A Reliable and Economical Access Point Solution for Secure Home Network

Neelakanta E
Research Scholar
Dept. of Computer Science
Dayananda Sagar College of Engineering
Bangalore, India

Dr. Krishnan R
Professor
Dept. of Computer Science
Dayananda Sagar College of Engineering
Bangalore, India

ABSTRACT

Personalized Home Networks use information technology to monitor the environment, control the home Appliance and communicates with the other devices. Personalized home networks are a complex technology, at the same time it is developing. A sample home environment monitors and control system that is one branch of the personalized home networks is addressed in this paper. Home Appliances connects to home networks by using Wi-Fi, Bluetooth or related standards but WLANs (Wi-Fi) provide true mobility and flexibility to users. It has changed the way people communicate and share information by eliminating worrisome factors of distance and location. In this work we have implemented the security panel for controlling the all home appliances based on WLAN networks. So that the home appliances (Personal Computers, Laptops, Cameras, PDAs, Cell phones, etc) are communicating with other devices through security system by using radio signal. The Security system also provides the access point functionalities. This core concept can support many applications for example monitoring and controlling wireless cameras for security purpose. The continuous streams of wireless camera images are viewed and monitored by the laptops and cell phones. The personalized Home network access point providing wireless services such that more secure and cost effective manner.

Keywords

Bluetooth, Home Appliances, Personalized home networks, security panel, WLAN (Wi-Fi).

1. INTRODUCTION

The Advancements in software and Networking technology provide great conveniences to daily human life. Usage of new generation technologies are became an important requirement in these days. Therefore, personalized home networks are used as an indispensable part of daily life. With the advancement of technology, today's modern home owners are expecting and demanding easy-to-use solutions to the problems of managing their home environment efficiently.   Personalized Home Networks is a developing system which can provide intelligent management but need most cost.

In order to implement affordable user friendly technology, it is necessary for the Wireless medium to communicate the diverse data and the development of security system to provide centralized coordinator functionality as well as access point functionality.

The prototype system described in this paper uses a WLAN (Wi-Fi) network [1] for the wireless mediu006D. The security system of the personalized home networks is designed to control and Monitor various types of devices. The Home appliances communicate with other through the security system. Although the Bluetooth technology[2] used for the home network has some limitations in a low bandwidth, low range and scalability and infrared technology requires line-of- sight with devices, So that these technologies replaced with a Wi-Fi technology for higher range and scalability.

In this paper, we have implemented the security system for home networks that can control and monitor the all home appliance and also provide the access point functionalities. The security panel should act as centralized coordinator, therefore no separate dedicated access point hardware required for each home network. In order to works as central coordinator, the security panel should support Wi-Fi access point functionalities for efficient communication between pair of home devices.

The rest of the paper is organized as follows. Section 2 provides the description of problem statement and existing system technologies. Section 3 describes the related work regarding Home Network. Section 4 provides description of System Architecture and Design description. Section 5 discusses the Experimental set up and result Analysis. Finally, Section 6 concludes the paper.

2. PROBLEM OVERVIEW

The Personalized Home Network must be readily scalable for future upgrades to incorporate emerging technologies with minimal hardware modifications. Generally In home environment each device require separate controller for controlling and monitoring devices (example door controller, ventilation controller, light controller, etc). The Advancement in Technology home appliances can communicate and control each other. The Access Point Hardware is most essential device to establish the Wireless network in Home environment. The dedicated access point is not affordable to establish normal home users. To overcome the limitations of existing home network, the security system of the personalized home network should provide the bridging functionality between home appliances. So that all devices capable to communicate with each other. In order to provide this functionality, the security system should behave as access point for efficient and secure communication.

3. RELATED WORK

The personalized home networks evolve with advancement of technology to make human life comfortable and easier. In 1979, the Stanford Research Institute presented to integrate household appliances and electrical equipment into family control bus [3]. In 1984, United Technologies Corporation built the first intelligent building, City Place Building. In 1988, American Electronics Industry Association prepared the home bus system standards (HBS). In October 2004, Digital Home Working Group (DHWG) completed design specifications Version1.0 [4] which realized the communication for music, images, video and other digital content. Honeywell announced single-family use of smart home system - "Smart Honeywell single-family home" (HRIS- 1000 series) in October 2009[5]. The Access point is essential building block in WLAN infrastructure and its taken care of channel allocation and Reallocation [6]. The Wireless video streaming systems are streams video to the heterogeneous clients with in the home networks; over time varying communication links [7]. In this paper we connect the home appliances with help of WLAN networks. The security system acts as centralized device control and monitors the all home appliances. The security panel also provides the access point functionality for efficient communication between the home appliances in the WLAN environment

4. SYSTEM ARCHITECTURE

In this work we are integrating Home networks with the Wi-Fi technology, so that the home appliances communicate with each other by radio signals.

## 4.1 Framework for personalized Home Network Security system Architecture

The heterogeneous home appliances connect each other with the help of centralized Home security panel as shown in Fig 1.The security system is control and monitors the all home appliances based on WLAN networks. So that the home appliances (Personal Computers, Laptops, Cameras, PDAs, Cell phones, etc) are communicating with other devices through security system by using 2.4GHz unlicensed radio spectrum. The Security system should provide the access point functionalities in WLAN environment.

Fig 1: Global structure of personalized home network with security system.

4.2 Internal Architecture of Personalized Home security system

In order to provide the access point functionalities the Home network security system mainly consists of Wi-Fi chip, processor and built-in antenna. The Structural view of security panel as shown Fig 2
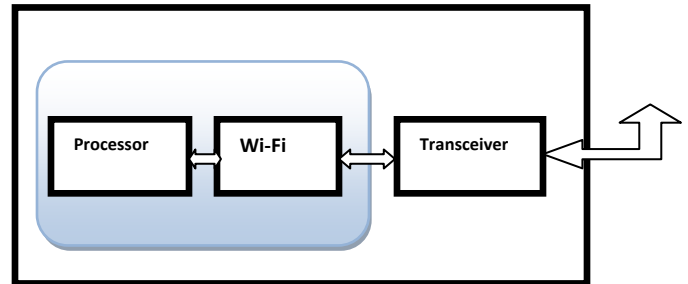
Fig 2: Internal Architecture of Security panel

The security system with built-in transceiver receives the radio signal and sends to the Wi-Fi card. Once the Wi-Fi card receives the signal, it raises the interrupt to processor by interrupt service routine. The processor processing the requested interrupt and response to the either network interrupt or hardware interrupt.

4.3 System Modeling

The Personalized home networks security system (Access point) mainly consists of 3 modules.

- ➢ Applications module
  - ▪ Event Generation/Reception.
  - ▪ Command Handling.
  - ▪ Application Utilities.
- ➢ Device Driver module.
- ➢ SDIO interface module.

The Communication between home appliances through Home security system described in the following steps.

Step 1: The home security system initializes the software/hardware and establishes the new network.

Step 2: The security system waiting for the interrupt from home devices.

Step 3: The all home appliances register with home security system and the security system continuously sending the Beacon information in fixed intervals to check the status of the devices.

Step 4: The security system associates and authenticates devices which wants communicates with other devices then assigns the unused channel.

Step 5: The devices establishes the connection through the security system and access the other devices.

Step 6: Once the communication is completed between the devices, the security system closes the connection and de allocate channel.
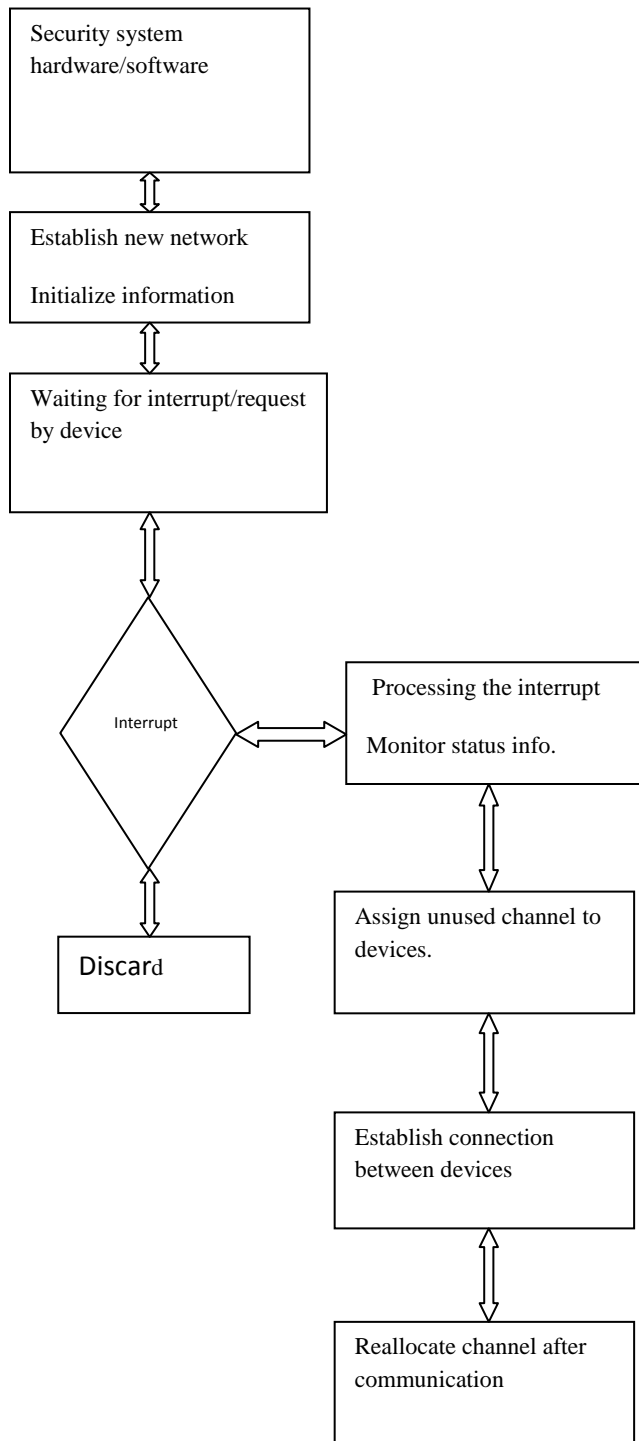
devices which wants communicates with other devices then assigns the unused channel

4.4 The Dataflow within system

The Wi-Fi card receives the signal from transceiver and send to the device driver (running in kernel space) through SDIO interface by using interrupt service routine. The Device drivers send/receive the data to/from applications which is running in the user space. The pictorial representation is shown in Fig 4.
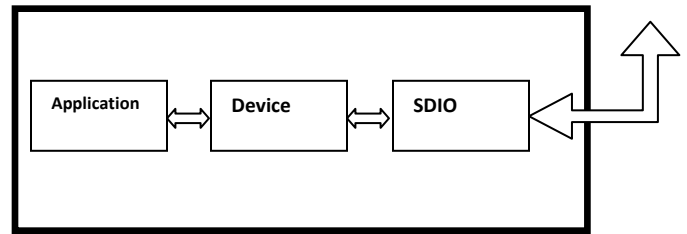
Fig 4: Data flow path within the system

5. EXPERIMENTAL SET UP AND RESULTS

In Personalized Home Networks the home appliances like Personal Computers, Laptops, Cameras, PDAs, And Cell phones Etc are equipped with the Wi-Fi cards for efficient communication. The security system acts as the central coordinator for all home appliances and running Linux operating system kernel 2.6.26 and equipped with the touch screen display. The security system provides all access point functionalities for accessing and controlling devices one another. This Personalized home network security panel range for indoor environment 70-100ft.

All the home appliances communicate with other devices through the home security system. Each device in the home can access and control the other devices through security system which is capable to provide access point functionalities.

The different scenarios of communicating home appliances with in home networks with the help of Security system are described in the following .

Scenario 1: The Cell phones, laptops and wireless cameras are registers with the security system. The security system checks the associations and authentication of each device then assigns dynamic addresses for devices. The Home appliances Ethernet address, name and other information displayed in security system touch screen fig 5

Scenario 2: The door, ventilation, lights are controlled by the mobile devices like PDAs, cell phones. The Wireless cameras accessed and controlled by laptops are shown in fig 6:
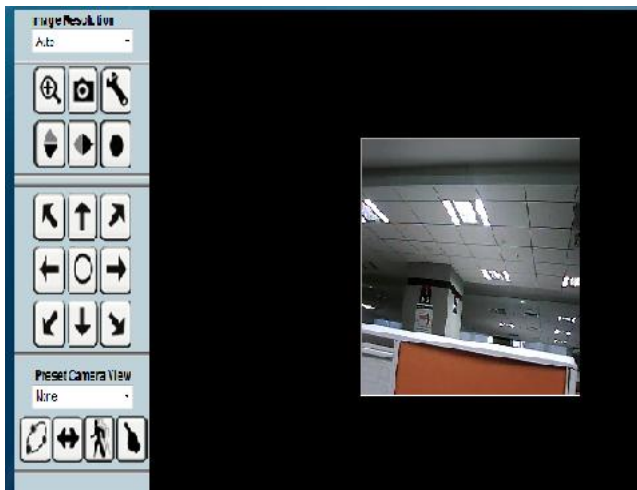
Scenario 3: Efficient file and resource (Ex. memory) sharing between the personal computer and laptops and mobile phones.

Fig 3: Flow chart of Home security panel

The personalized home security system initializes the software and hardware and establishes the network. The home appliances are request to security panel for communicates with other devices. Then the security panel associates and authenticates the

Fig 5: Home appliances Ethernet address, name information

Fig 6: Camera accessed and controlled by laptops.

6. CONCLUSION AND FUTURE WORK

Most traditional home control networks use wire technology and this kind of scheme has shortcomings of poor expansibility, complicated wiring and high cost. The Home security panel provides full-scale home monitors and control function with access point functionalities for efficient communication in personalized home networks. The personalized home security panel integrating with Wi-Fi networks acts as central control unit for controlling the home appliances. All the home appliances can access each other in secure and efficient manner.

As a future direction of this work, the home security panel should support load balancing functionality to overcome extensive traffic conditions and also support fault tolerance functionality by continuous updating with reliable home appliances.

7. REFERENCES

[1] IEEE 802.11 Working Group: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. The Institute of Electrical and Electronics Engineers, Inc., 1999.

[2] Design and Implementation of a Bluetooth based General Purpose Controlling Module Authors: Wijetunge S.P, Samarasinghe

[3] Chengyan Jiang, Siyuan Wu, Wei Chen, Smart Home System Based on Wireless Sensor Networks, Control &Automation, Vol 23, pp.199-201, May 2007.

[4] Xiaomei Zhang, Jun Lu, Bingqin Peng et c., Design and Realization of Embedded Intelligent Home Supervis ion System, Control &Automation, Vol 23, pp.55-56, Jan. 2007.

[5] Peter Bergstrom, Kevin Driscoll, John Kimball, Honeywell Laboratory, "Making Home Automation Communications Secure" October, 2009.

[6] Path Loss Models for 802.11a Wireless local area networks. Authors: Fabiana Capulli, Cristiano Monti, Franco Mazzenga.

[7] Secure and Scalable Video Streaming over IEEE 802.11e based Home Networks. Authors: Azfar Moid, Abraham O.Fapojuwo, Robert J.Davies.

[8] Nortel and NorWeb Launch Improved Technology to Provide Data Service and Internet over Electricity Lines

[9] Home automation to promote independent living in elderly populations, Authors: A. M. Cole and B.Q. Tran Homecare &Telerehabilitation Technology Center, Department of Biomedical Engineering the Catholic University of America, Washington, DC

[10] High-speed Home Networking Over AC Power Lines Enikia Inc-Power Line White paper