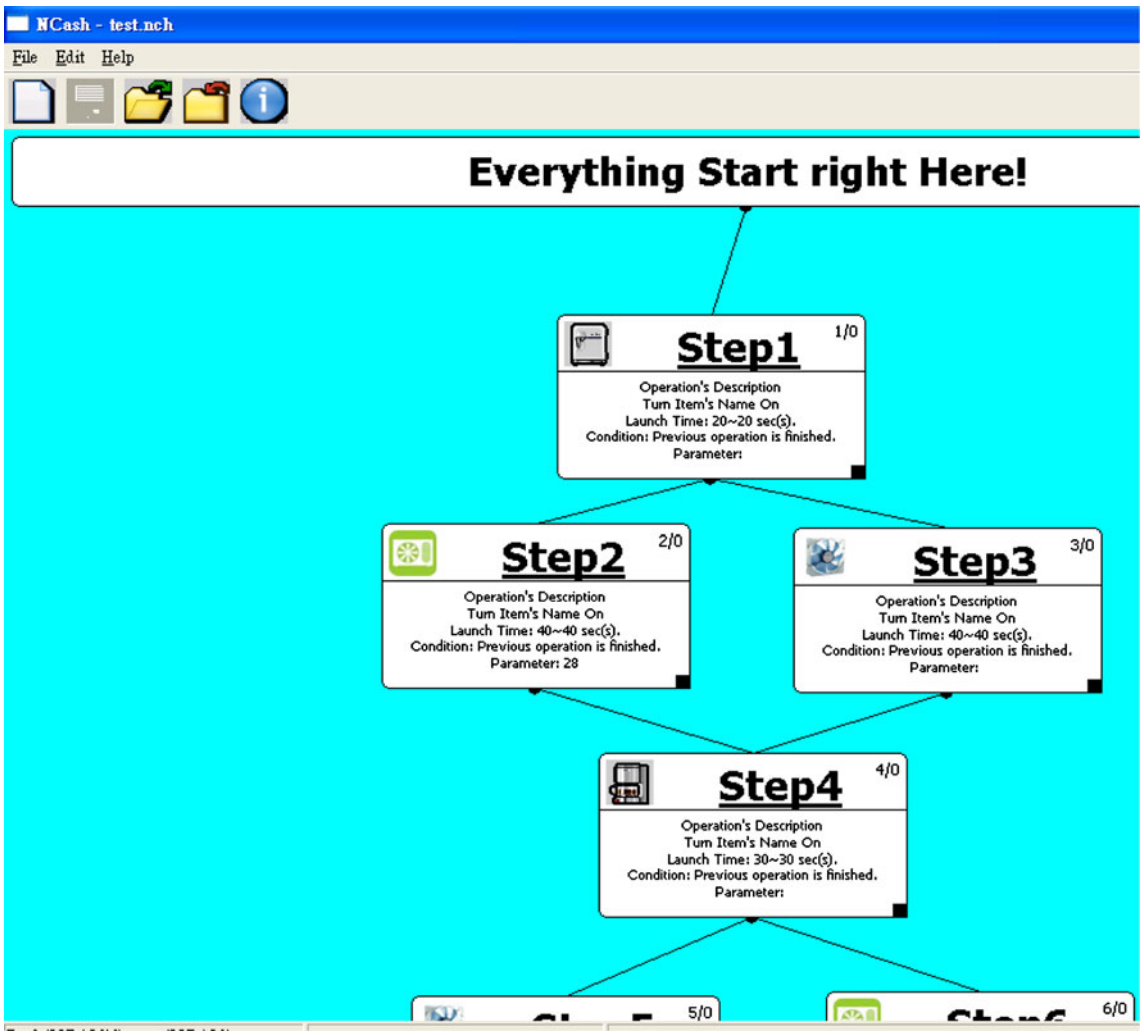

Fig. 10 Control flow designer

to the reader via NFC interface. The following is a list of the XML tags: *RefID*, *StartTime*, *Control Act*, and *FolID*. Taken in order, *RefID* simply shows the sequence of control context, *StartTime* refers to the remaining time for initiating a device, *Control Act* represents the action of a device, and *FolID* refers to the ID of the next device to be initiated.

5.2 Control bundle implementation

In this work, each component of CE and HE was implemented as an individual bundle using Prosyst's Equinox Framework[14], that is, an OSGi framework. These bundles can invoke each other to complete a user request. The function of most HE and CE components are similar. Here, we only depict the implementation of HE.

As shown in Fig. 9, when CE receives a NFC request for authentication for a user wishing entry to the residential community, *Manager bundle* extracts the context that is encapsulated in the request message and sends it to HE. Then, as shown in Fig. 12, HE executes the following steps. *Manager bundle* extracts the user ID, saving the control context in a XML file for further processing, and then sends the ID to Authentication bundle to check authentication. If authentication is ok, *Manager bundle* sends the context formatted in XML to CB for scheduling control, which is done by invoking Control Point step-by-step. The following shows the sequence of operations by which CB reads and schedules control context and passes context FOR each device to *Control Point Bundle*.

1. Read control context, which is in XML format, as shown in Fig. 11.
2. Parse the XML-formatted control context and constructs it as a *DOM* tree.

[14] Prosyst's Equinox Framework, http://dz.prosyst.com/oss/.

```
- <Initial-NCashAction Name="Start" ACTID="0">
    <System>Open NCash System</System>
    <System>Time Count System</System>
    <Next>1</Next>
  </Initial-NCashAction>
- <NCashAction Name="Step1" ACTID="1">
    <RefID>0</RefID>
    <StartTime Costtime="1">10</StartTime>
    <Control Act="On" Set="60">hot-water heater</Control>
    <FolID>2</FolID>
    <FolID>3</FolID>
  </NCashAction>
- <NCashAction Name="Step2" ACTID="2">
    <RefID>1</RefID>
    <StartTime Costtime="1">20</StartTime>
    <Control Act="On" Set="28">living room air conditioner</Contrc
    <FolID>4</FolID>
  </NCashAction>
- <NCashAction Name="Step3" ACTID="3">
    <RefID>1</RefID>
    <StartTime Costtime="1">20</StartTime>
    <Control Act="On">living room light</Control>
    <FolID>4</FolID>
  </NCashAction>
- <NCashAction Name="Step4" ACTID="4">
    <RefID>2</RefID>
    <RefID>3</RefID>
    <Condition>and</Condition>
    <StartTime Costtime="1">30</StartTime>
    <Control Act="On">Coffeemaker</Control>
    <FolID>5</FolID>
    <FolID>6</FolID>
  </NCashAction>
- <NCashAction Name="Step5" ACTID="5">
    <RefID>4</RefID>
```

Fig. 11 Partial control sequence of home appliance

3. One a *NCashAction* node is received, start the scheduling.
4. Read the content of *NCashAction.*
5. Pass the control context for each device to *Control Point Bundle* (CPB).
6. Repeat steps 3–6 until end of file.

5.3 System prototyping

In this prototyping, we utilize a WAVE-TEK WR100 RFID/NFC HF Reader[15] to perform the functionality of a NFC device, which can transmit data up to 424 Kbps. We also use a FUJITSU LifeBook-U1010 UMPC to tie the reader to emulating a NFC phone. The emulated phone can contact the reader, which is installed in a desktop, as shown in Fig. 13a. When emulated phone contacts the reader, it not only sends the *Key* that allows entry to the residential community, but also the personal preference encapsulated in GCRTD. In addition, we emulate home appliances using a DMA-2400XP embedded system, as shown in Fig. 13b. All appliances are connected in a 100 Mbps Ethernet network. The community gateway (CE) is run on a Notebook with Pentium Dual Core CPU, 1.86 GHz, 2.00 GB RAM and the home gateway (HE) on a UMPC with Pentium M processor 1.73 GHz, 1.49 GB RAM. To demonstrate the feasibility of the proposed architecture, we emulate all the home appliances by porting a UPnP code into the embedded system. Then, we add the control code segment of the peripheral device into the UPnP stub. Finally, we port the UPnP device code into the embedded system to emulate the home appliances, so that Control Point Bundle (CPB) can utilize UPnP protocol to deliver the control code to these UPnP devices. Finally, we implement home appliances to demonstrate feasibility, as shown in Fig. 13c.

[15] http://www.wave-tek.com/Products_CHT.htm.

6 Performance evaluation and discussion

6.1 Performance measurement

Performance measurement is important in evaluating a real-world system. To measure system performance, the total latency of the system can be defined as follows:

$$\text{Total latency} = T_{\text{NFC}} + \sum_{i=1}^{n} T_{\text{CE}_i} + T_{\text{HE}}$$

where n is the number of CE on the path to the home of the user. T_{NFC} is the time consumed at reader NFC, $T_{\text{CE}i}$ is the time consumed at CE, T_{HE} is the time consumed at HE

We assume here that if each CE and HE records the same time consumed, the total latency can be simplified to $T_{\text{NFC}} + (n+1)T_{\text{CE}}$. Because the transmission rate of the NFC device is up to 424 Kbps, the T_{NFC} can be simply obtained by computing transmission time between NFC peers. Therefore, performance measurement can be directly divided into two parts, the first being US-NFC, and the second, CE. In the measurement of the first, the latency of US-NFC obviously dominates the overhead of front end, while the NFC reader also utilizes the US-NFC platform.

First, we measure the latency of the key setting. When a NFC phone is intended to serve as the entrance key to the smart home, it must first set an authentication key. Figure 14 shows the latency of the key setting. The phone sends the key setting to the reader, which receives and parses the request, and extracts the authentication key from the request, and stores it in the NFC tag repository. As shown in Fig. 14, the latency of receiving and parsing the tag consumes less than 0.4 ms, which is the major part and dominates the latency. The time consumed by RM (Record Manager) is less than 13 μs, and DP less than 5 μs. The total time consists of that spent by the phone sending the tag and that of the reader receiving it. Obviously, it is near double the latency consumed by a single component, which is reasonable. However, the latency does not affect the system performance.

Second, we measure the latency of authentication. Here, we assume that the phone keeps multiple entrance keys for

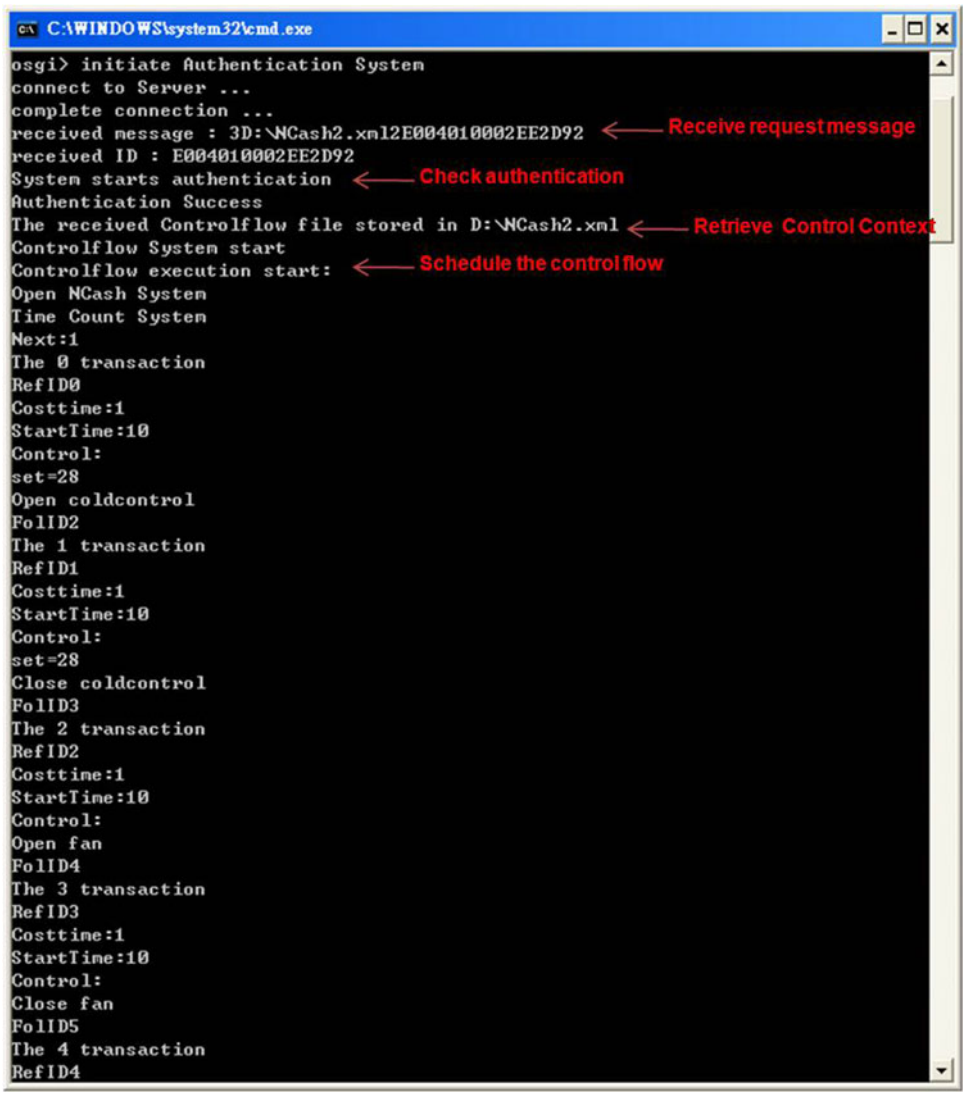

Fig. 12 Parsing control flow for controlling home appliances

a residential building. In the authentication scenario, the NFC reader first sends a request for an authentication tag to the NFC phone. On receiving the request, the phone encapsulates all the keys it has into a tag, which it sends to the reader for authentication. The purpose of this operation is to improve performance. There is no problem in encapsulating single key into a tag. It is clear that the latency increases with any increase in the number of keys in the phone. In the example, the length of the request sent by the reader is 43 bytes and the authentication key is 57 bytes. Figure 15 shows the latency of the authentication process. Here, we measure only the time consumed by the US-NFC on the NFC reader-side, since the latency is approximately equal to the latency of the NFC phone in our test-bed.

Figure 15a refers to the case of 1 key in the tag repository of the NFC reader, Fig. 15b to the case of 5 keys, and Fig. 15c to the case of 10 keys. In each case here, similar to key setting, the time for receiving and parsing the tag constitutes the main part of the latency. In addition, these cases make it clear that the more keys that are encapsulated in the tag, the more time is consumed during the steps of receiving and parsing. The reason is that not only do multiple encapsulations of keys increase the size of the tag, but also the Record Parser module needs more time for parsing the extra keys. Figure 15a gives a total time of less than 0.25 ms, Fig. 15b less than 0.4 ms and Fig. 15c less than 0.41 ms. This is reasonable because the more keys the NFC has, the more time is needed to check authentication.

There are two cases needing further explanation. The first concerns the possible scenario of a single key encapsulated in a tag in a reply message failing in the authentication process, thus triggering the reader to send an alert to the phone requesting another key. If this happens, total time for authentication will be a multiple of that for case Fig. 15a, and total latency will exceed that for case

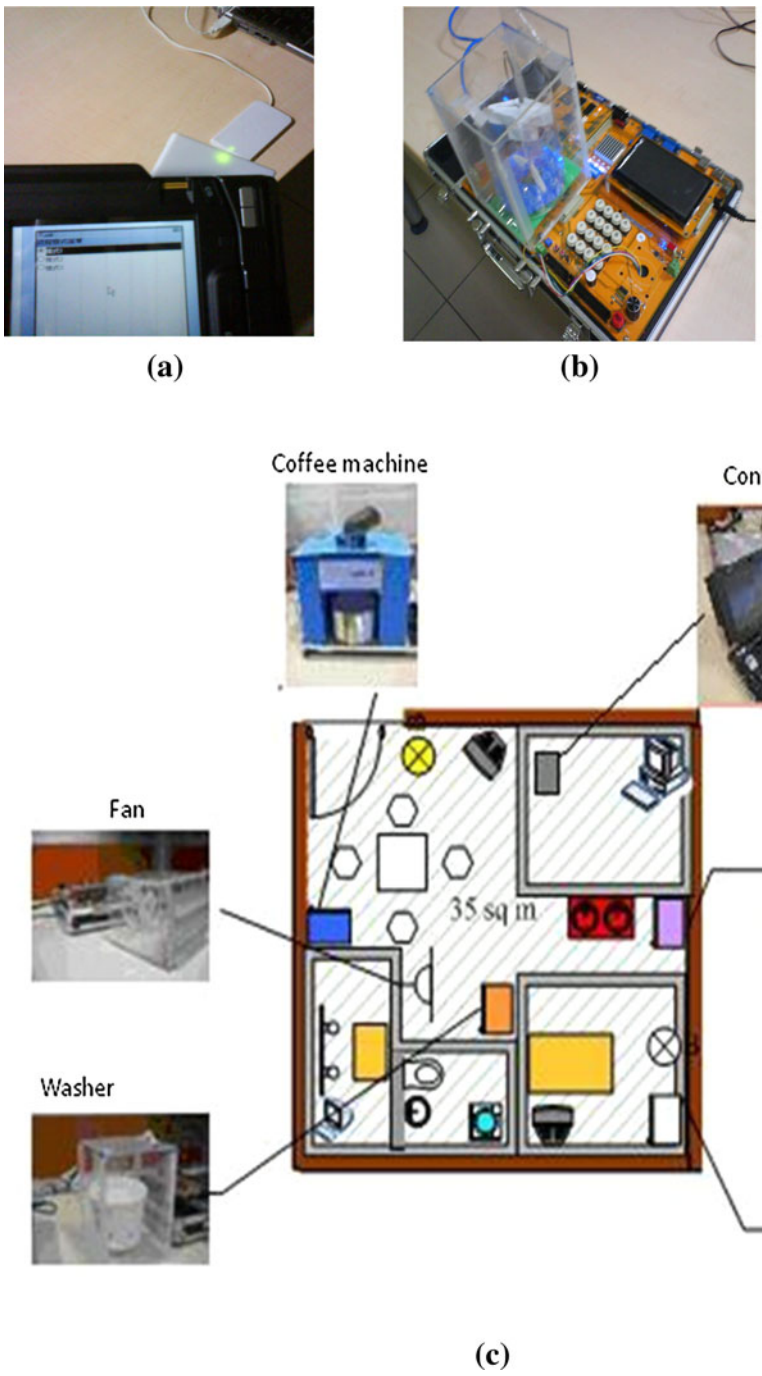

Fig. 13 A prototype using DMA-2400XP embedded system. **a** Emulated NFC phone contact NFC reader. **b** An emulated home appliance. **c** Home appliances deployment

Fig. 15b. In response to that scenario, it appears that a scheme in which multiple keys are encapsulated in a tag is superior to one of one-key-only-in-a-tag. It is in fact usual for users to hold multiple keys. The second scenario concerns the acceptable total time for parsing multiple keys (e.g., 10) from a tag. We can deduce from Fig. 15c that if a user holds up to 100 keys in the NFC phone, the total time for parsing and extracting keys from the replied tag is also acceptable based on the US-NFC framework.

In addition to measuring the latency of authentication checking in the NFC reader, we also measure the latency of controlling home appliances. We do two experiments to measure the response time for evaluating system performance, as shown in Fig. 16. The first involves measuring the response time between a Controller Bundle (CB) and home appliances, and the second the response time between a Control Point Bundle (CPB) deployed in the home and home appliances.

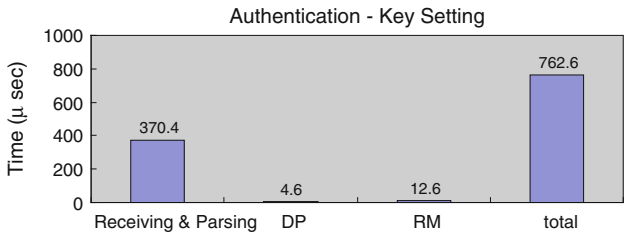

Fig. 14 The performance of key setting

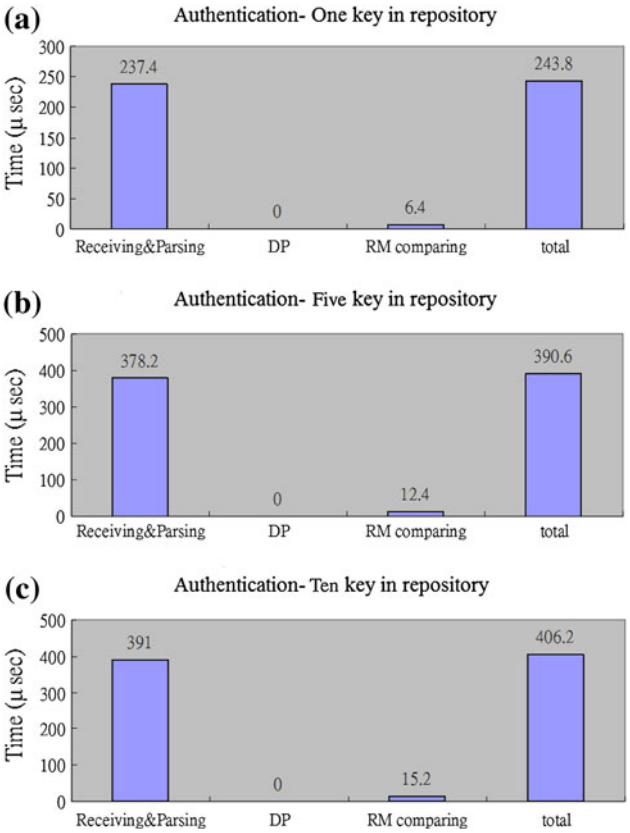

Fig. 15 The performance of authentication if a NFC phone has 1, 5 or 10 keys in its database. **a** 1 key. **b** 5 Keys. **c** 10 Keys

Figure 16a shows the response time for home appliances measured at CB, the average being about 1 ms. The response time mainly comprises the time for execution of the embedded system and network latency. We believe that response time will increase as the size of the XML-based rules increases. Figure 16b shows the response time of home appliance measured at CPB, the average being less than 1 ms. It is reasonable because most of the overhead comprises the execution time of the embedded system and network latency. Similarly, we can deduce from Fig. 16c the circumstances for a home that ties 20 or fewer appliances in the framework, the latency to schedule the control context is also acceptable.

From the above evaluation and definition of total latency, we can summarize that the system is efficient, even

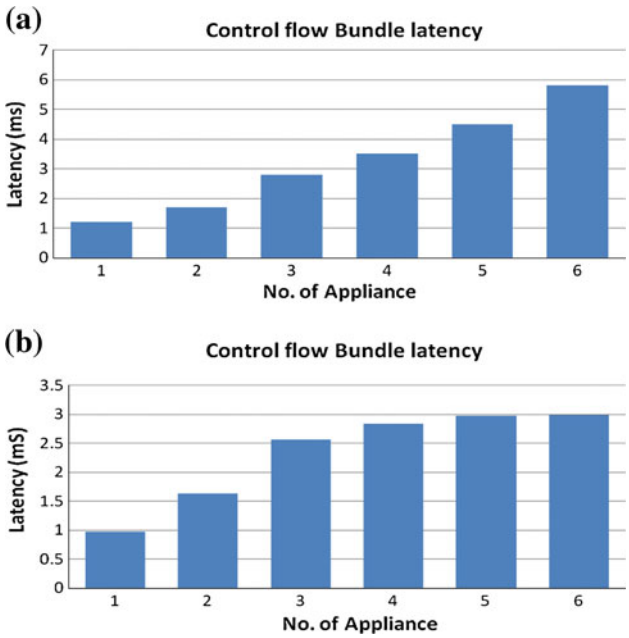

Fig. 16 The latency measurement. **a** Response time of home gateway. **b** Response time of control point

if the user has many *Keys* and many appliances are deployed in the community and in the home. Total latency will not affect system operations.

6.2 Discussion

This section will discuss some issues related to the pros and cons of the proposed approach. These are security, preference confliction, and other advantages.

6.2.1 Security issue

Cryptography support is important not for identity authentication, but also for making home automation secure, such as in [17], employed in a single well-developed reliable transport protocol. Fortunately, in recent years, many excellent cryptography algorithms for RFID to enhance security have been proposed [16, 30, 31] and we see no need to attempt in this paper to add any new ones. In our approach, we develop the framework in a modularized scheme. Any cryptography algorithm can be easily embedded into an authentication bundle of the Authentication Module (AM) easily or replaced directly. In addition, cryptography algorithms in CE and HE can be different, so that security can be greatly improved. Therefore, in the proposed approach, our scheme enhances and guarantees both security and privacy.

6.2.2 Preference conflict

All approaches that support user preference raise preference conflict [32]. In the last decade, much research

concerning conflict resolution has gone into proposals for the smart homes and the intelligent office [33]. We do not discuss the security issue here, nor do we propose any new conflict resolving algorithm. In the modularized architecture, any excellent conflict resolving algorithm can be easily embedded into the controller bundle of the Control Processing Module (CPM) or replaced directly.

6.2.3 Advantages

Further relevant points when comparing the advantages of our proposed system with the two featured in Sect. 1.1, that is, the so-called Mobile-controlled Home Automation,[16,17] (MC) and Web Services-based Home Automation (WS) [14, 15]:

- *Energy Saving and Carbon Reduction* With our system, appliances can be activated only when the user arrives home, while with MC and WS activation must be executed some time before that point. Obviously, our system may score higher for energy saving and carbon reduction, but could be considered inconvenient for an appliance that the user may wish to activate before arriving home, e.g., a rice cooker.
- *Diversity* Our system provides for automation not only in the home space, but also in the communal space. The user preference can cover any communal appliance that is authorized to the user and, in addition, multiple preferences can be stored in the NFC phone. Users can easily initiate and control appliances employing user preferences separated out by place and time. In addition, as may be observed from Fig. 7, this automation system can be flexibly deployed in a large-scale residential community as well as in quite different circumstances [34], for instance, in a manufacturing environment.
- *Connection Cost* The MC approach incurs extra connection costs when mobile phones are used to connect to a home gateway, whereas both WS and our proposed approach do not. However, MC can control appliances anytime and anywhere.
- *Convenience* Adopting the proposed approach, a range of appliances can be activated by a series of minor operations that cover authorization, authentication and checking, affording control by a one-touch NFC phone and NFC reader with no need for operations and interactions with other systems. It is thus far easier than MC and WS.

[16] http://www.mobilecomms-technology.com/projects/foma/.

[17] http://blog.neonascent.net/archives/mobile-controlled-home-automation/.

7 Conclusion and future work

In this paper, we proposed a novel application for a NFC phone, namely, a NFC-driven digital home environment. The application allowed the user of a NFC phone to control home appliances in a smart home space, with the control driven by requests sent by the phone in the shape of predefined user preference. The phone acted not only as the key for accessing the space, but also delivered a personalized control context that regulated numbers of appliances in the space. First, a previously proposed Universal Service framework for the phone (US-NFC), designed as a negotiation mechanism between NFC devices, was used to construct a flexible NFC-driven Home Automation Environment (HAE) architecture that was suitable for inferring user preference for appliances both in communal and domestic spaces. In addition, a simple authoring tool for creating user preference for all appliances was presented, as well as a prototype to demonstrate the feasibility of the architecture and evaluate the performance and efficiency of the system. Finally, we discussed the usability and effectiveness of the proposed approach.

Looking to the future, we shall make it our task to apply a conflict resolving algorithm to the CPM and integrate the architecture with ontology technology and rule-based reasoning with the aim of constructing personalized context-aware smart spaces. The appliances can be controlled and driven by requests sent from a NFC phone with no need to consider the context of the environment.

Acknowledgments We are grateful for the many excellent comments and suggestions made by the anonymous referees. This work was supported by the Nation Science Council of Republic of China under Grant No. 100-2221-E-305-013-.

References

1. Sangani K (2006) Home automation—it's no place like home. IEEE Eng Technol 1(9):46–48
2. Han J, Lee H, Park K-R (2009) Remote-controllable and energy-saving room architecture based on ZigBee communication. IEEE Trans Consumer Electron 55(1):264–268
3. Nikolova M, Meijs F, Voorwinden P (2003) Remote mobile control of home appliances. IEEE Trans Consumer Electron 49(1):123–127
4. Park W-K, Han I, Park K-R (2007) ZigBee based dynamic control scheme for multiple legacy IR controllable digital consumer devices. IEEE Trans Consumer Electron 53(1):172–177
5. Gu T, Pung H-K, Zhang D-Q (2005) A service-oriented middleware for building context-aware services. J Netw Comput Appl 28(1):1–18
6. Intille S–S, Larson K, Tapia E-M, Beaudin J-S, Kaushik P, Nawyn J, Rockinson R (2006) Using a live-in laboratory for ubiquitous computing research. Lect Notes Comput Sci 3968:349–365
7. Kidd C-D, Orr R, Abowd G-D, Atkeson C-G, Essa I-A, MacIntyre B, Mynatt E, Starner T-E, Newstetter W (1999) The aware

home: a living laboratory for ubiquitous computing research. Lect Notes Comput Sci 1670:191–198
8. Malan D, FulfordJones T, Welsh M, Moulton S (2004) Codeblue: an ad hoc sensor network infrastructure for emergency medical care. In: Proceeding of int'l. workshop on wearable and implantable body sensor networks, 2004
9. Wood A-D, Stankovic J-A, Virone G, Selavo L, He Z, Cao Q, Doan T, Wu Y, Fang L, Stoleru R (2008) Context-aware wireless sensor networks for assisted living and residential monitoring. IEEE Netw 22(4):26–33
10. Wu J, Huang L, Wang D, Shen F (2008) R-OSGi-based architecture of distributed smart home system. IEEE Trans Consumer Electron 54(3):1166–1172
11. Wu C-L, Liao C-F, Fu L-C (2007) Service-oriented smart home architecture based on OSGi and mobile-agent technology. IEEE Trans Syst Man Cybern Part C Appl Rev 37(2):193–205
12. Kim Y, Lee D (2006) A personal context-aware universal remote controller for a smart home environment. In: Proceeding of the 8th international conference on advanced communication technology 3:1521–1525
13. Park K-L, Yoon U-H, Kim S-D (2009) Personalized service discovery in ubiquitous computing environments. IEEE Pervasive Comput 8(1):58–65
14. Kirchhof M, Linz S (2005) Component-based development of Web-enabled eHome services. Pers Ubiquit Comput 9(5):323–332
15. Perumal T, Ramli A-R, Leong C-Y (2008) Design and implementation of SOAP-based residential management for smart home systems. IEEE Trans Consumer Electron 54(2):453–459
16. Juels A (2006) RFID security and privacy: a research survey. IEEE J Sel Areas Commun 24(2):381–394
17. Bergstrom P, Driscoll K, Kimball J (2001) Making home automation communications secure. Computer 34(10):50–56
18. Michahelles F, Thiesse F, Schmidt A, Williams J-R (2007) Pervasive RFID and near field communication technology. IEEE Pervasive Comput 6(3):94–96
19. Beny'o B, Vilmos A, Kovacs K, Kutor L (2007) NFC applications and business model of the ecosystem. In: 16th IST mobile and wireless communications summit 2007, pp 1–5
20. Bravo J, Hervas R, Chavira G, Nava S (2007) Adapting technologies to model contexts: two approaches through RFID & NFC. In: Proceeding of 2nd international conference on digital information management, vol 2, pp 683–688
21. Csapodi M, Nagy A (2007) New applications for NFC devices. In: 16th IST, mobile and wireless communications summit, pp. 1–5
22. Antoniou Z, Varadan S (2007) Intuitive mobile user interaction in smart spaces via NFC-enhanced devices. In: Proceeding of third international conference on wireless and mobile communications, 4–9 Mar
23. NFC Forum (2008) Generic control record type definition, NFCForum-TS-GenericControlRTD_1.0, 2008.3.7
24. Sheng Q, Li X, Zeadally S (2008) Enabling next-generation RFID applications: solutions and challenges. IEEE Comput 41(9):21–28
25. Falke O, Rukzio E, Dietz U, Holleis P, Schmidt A (2007) Mobile services for near field communication. Technical report, University of Munich; Mar 2007. LMU-MI-2007-1
26. Siemens AG Corporate Technology (2005) Intelligent autonomous system (CT IC 6), BenQ mobile phones—technology and innovation (MD PBM TI). NFC Service Platform User Guide. Version 1.2.2, 06.10.2005
27. Nokia (2005) Nokia NFC & RFID SDK 1.0 Programmer's Guide NFC. V 1.0, http://europe.nokia.com/nokia/0,,76301,00.html
28. Nichols J, Myers B-A (2006) Controlling home and office appliances with smart phones. IEEE Pervasive Comput 5(3):60–67
29. Schimanke C, Maugars P (2005) Cellular system solutions for NFC-enabled handsets. Business line cellular systems philips semiconductors. http://www.eetasia.com/ARTICLES/2005FEB/B/2005FEB01_RFD_DSP_PD_TA.pdf
30. Chien H-Y, Chen C-H (2007) Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards. Comput Stand Interf 29(2):254–259
31. Choi E-Y, Lee D-H, Lim J-I (2009) Anti-cloning protocol suitable to EPCglobal Class-1 Generation-2 RFID systems. Comput Stand Interf 31(6):1124–1130
32. White C–C, Sykes E-A (1986) A user preference guided approach to conflict resolution in rule-based expert systems. IEEE Trans Syst Man Cybern 16(2):276–278
33. Thyagaraju G-S, Math M-M, Kulkarni U-P, Yardi A-R (2009) Conflict resolving algorithms to resolve conflict in multi-user context-aware environments. In: IEEE international advance computing conference, pp 202–208
34. Chang Y-S, Fan C-T, Wu Y-S (2011) Agent-based Intelligent software exploits near-field communication. IEEE IT Prof 13(2):30–36
35. Pan G, Wu J, Zhang D, Wu Z, Yang Y, Li S (2010) GeeAir: a universal multimodal remote control device for home appliances. Pers Ubiquit Comput 14(8):723–735
36. Conejero J-M, Clemente P-J, Rodríguez-Echeverría R, Hernández J, Sánchez-Figueroa F (2011) A model-driven approach for reusing tests in smart home systems. Pers Ubiquit Comput 15(4):317–327