Information Fusion 21 (2015) 57–67

Contents lists available at SciVerse ScienceDirect

Information Fusion

journal homepage: www.elsevier.com/locate/inffus

An intelligent context-aware communication system for one single autonomic region to realize smart living

Ya-Fen Chang [a], Chia-Chen Chen [b,*], Shao-Cian Lin [a]

[a] Department of Computer Science and Information Engineering, National Taichung University of Science and Technology, Taichung 404, Taiwan
[b] Department of Management Information Systems, National Chung Hsing University, Taichung, Taiwan

ARTICLE INFO

Article history:
Available online 2 April 2013

Keywords:
Smart living
GSM
GPS
ARM (Advanced RISC Machine)
Embedded system

ABSTRACT

Wireless communication plays an important role in smart living applications. People can use mobile devices to access various kinds of services via various wireless technologies such as Zigbee, RFID (Radio Frequency Identity). Conventional smart living applications tend to be designed for convenience while ignoring essential restrictions. Actually, ubiquitous communication is the privilege of authorized users in some places for specific requirements and reasons. For example, a nursing attendant may be issued a handset to communicate with a patient's family in the hospital while unauthorized communication is not allowed to prevent the handset from being misused by the nursing attendant. Principles for essential restrictions should be determined and put into practice by an administrator within a predefined region, which is defined to be single autonomic region. In this paper, an intelligent context-aware communication system is proposed to provide ubiquitous communication under location and communication party restrictions to realize smart living in one single autonomic region. We design the system by integrating heterogeneous communication technologies and one novel security protocol, double-lock protocol. We implement the designed system with an ARM-based processor on the embedded system experimental board DMA-2440XP and two pluggable modules, GSM (Global System for Mobile Communications) and GPS (Global Positioning System). In the designed communication system, only legal users can use a legitimate communication device to communicate with legal ones within the authorized area.

1. Introduction

Wireless communication plays an important role nowadays. Pager [1], WLAN (Wireless Local Area Network) [2], WMAN (Wireless Metropolitan Area Network) [3], Bluetooth [4], Wireless Sensor Network, Zigbee [5], RFID [6–8], 1G (First Generation), 2G (Second Generation), 3G (Third Generation), GPRS (General Packet Radio Service) and 3.5G [1,9,10] are a part of wireless communication. Wireless communication is regarded as the landmark of communication technologies because it provides convenience greater than wired communication. Wired communication technologies make users access a server remotely but constrained to stay at locations of computers while wireless ones enable users to get services anytime and anywhere. via wireless communication, a variety of smart living applications are proposed to provide convenience. Most of them are designed for publics and seldom take specific essential restrictions into consideration. Among these smart living applications, ubiquitous communication is always regarded as a basic function. In fact, ubiquitous communication is the privilege of authorized users in some places for specific requirements and reasons such as security and location restriction. In the following, some scenarios are given.

As we know, health care is one major domain of smart living. A nursing attendant is very important in health care to ensure a patient obeys doctor's instructions especially for disabled people. For convenience, a nursing attendant may be issued a handset by a patient's family to communicate with them when he takes care of the patient in the hospital only. That is, unauthorized calls made by the attendant are not allowed by the patient's family. On the other hand, personal communication equipment may bring security threats. Modern communication equipment not only possesses communication ability but also provides advanced multimedia functions such as cameras and video phones. These functions easily result in confidential information leakage. Conventional information protection approaches such as access control and permission management cannot ensure the security of confidential information. It is because modern communication equipment can easily store or photograph the confidential information such as a blueprint and secrets processed by many people in many places. For example, such modern equipment is not allowed in some specific places, military control area, examination preparation area, proprietary investigation site, secret-protecting buildings, and so on.

[*] Corresponding author.
E-mail addresses: cyf@cs.ccu.edu.tw (Y.-F. Chang), emily@nchu.edu.tw (C.-C. Chen), ksd19880803@hotmail.com (S.-C. Lin).

1566-2535/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.inffus.2013.03.002

The simplest but negative way to protect confidential information is prohibiting users from carrying personal communication or storage equipment into the place where the confidential information is. It is hard to find someone in a wide field when no personal communication equipment is available so authorized mobile devices are required.

How to find a solution to achieve these special requirements while providing convenience is an urgent issue. An intuitive approach is inventing a new communication protocol and equipment, but it takes much money and time. Thus, we tend to design a context-aware communication system with an existing and working mobile communication system chosen from 1G, 2G and 3G because a mobile communication system releases the burden of constructing and maintaining the base stations. After taking properties of these three mobile communication systems into consideration, GSM is chosen because digitalized communication is required while no high speed data transfer is needed. The other reason to choose GSM as the base communication system is because the calling rate of 2G is lower than 3G. Meanwhile, the user location needs to be known because a user only can communicate with other legal users within an authorized region. So GPS [1] is employed to provide location information to check if a user is within the authorized region or not. Unlike conventional context-aware applications, RFID is not used to get location information because the construction fee of this approach is more expensive than that of adopting GPS directly. The advantages and disadvantages of implementing the designed system with difference communication technologies are listed in Table 1. After choosing GSM and GPS to design a secret-protecting mobile communication system, we further design one security protocol, double-lock protocol, to ensure that a SIM (Subscriber Identity Module) card is protected from being misused even if it is stolen.

To ensure that only legal users can use a legitimate communication device to communicate with legal ones within the authorized region, a secure secret-protecting communication system must not be vulnerable to the following scenarios, which the original security protocols for GSM [11–17] and previous GSM/3GPP-related ones [18–21] may not resist.

Illegal user access: An unauthorized/illegal user tries to access the GSM communication service. The illegal user enters PIN (Personal Identification Number) for authentication to activate the communication module of the designed system.

Illegal SIM card: A user inserts an illegal SIM card into the designed system and tries to be authenticated successfully.

Table 1
Advantages and disadvantages of implementing the designed system with difference communication technologies.

Technology	Advantages	Disadvantages
Communication systems		
1G	No need to construct and maintain the communication system	Security concerns because signals in 1G systems are analog
2G	No need to construct and maintain the communication system a low calling rate	No high speed data transfer
3G	No need to construct and maintain the communication system	A high calling rate
Positioning systems		
GPS	No need to construct and maintain the positioning system	Possible incorrect position information in an indoor environment
RFID	Precise position information in an indoor environment	High cost to construct the positioning system needing RFID devices attached for receiving or transmitting RFID signals

Illegal mobile equipment: A user takes an authorized SIM card of the designed system and inserts it into an illegal mobile device. Thereupon, the user enters PIN to activate the communication module.

Illegal location: A user possesses a legal SIM card and communication equipment and enters correct PIN. Then, a user tries to make a phone call or pick up a phone call out of the authorized region.

Illegal communication party: Within an authorized region, a legal user possesses a legal SIM card and communication equipment and enters correct PIN, but he tries to communicate with an illegal or unauthorized communication party.

In this paper, we design an intelligent context-aware communication system based on GSM and GPS to provide efficient user authentication and defend against the security threats mentioned above. In the designed system, a user enters PIN which is composed six decimal digits. There exist six PIN transformation tables, each of them is composed of 256 entries, and each entry is a decimal digit in $[0,9]$ randomly. A symmetric encryption operation is executed to transform each digit of PIN to an index of a corresponding PIN transformation table to find the transformed decimal digit. Then, the entered PIN is used to be the seed of a sequence generation function to find two indices. Two digits of these two indices in the six transformed decimal digits are deleted to get the real personal identification number PIN' to activate the communication module. We implement the designed communication system with an ARM-based processor on the experimental board DMA-2440XP and two pluggable modules, GSM and GPS modules. via the implementation, the designed communication system is proved to be realized and utilized. Moreover, the designed mobile communication system can be implemented with other base mobile communication system or position system because the designed mobile communication system only uses the functions they provide without modifying them.

The rest of this paper is organized as follows. Definition of single autonomic region and properties of smart living applications needing the designed context-aware communication system are given in Section 2. Preliminaries are reviewed in Section 3. The proposed system is shown in Section 4 followed by the corresponding security analysis in Section 5. The implementation, with an ARM-based processor on the experimental board DMA-2440XP and two pluggable modules, and the corresponding discussions are given in Section 6. Finally, some conclusions are drawn in Section 7.

2. Definition of single autonomic region and suitable smart living applications

As mentioned above, conventional smart living applications do not consider specific requirements. In the following, the term, single autonomic region, is first defined formally.

Single autonomic region: Within a predefined region, an administrator can determine principles and put them into practice thoroughly. The size of one single autonomic region is not constrained. It can be as small as a device or as large as a nation. If a device is one single autonomic region, the user who can define usage principles of the device is regarded as the administrator.

After giving the definition of single autonomic region, properties of smart living applications needing the designed context-aware communication system are given as follows.

Single autonomic region based: The smart living application must obey instructions or principles determined by the administrator.

Location restriction: When a user accesses the application, he must be located in an authorized area.

Communication restriction: When a user accesses the application, the other communication party must be authorized.