Transparent Heterogeneous Networks for Remote Control of Home Environments

Khusvinder. Gill, Student Member, IEEE, Fang. Yao, and Shuang-Hua. Yang, Senior *Member, IEEE*

Abstract— **Home environment has seen a rapid introduction of network technologies. The types of home networks introduced, include home automation, multimedia entertainment, and security networks. These networks are often developed by different organisations and consist of varying network technologies. Consequently, little attention has been given to the coexistence and interoperability of these networks. This naturally developing heterogeneous network architecture introduces new and significant usability and safety concerns. This paper addresses these concerns, through the design and implementation of a home gateway. A case study is implemented showing the application of the home gateway, to facilitate interoperability, between a home automation and a video surveillance network.**

I. INTRODUCTION

IN recent years the home environment has seen a rapid introduction of network enabled, digital technology. This technology offers new and exciting opportunities, to increase the connectivity of devices within the home. Home automation is the general term used to represent this relatively new breed of technology. The adoption of network enabled products into the home has proceeded in an unplanned and ad-hoc manner. This pattern of adoption has lead to a home environment, consisting of a complex maze of heterogeneous networks. The application domains of home automation differs significantly, including home security, energy conservation and multimedia entertainment networks.

Home automation has been described by [1] as the introduction of technology within the home to enhance the quality of life of its occupants. There have been many proposed home automation systems. [2] developed a Java based home automation system, which used an embedded board to connect all the home automation devices together. However, the system requires an intrusive and expensive wired installation and the use of a high end pc. [3] introduces a Bluetooth based home automation system, consisting of a primary controller and a number of Bluetooth sub-controllers. It would be desirable for each device to have its own Bluetooth module. However due to its fiscal expense, a single module is shared amongst several devices. [4] introduces a phone based remote controller for home and office automation. The system differs in that all communications occur over a fixed telephone line and not the Internet. The disadvantages of this system are threefold: users are not provided with a graphical user interface, users have to remember an access code and they have to remember which buttons to press for control of devices.

These home automation systems describe a few of the technologies and approaches, which have emerged, in the field of home automation. Each system achieves a similar functionality, however differs significantly in the communication medium, protocol and interface devices. It has been recognised, that it is not feasible to envisage a single dominant approach to home automation emerging in the near future. The heterogeneous nature of home automation applications and adoption by large multi-nationals, have cumulated in the prevention of a dominant home networking standard from emerging. The benefits of adoption of network technologies, by large multinationals, into their consumer offerings has helped drive down the cost and improve usability of network technology. This has been achieved through the obtainment of effective economies of scale. The British Telecommunications (BT) Home Hub, which incorporates high speed Internet access and a wireless personal area network, is one example of commercial adoption. Sky Multiroom provides a second example of a multimedia network, which streams sky contents to different rooms in the home [5]. The consequences of commercial adoption by large multinationals, has been the introduction of differing communication standards and communication mediums, into the home environment. Inherently, due to a lack of planning and commercial concerns, these systems offer very little interoperability. This lack of interoperability between co-existing networks, leads to three potential problems: 1) Duplication of monitoring activities, 2) the possibility of interference, between co-existing networks and, 3) the potential for two simultaneous, autonomous actions, on co-existing networks, interacting and resulting in an undesirable or even potentially dangerous outcome.

To overcome these difficulties, a home gateway is required to provide interoperability between networks, through a

Manuscript received September 28, 2007. This work was supported in part by the Department of Computer Science at Loughborough University.

K. Gill. is with the Department of Computer Science, Loughborough University, Loughborough, LE11 3TU, UK (phone: + 44 (0)1509 635 648; fax: + 44 (0)1509 635 722; e-mail: k.gill@lboro.ac.uk).

F. Yao. is with the Department of Computer Science, Loughborough University, Loughborough, LE11 3TU, UK (phone: + 44 (0)1509 635 648; fax: + 44 (0)1509 635 722; e-mail: f.yao@lboro.ac.uk).

Prof. S.H. Yang. is with the Department of Computer Science, Loughborough University, Loughborough, LE11 3TU, UK (phone: + 44 (0)1509 635 670; fax: + 44 (0)1509 635 722; e-mail: s.h.yang@lboro.ac.uk).

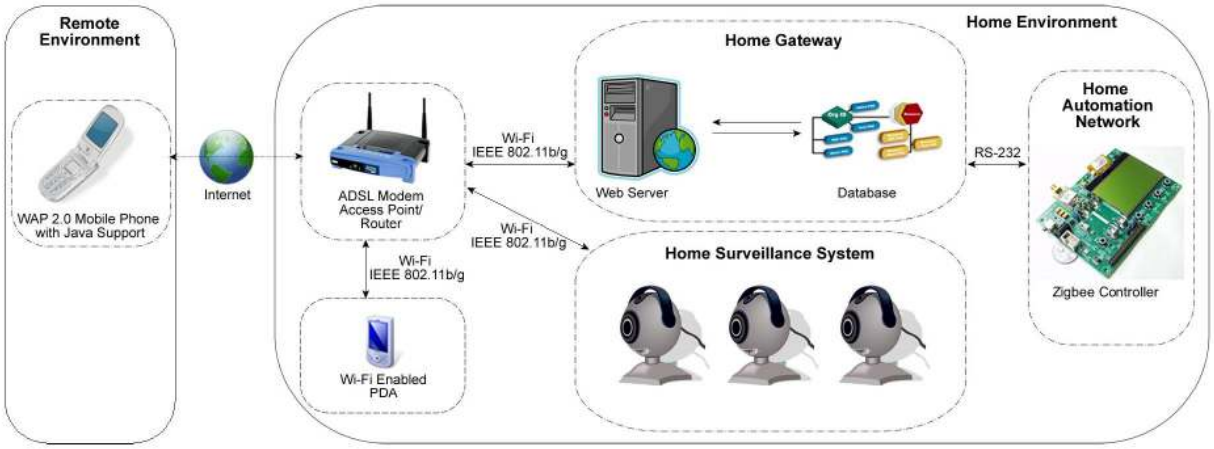


Fig. 1. High Level Architecture Overview

common interface. [6] defined a home gateway as the point of ingress between a personal area network and a public access network. The home gateway interconnected IEEE1394 with a power line based home automation system and the Internet. [7] proposed a home energy management focused home gateway, which connected the home network with the Internet. [8] proposed a home gateway based on the OSGI(Open Service Gateway Initiative), which allows service providers to access home automation systems for administration and maintenance services. This open architecture raises privacy issues, which for some users may be insurmountable, compared to the advantages offered by granting third party access. [9] implements a home gateway, which accepts mobile phone signals and activates or deactivates an LED representing a home device. The proposed system uses socket communications, which raises issues with proxy servers and firewalls, as many block non common ports from communicating.

This paper presents a novel, low-cost and flexible solution for a home gateway. Home owners can control a Zigbee based home automation system and a Wi-Fi based home surveillance system, through a common interface. The home owners can control devices on either network, remotely using any Internet enabled device which supports java and locally through a Wi-Fi personal area network. A common, user interface is developed using Java applet technology and delivered from a web server to any requesting device that is capable of accessing the Wi-Fi personal area network or the public access network.

This paper is organised as follows: Section II discusses the developed gateway and home network architecture, including a review of the technologies used. Section III describes the implementation of the proposed architecture, using a Wi-Fi enabled web server, a Zigbee home network and Wi-Fi based surveillance system and Section IV provides a conclusion.

II. System Architecture

It has been shown, that there exists a complex maze of heterogeneous networks within the home environment. The reasons for this naturally occurring architecture, such as the heterogeneity of requirements for network applications, have been reviewed. It is proposed that consequently, the emergence of a single, universal and dominant network standard is unlikely. A comprehensive review of existing network standards and network technologies in the home environment has been conducted. The review has shown that the use of two complimentary, wireless network standards caters for the majority of network applications. This section illustrates the architecture of a flexible home network infrastructure. In the proposed architecture, a Zigbee based home network is implemented, as the low data rate wireless communication standard. It is believed that the Zigbee standard offers the greatest potential for device control. The Wi-Fi (IEEE 802.11g), wireless, high data rate, standard is implemented to provide communications for multimedia applications. A home gateway is implemented in the home network architecture to provide interoperability, between the heterogeneous Zigbee and Wi-Fi networks, and facilitate remote and local control, over the home networks through a common interface. This architecture is depicted in Fig. 1.

As discussed, the proposed system architecture implements a ZigBee based home automation network and a Wi-Fi based multimedia surveillance network. Alternative standards could have been integrated with the home gateway. However the use of Zigbee and Wi-Fi offers certain advantages.

A. *ZigBee based Home Automation Network*

In the proposed system architecture, a Zigbee based home automation system is implemented. The home automation network extends work, detailed in [10].

The ZigBee standard is a low rate, two way, wireless communication standard. The ZigBee standard is defined by the Zigbee Alliance, a body formed by leading organisations including Motorola, Siemens and Samsung. ZigBee is built on the IEEE 802.15.4 standard. A Zigbee network consists of a network controller, tasked with the creation and

maintenance of the network and end devices. The end devices are wirelessly connected to the controller. The ZigBee standard provides four main advantages, over rival technologies such as Bluetooth. ZigBee has a very low component cost, a low running cost, a flexible address scheme, and provides device interoperability through the use of device profiles.

Low Component Cost: Zigbee offers a low component price of $5 for an integrated microprocessor and RF Radio. For the home automation market, where large numbers of devices will require an integrated Zigbee radio frequency module, low component price is crucial for public adoption.

Low Running Cost: The Zigbee architecture provides for a long battery life. Home automation devices are not required to operate all the time. Experimentation has shown, under certain conditions, with two batteries of 1000mA capacity, in sleep mode and waking repeatedly to transfer 64 bytes of effective data every 10 minutes. A Zigbee device can work theoretically for nearly 25 years.

Flexible Address Scheme: This Zigbee standard allows the network controller to support up to 65, 535 network devices. This provides a great deal of flexibility and scope for more home automation devices to be added at a later stage.

Device Profiles: The Zigbee architecture implements device profiles. A device profile specifies the commands supported by a device and the corresponding communication format. There are two types of profiles: public and private. A device manufacture can use a public profile for their device, in which case all devices supporting the public profile will be interoperable. If a device manufacture wishes to design a device that is not compatible with other manufactures products, a private profile can be used.

B. *Wi-Fi based Home Surveillance Network*

In the proposed system architecture, Wi-Fi is used as the communication standard for a multimedia surveillance system consisting of Wi-Fi enabled video cameras. In addition, the Wi-Fi standard was implemented in the system as a means of control over the Zigbee home automation network, instead of using a Zigbee based controller. This approach was taken because homes increasingly have Wi-Fi networks and Wi-Fi enabled devices such as PDA's and mobile phones. The additional cost of a Zigbee based local control, in these situations is unwarranted. Wi-Fi implements the IEEE 802.11 standard and offers wireless networking through the use of radio frequency. The use of Wi-Fi offers several advantages over alternative technologies. The Wi-Fi standard is more established in homes in the UK, than the alternatives such as Bluetooth, as a wireless home networking technology. The result is less equipment expense for the consumer, and the use of a technology that users are familiar with.

C. *Network Coexistence and Interference*

The home automation network and surveillance network will coexist in the same environment. There is a risk that there may be interference between wireless standards. [11] researched the co-existence of Zigbee, Bluetooth and Wi-Fi. The three protocols use the same 2.4 GHz ISM band. It was found that Zigbee interference has an insignificant effect on Wi-Fi throughput. The effect of Wi-Fi on Zigbee throughput is a 10% reduction, which provides an operable solution. The results are summarised in Table 1. The experiment was repeated using Wi-Fi and Bluetooth. The results showed a 4% – 12% reduction in Wi-Fi throughput and a more serious reduction of 17% - 21% in Bluetooth throughput. The results are summarised in Table 2.

TABLE 1
ZIGBEE AND WI-FI INTERFERENCE [11]

Test Case	% drop in WI-FI throughput	% drop in Zigbee throughput
1	Insignificant	10%
2	Insignificant	10%
3	Insignificant	22%

TABLE 2
BLUETOOTH AND WI-FI INTERFERENCE [11]

Test Case	% drop in WIFI throughput	% drop in Bluetooth throughput
1	12%	21%
2	6%	36%
3	4.6%	17%

It can be concluded that the use of the unlicensed part of the wireless spectrum by Zigbee causes interference problems. Technologies such as Bluetooth, microwave ovens and cordless telephones can cause interference with Zigbee [12]. However, Zigbee and Wi-Fi can exist together with less interference problems than those of the alternative technologies currently available.

D. *Home Gateway*

The home gateway as shown in Fig. 2., is composed of a personal computer hosting a web server and device database. The home gateway is tasked with providing the home networks with the following functionalities:

User Interface: The user interface will be accessed from both the public access networks, such as the Internet, and the home networks, such as Wi-Fi network. The interface must provide a single, common, interface for all devices on the home networks.

Firewall Function: The home network is connected to the public access network. This provides the advantage of world wide connectivity. The potential of skilled attacker who can attempt to interfere with the system is also increased

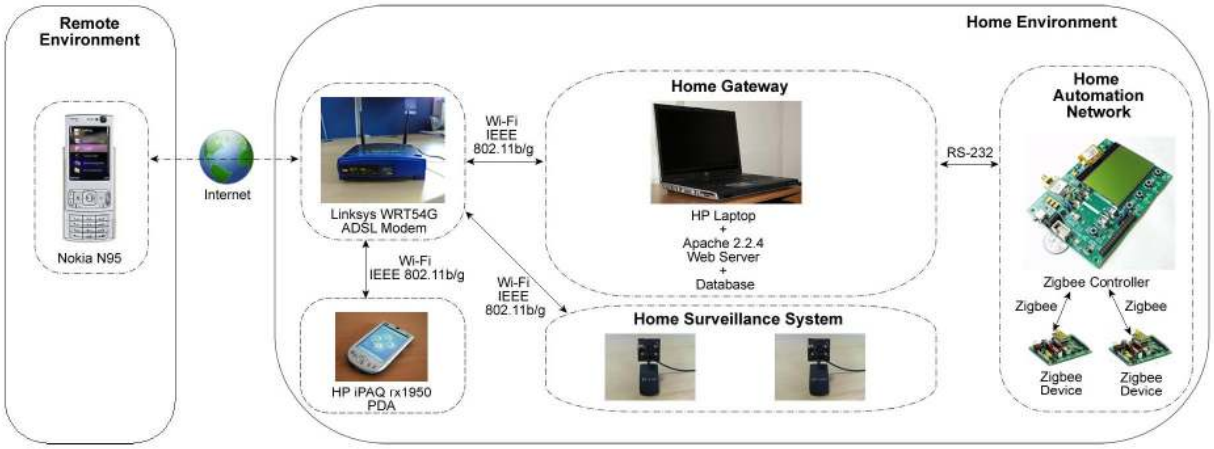


Fig. 2. The Implementation of the Home Gateway

exponentially. The purpose of the firewall is to prevent attackers from gaining unauthorised access and disrupting the normal operation of the system.

Device Database: The Home Gateway must maintain a record of all devices connected to the home networks and their current state. The home automation network collects this information and presents it in a common interface.

Remote Control: A remote user, from anywhere in the world, may wish to access a device on the home network through the internet. The home gateway must handle all authorised user requests.

Local Control: A local user within the range of the home environment, may wish to access the system. The home gateway must handle all authorised user requests and provide the appropriate responses.

III. Implementation

The proposed Home Gateway architecture interconnects a Zigbee home automation network with a Wi-Fi Surveillance network, the local Wi-Fi network and the Internet. The home gateway provides remote access from users on the Internet and local access to users using a Wi-Fi enabled device, such as a PDA or mobile phone. Fig. 2. illustrates that regardless of which network or devices are used to access the system, the interface is consistent.

A. *Hardware Implementation*

The realisation of the system architecture is detailed below. The implementation of this environment can be seen in Fig. 2.

Zigbee Home Automation Network: The Zigbee home automation network was implemented using a Jennic development kit, model JN5139. A more detailed overview of the Zigbee based home automation network is available in the paper [10].

Surveillance Network: The Wi-Fi enabled IP cameras were emulated with the available resources. A web camera was connected to a Wi-Fi enabled laptop through a USB connection. The laptop was running the windows XP operating system, Java Runtime environment (JRE) version 6 update 2, and Java Media Framework (JMF) 2.1.1e.

Home Gateway: The home gateway was implemented using a laptop. The laptop was running the Windows XP operating system, Internet Explorer 7 web browser, Apache Tomcat 6.0.14 web server, and Java Development kit version 1.4.2_07. The laptop was Wi-Fi 802.11g enabled.

ADSL Modem: The device used was a Linksys WRT54G Wireless ADSL Modem Router, incorporating a 4 port switch, with support for IEEE 802.11b/g. The device is connected to the Internet with a fixed IP address. The router is configured to provide a connecting web server with a fixed IP address.

Local Access Device: The device used to access and control the Zigbee network using the Wi-Fi connection, was a HP iPAQ rx1950. The iPAQ comes with the Microsoft Windows Mobile 5.0 Premium Edition operating system, and includes Internet Explorer Mobile, Java runtime environment, Java Media Framework 2.1.1e and a maximum 240x320 pixel resolution.

Remote Access Device: The device used to access and control the, home network devices, from a remote location over the Internet, was a Nokia N95 mobile phone. The Nokia N95 comes with the Symbian operating system version 9.2 running WAP 2.0/xHTML, HTML browser, Java MIDP 2.0 support and Java Media Framework 2.1.1e.

B. *Software Implementation*

The software architecture is composed of a Java Applet, Java Media Framework 2.1.1e, MySQL Database and Java Server Pages. These in unison with the hardware provide the functionality of the home gateway as shown in Fig. 3.

Java Media Framework (JMF): The JMF is installed on the client machines and the laptops, emulating the Surveillance camera. The JMF is required to relay commands from the client to the web camera, when emulating a Wi-Fi network web camera. The JMF component can be removed, with the seamless replacement of the emulated camera with a real Wi-Fi network camera.

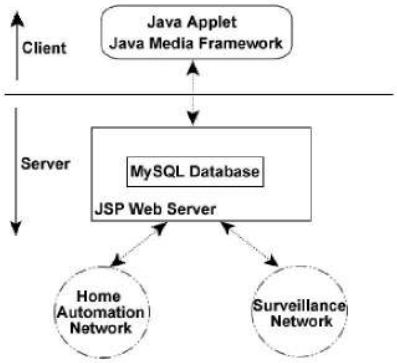


Fig. 3. Software Architecture

Database: The database maintains the state of the devices connected to the home networks and the surveillance network and provides the information for facilitating a single common interface for all the devices. The database also contains the commands associated with the devices on the home network.

C. *System Implementation*

As illustrated in Fig 2, when a user accesses the home gateway, from either the Internet or the local Wi-Fi network, the ADSL modem routes all their communications to the home gateway. The gateway responds on the initial access, by delivering a web page and applet to the client. The applet runs on the browser, providing the user interface on the client machine. All communications are sent by http to avoid problems with security issues, arising due to the use of non web ports as described earlier. The Java applet monitors the database on the web server and updates the user display as appropriate. The Java application relays the commands received to either the home network or the surveillance network and updates the device database. As shown in Fig. 4. The IP camera waits to receive a request from a client, to start streaming video. Once the request is received the Video is streamed to the clients IP address. The client's browser creates a media player, in which the video stream is displayed. The software interactions of the home automation system and the home gateway are shown in Fig. 5. The home gateway waits to receive a command. Once this command is received, it is routed to the home automation system. The ZigBee controller acts upon and responds to the command received, from the home gateway. The effects of the commands actions are relayed to the client, through the interface provided by the home gateway.

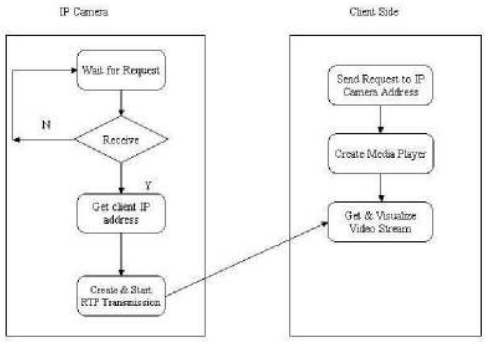


Fig. 4. Work Flow of Surveillance System

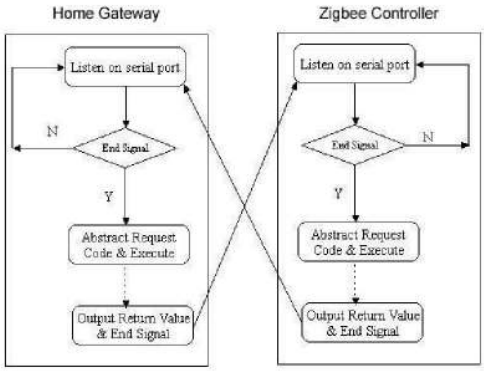
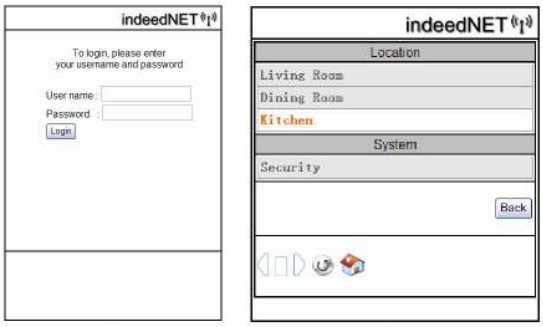


Fig. 5. Work Flow of Home Automation System

The login screen is the initial screen, a user accessing the system will see, as shown in Fig. 6.a. After successful authentication, the user is directed to the main menu page as shown in Fig 6.b. The main menu page allows the user to browse the connected devices by location or system.



a. b.

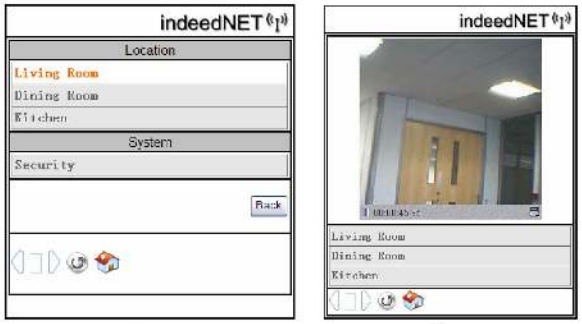
Fig. 6. (a) System Login Screen; (b) Main Interface Screen.

Fig. 7.a. illustrates a ZigBee node on the home automation network. The LED on the circuit board is off. This LED represents a light in a light network. A user may view the current status of the LED, through the user interface as shown in Fig. 7.b. The user can modify this setting, as shown in Fig. 7.c. The LED is now on.

a. b. c.

Fig. 7. (a) ZigBee device node, showing an inactive LED; (b) Common Interface, for modifying ZigBee network; (c) ZigBee device node, showing an active LED.

The network type to witch a home device is connected, is transparent to the user as can be seen in Fig. 8.a. The user selects a location in the home or a device, in this case the security system. The user is then presented with the output of the surveillance network as shown in Fig. 8.b.



a. b.

Fig. 8. (a) Screen shot showing the common Interface used to access surveillance network; (b) The users view of the Surveillance Camera Output.

The code to create the media player and access the stream from the surveillance camera is as follows:

```
objectAddress =
"rtp://"+ipCameraAddress+":"+port+"/video";
        ml = new MediaLocator(objectAddress);
        player=Manager.createRealizedPlayer(ml);
        player.start();

javax.media.Time comp2 = player.getMediaTime();

Component comp = player.getVisualComponent();
        player.setMediaTime(comp2);
```

IV. CONCLUSION

A home gateway architecture, incorporating two heterogeneous home networks, is designed, implemented and tested. The two home networks consist of a home automation system, and a surveillance system. The home gateway connects to the Internet, a public access network, and Wi-Fi, a local area home network. This in turn allows them to access and interact with the Zigbee IEEE 802.15.4 based home automation network and the Wi-Fi IEEE 802.11g based surveillance network. This interaction is mediated, through a common interface, regardless of the network used to access the home gateway. The system implements a method of data translation between ZigBee and Wi-Fi, two complimentary, heterogeneous standards. Through the use of these complimentary technologies, a home network structure capable of fulfilling the requirements of most home automation applications has been implemented. The advantage of the proposed architecture, over those who provide Zigbee networks without a home gateway, is the expansion of access from the local environment to a global environment. The existing home gateways have used methods of communication, such as socket communications. However firewalls and proxy servers often block ports from communicating. To overcome these issues common web ports have been used in the proposed architecture, which are accessible from most networks. The home gateway provides the same interface for all the products connected to the home network. This will help overcome the users being overwhelmed by multiple interfaces, unlike other home gateways which provide different interfaces depending on the access network used. The limitation imposed by the home gateway architecture, requires the use of an expensive personal computer to act as the web server.

REFERENCES

[1] K. Bromley, M. Perry, and G. Webb, eds. Trends in Smart Home Systems, *Connectivity and Services*. www.nextwave.org.uk, 2003.

[2] A. R. Al-Ali and M. Al-Rousan, Java-based home automation system, *IEEE Transactions on Consumer Electronics*, 50(2), 2004, 498-504.

[3] N. Sriskanthan, F. Tan and A. Karande, Bluetooth based home automation system. *Microprocessors and Microsystems*, 26(6), 2002, 281-289.

[4] H. Ardam and I. Coskun, A remote controller for home and office appliances by telephone. *IEEE Transactions on Consumer Electronics*, 44(4), 1998, 1291-1297.

[5] Sky. *Sky Tv Prices and Packages*, http://www.sky.com/portal/site/skycom/skyproducts/skytv/pricesandpackages, 2007.

[6] T. Saito, I. Tomoda, Y. Takabatake, J. Ami and K. Teramoto, Home Gateway Architecture And Its Implementation. *International Conference on Consumer Electronics*, 2000, 194-195.

[7] N. Kushiro, S. Suzuki, M. Nakata, H. Takahara and M. Inoue, Integrated home gateway controller for home energy management system. *Proceedings of IEEE International Conference on Consumer Electronics*. 2003, 386-387.

[8] S. Ok and H. Park, Implementation of initial provisioning function for home gateway based on open service gateway initiative platform. *The 8th International Conference on Advanced Communication Technology*, 2006, 1517-1520.

[9] D. Yoon, D. Bae, H. Ko and H. Kim, Implementation of Home Gateway and GUI for Control the Home Appliance, *The 9th International Conference on Advanced Communication Technology*, 2007, 1583-1586.

[10] F. Yao, K. Gill and S. Yang, A ZigBee Based Low Cost Automation System. *The 13th Annual Conference of Chinese Automation and Computing Society in the UK*, 2007.

[11] K. Shuaib, M. Boulmalf, F. Sallabi and A. Lakas, Co-existence of Zigbee and WLAN - a performance study. Wireless and Optical Communications Networks, *IEEE International Conference on Wireless and Optical communications*, 2006, 5-9.

[12] Jennic, JN-AN-1059 Deployment guidelines for IEEE 802.15.4/ZigBee wireless networks. 2007, 37-38.