A ZigBee-Based Home Automation System

Khusvinder Gill, Shuang-Hua Yang, Fang Yao, and Xin Lu

Abstract — *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 for the purpose of home automation. Moreover, with the rapid expansion of the Internet, there is the added potential for the remote control and monitoring of such network enabled devices. However, the adoption of home automation systems has been slow. This paper identifies the reasons for this slow adoption and evaluates the potential of ZigBee for addressing these problems through the design and implementation of a flexible home automation architecture. A ZigBee based home automation system and Wi-Fi network are integrated through a common home gateway. The home gateway provides network interoperability, a simple and flexible user interface, and remote access to the system. A dedicated virtual home is implemented to cater for the system's security and safety needs. To demonstrate the feasibility and effectiveness of the proposed system, four devices, a light switch, radiator valve, safety sensor and ZigBee remote control have been developed and evaluated with the home automation system.*

Index Terms — Home Automation, ZigBee, Sensor Network.

I. INTRODUCTION

In recent years the introduction of network enabled devices into the home environment has proceeded at an unprecedented rate. Moreover, with the rapid expansion of the Internet, there is the potential for the remote control and monitoring of such network enabled devices. However, the new and exciting opportunities to increase the connectivity of devices within the home for the purpose of home automation remain largely unexploited.

A. Existing Home Automation Technologies

There are many definitions of home automation available in the literature. [1] describes home automation as the introduction of technology within the home to enhance the quality of life of its occupants, through the provision of different services such as telehealth, multimedia entertainment and energy conservation.

There has been significant research into the field of home automation. The X10 industry standard, developed in 1975 for communication between electronic devices, is the oldest standard identified from the author's review, providing limited control over household devices through the home's power lines. Recently, research into the field of home automation has continued to receive much attention in academia. [2] developed a Java based home automation system. An embedded board physically connected all the home automation devices and, through integration with a personal computer (PC) based web server, provided remote access to the system. The use of Java technology, which incorporates built-in network security features, produces a secure solution. However, the system requires an intrusive and expensive wired installation and the use of a high end PC. [3] introduced a Bluetooth based home automation system, consisting of a primary controller and a number of Bluetooth sub-controllers. Each home device is physically connected to a local Bluetooth sub-controller. The home devices communicate with their respective sub-controller using wired communications. From the sub-controller all communications are sent to the primary controller using wireless communications. It is desirable for each home device to have a dedicated Bluetooth module. However, due to the fiscal expense of Bluetooth technology, a single module is shared amongst several devices. This architecture reduces the amount of physical wiring required and hence the intrusiveness of the installation, through the use of wireless technology. However, the architecture does not completely alleviate the intrusiveness of the installation due to the incorporation of some wired communications. Moreover the sharing of a single Bluetooth module between numerous devices has the disadvantage of incurring an access delay. [4] introduced 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 over the Internet. The system can be accessed using any telephone that supports dual tone multiple frequency (DTMF). 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 the control of connected devices. [5] proposed a novel control network, using hand gestures. The controller uses a glove to relay hand gestures to the system. The problem with the system lies in the inaccuracy of hand gestures, with the potential for normal arm movements being inaccurately interpreted as commands. Moreover, there is the risk of user fatigue if repetitive hand gestures are required.

The introduction provides a short review of the existing academic research into home automation. The publically available research into home automation lies predominantly in the academic arena, with little industrial research being publically available. The adoption of home automation technologies into commercial systems has been limited, and where available consumer uptake has been slow.

The aforementioned systems offer little in the way of interoperability. Attempts have been made to provide network

K. Gill, S. H. Yang, F. Yao and X. Lu are with the Computer Science Department, Loughborough University, Loughborough, England, LE11 3TU (e-mail: s.h.yang@lboro.ac.uk).

Contributed Paper
Manuscript received November 8, 2008

interoperability and remote access to home automation systems through the development of home gateways. [6] defined a home gateway as the point of ingress between a personal area network and a public access network. They developed a web server based home gateway to interconnect IEEE1394, with a power line based home automation system, and the Internet. To make the system more attractive to home owners, a real time AV transcoding capability was included. The system offers an insightful look into the development of a home gateway; however, the use of power lines as the communication medium limits the positioning of devices within the home to areas in close proximity to power sockets. [7] proposed a home energy management focused home gateway, which connects the home network with the Internet. The system was installed in twenty houses in the Tokyo area. [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. The proposed system is divided into two subsystems. The first is the DSM (Digital Home Service Distribution and Management System), which provides a user interface for the control and monitoring of connected home automation devices. The second is the Home Gateway, which is responsible for managing the home automation system. This open architecture raises privacy problems which, for some users, may be much greater than the advantages offered by granting third party access. [9] implements a home gateway that accepts mobile phone signals and activates or deactivates a LED representing a home device.

These systems have made a significant contribution to the development of a home gateway. However, the existing network infrastructure within the home environment has not been taken into consideration when selecting the networks for integration with the respective home gateways. Moreover, the existing research has focused on the provision of remote connectivity and has largely neglected investigating the integration of existing local networks.

B. Analysis of the Existing Systems

The adoption of home automation technology by consumers has been limited. We propose that, from the home automation domain analysis, the problems limiting wide spread consumer adoption can be grouped into five general categories. Firstly, ***complex and expensive architecture***: the existing systems architectures generally incorporate a personal computer for the purposes of network management and provision of remote access. This adds additional complexity to the system, hence increasing the overall fiscal expense. Secondly, ***intrusive installation***: the majority of systems require varying levels of physical wiring in their architectures. This, in some cases, is due to the expense of the alternative wireless technologies. Hence, these systems require intrusive and expensive installations. Thirdly, ***lack of network interoperability:*** both home networks and the home automation systems which utilise them have been developed and adopted in an unplanned and ad-hoc manner. This has lead to a home environment consisting of a complex maze of heterogeneous networks. These networks and the systems that utilise them normally offer little interoperability; leading to three potential problems

- *duplication of monitoring activities, due to lack of interoperability;*
- *the possibility of interference, between co-existing networks; and*
- *the potential for two simultaneous, autonomous actions on co-existing networks, interacting and resulting in an undesirable outcome.*

Fourthly, ***interface inflexibility***: the existing systems offer varying approaches for users to control and monitor the connected devices. However, this is normally limited to a single method of control, which offers users limited flexibility. The systems which provide more than one interface device normally provide different user interfaces and risk confusing users. Finally, ***security and safety***: the existing approaches have not focused on security and safety problems that may arise from their implementation. Moreover, the systems that offer some degree of security have neglected the problems with sharing information between devices produced by multiple vendors for the purposes of establishing security.

C. Features of the proposed System

This paper presents a novel, stand alone, low-cost and flexible ZigBee based home automation system. The architecture is designed to reduce the system's complexity and lower fiscal costs. Hence, the system endeavours not to incorporate complex and expensive components, such as a high end personal computer, where possible. The system is flexible and scalable, allowing additional home appliances designed by multiple vendors, to be securely and safely added to the home network with the minimum amount of effort. The system allows home owners to monitor and control connected devices in the home, through a variety of controls, including a ZigBee based remote control, and any Wi-Fi enabled device which supports Java. Additionally, users may remotely monitor and control their home devices using any Internet enabled device with Java support. A home gateway is implemented to facilitate interoperability between heterogeneous networks and provide a consistent interface, regardless of the accessing device.

A virtual home pre-processes all communications before they are realised on the real home automation system. All communications are checked for security and safety before being allowed to continue to their respective destinations.

This paper is organised as follows: Section 2 discusses the developed home automation architecture, including a review of the technology used. Section 3 describes the implementation of the proposed system. Section 4 provides a discussion of the system evaluation and Section 5 provides a conclusion.

II. SYSTEM ARCHITECTURE

This section describes the conceptual design of a flexible and low cost home automation infrastructure (see Figure 1). The home's low data rate, control and monitoring needs are catered for using Zigbee. The home's high data rate needs, such as multimedia applications, are met by the Wi-Fi (IEEE 802.11g) standard.

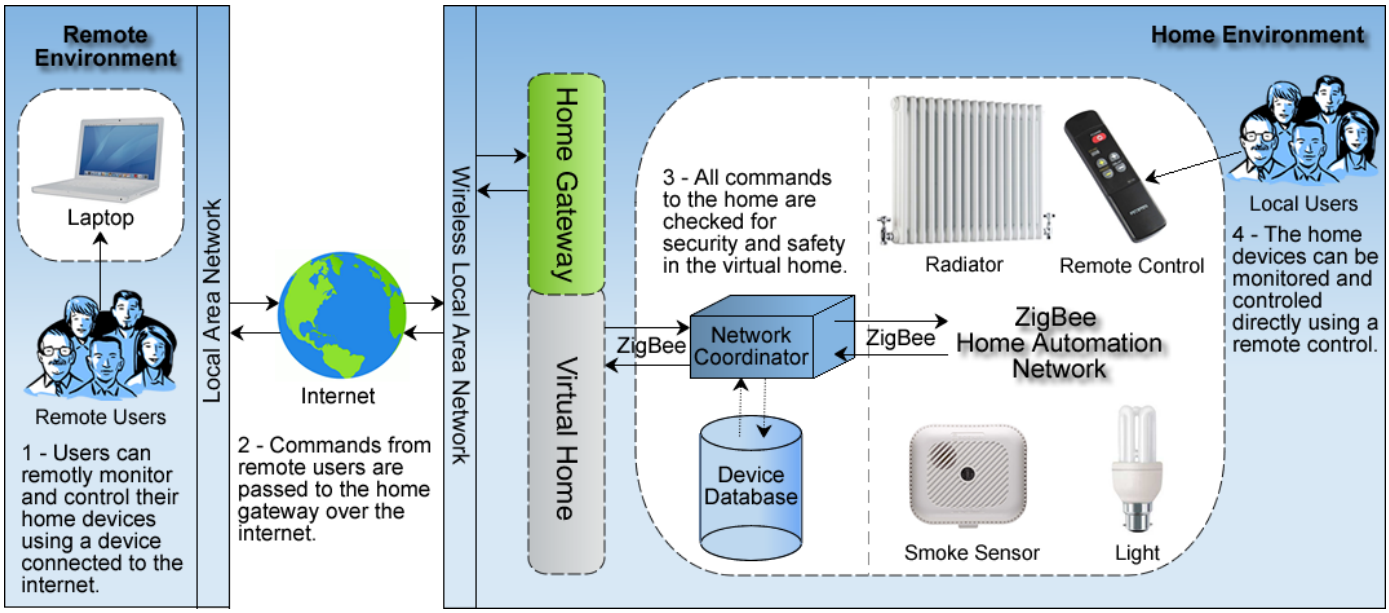

Fig. 1. Conceptual Architecture Overview.

A home gateway is implemented to provide interoperability between the heterogeneous Zigbee and Wi-Fi networks, and facilitate local and remote control and monitoring over the home's devices. A virtual home is implemented for the provision of real time security and safety for the home and its inhabitants.

As depicted in Figure 1, the proposed system consists primarily of four steps. Remote user can access the system using the Internet. The remote user's communications traverse the internet until they reach the home network. They are then wirelessly transmitted to the Home Gateway using the homes Wi-Fi network. The Home Gateway is integrated with a virtual home. These communications are checked and processed by the home gateway and virtual home, as discussed in greater detail later. This checking process involves communication with the home networks coordinator, which is integrated with the home's device database and contains the status of all connected devices. Once checked the communications are sent to the real home automation system and the respective device. Additionally, a local ZigBee based remote control can be used to directly control connected devices.

A. Residential Networks

As discussed, the proposed system architecture implements a ZigBee based home automation network and a Wi-Fi based multimedia network. Alternative standards could have been integrated with the home gateway. However, the use of Zigbee and Wi-Fi offers certain advantages. Zigbee technology is designed to be used on applications that require low data rate, low-cost, low power consumption, and two way wireless communications. The Wi-Fi standard is designed to provide relatively high data rate communications. Wi-Fi has the advantage of an existing and wide spread presence in homes in the United Kingdom. The combination of Zigbee and Wi-Fi technologies has the potential to provide a comprehensive home automation solution.

Zigbee technology

ZigBee is a radio frequency (RF) communications standard based on IEEE 802.15.4. Figure 2 depicts the general architecture of a Zigbee based home automation network. The Zigbee coordinator is responsible for creating and maintaining the network. Each electronic device (i.e. Washing Machine, Television, Lamp etc) in the system is a Zigbee device managed by the coordinator. All communication between devices propagates through the coordinator to the destination device. The wireless nature of ZigBee helps overcome the intrusive installation problem with the existing home automation systems identified earlier. The ZigBee standard theoretically provides 250kbps data rate, and as 40kbps can meet the requirements of most control systems, it is sufficient for controlling most home automation devices. The low installation and running cost offered by ZigBee helps tackle the expensive and complex architecture problems with existing home automation systems, as identified earlier.

Wi-Fi Technology

In the proposed system architecture, Wi-Fi is used for two primary purposes. Firstly, it is the chosen communication standard for multimedia applications in the home. Secondly, it is used to provide access to the home automation system from Wi-Fi enabled devices, as an alternative to the Zigbee based local 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 controller in these situations is unwarranted. Moreover, the high data rate nature of Wi-Fi allows for greater flexibility in interface design. Wi-Fi implements the IEEE 802.11 standard and offers wireless networking through the use of radio frequency. There are different versions of this protocol. The dominant protocol in use today is IEEE 802.11g, which operates in the unlicensed 2.4 GHz band and provides a maximum raw data rate of 54 Mbps.

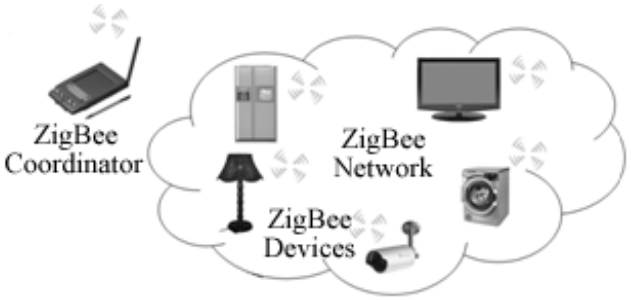

Fig. 2. Zigbee Home Automation Architecture.

The use of Wi-Fi offers several advantages over alternative technologies. The Wi-Fi standard is more established in homes in the UK than 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 users are familiar with.

Network Coexistence

Heterogeneous and homogenous home networks may co-exist with each other in the same environment. The problem of interference between these networks increases as more and more standards emerge which use the same communication mediums. The interference problems between the possible standards have been investigated. [10] 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 in throughput, which provides an operational solution. The experiment was repeated using Wi-Fi and Bluetooth. The results showed a significant reduction in Wi-Fi throughput and Bluetooth throughput. 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 [11]. However, Zigbee and Wi-Fi can exist together with less interference problems than alternative technologies currently available, hence offering the best combination available for use in our purposed architecture.

B. Home Gateway

The home gateway, as depicted in Figure 1, is charged with providing interoperability between different connecting networks. The home gateway provides two primary functions for the proposed architecture. Firstly, the home gateway provides data translation services between the Internet, Wi-Fi, and ZigBee networks. Secondly, the home gateway provides a standardised user interface for devices connecting to the ZigBee home network, remotely using the Internet or locally using the Wi-Fi network. The home gateway does not provide a standardised interface for the local ZigBee remote control (See Figure 1). This decision was made to provide greater freedom for interface design and avoid limitations that have to be taken into consideration in the design of the low data rate, low power ZigBee remote control interface. Although, as depicted, the close cooperation between the home gateway and device database allows for the real time control and monitoring of all home devices, regardless of the access device and network used. The home gateway is implemented in the system architecture to overcome the problem of insufficient network interoperability, identified in existing home automation approaches. Moreover, the proposed approach looks at the existing network structure within the home environment and integrates networks which are predominantly established in the existing home environment. Additionally, the home gateway reduces the inflexibility in the control modes of existing home automation systems; this is undertaken through the prevision of manual, local and remote control. Furthermore, the interface of the controlling devices is standardised across the control modes.

C. Virtual Home

The virtual home, as depicted in Figure 1, is responsible for the administration of security and safety for the home automation system. The virtual home, as the name suggests, is a virtual environment where the actions requested by users are checked. For the purposes of security, all the messages received by the virtual home are checked by authenticating the senders, checking the integrity of the messages to ensure they have not been tampered with, and protecting the confidentiality of messages through the use of encryption. The system's safety is protected by ensuring the commands received are appropriate for the respective home network and that all changes requested fall within the specified safety limits. The primary objective of the virtual home is to prevent any event that may pose a security or safety concern from implementation in the home networks. The virtual home is included in the proposed architecture to tackle the security and safety problems.

D. Device Engine

The home automation system is designed to be flexible, allowing different devices designed by multiple vendors to be connected. Each device incorporates a dedicated engine, responsible for providing the necessary application functionality and ZigBee network connectivity. Moreover, each device engine may contain dedicated security and safety measures. Critical devices should check all requested operations to ensure that they will not result in an undesirable outcome. Furthermore, collaboration with the virtual home should provide the necessary information to facilitate secure communications.

III. SYSTEM IMPLEMENTATION

The implementation of the proposed system is illustrated in Figure 3. As depicted, a ZigBee based home automation system is implemented for the monitoring and control of household devices. To cater for the household's high data rate needs, such as multimedia entertainment, a Wi-Fi network is implemented. A home gateway has been developed to provide interoperability between these networks. The home gateway presents a unified interface for users to locally and remotely access home networks. The security and safety of the home automation network is realised through the development of the earlier described virtual home on the Home Gateway. To demonstrate the feasibility and effectiveness of the proposed

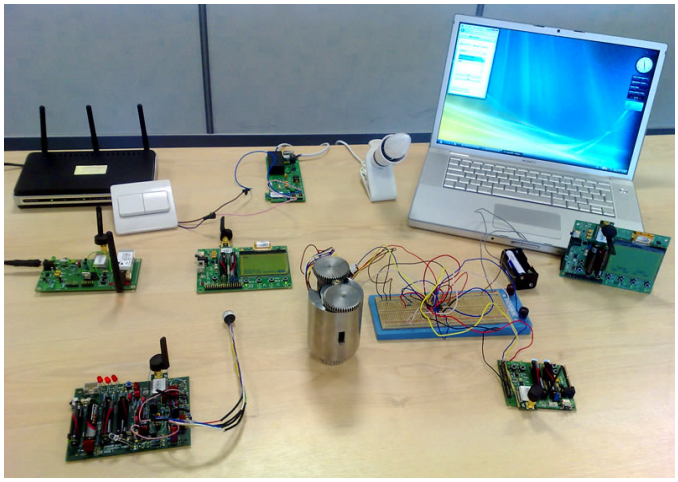

Fig. 3. System Implementation.

system four devices, a light switch, radiator valve, safety sensor and ZigBee remote controller have been developed and integrated with the home automation system. This section provides a thorough discussion of the system implementation.

A. ZigBee Home Automation Network

The ZigBee home automation network consists of a coordinator, routers and several end devices. The coordinator is responsible for starting the ZigBee network. During the network initialisation phase, the coordinator scans the available radio channels to find the most suitable. Normally this will be the channel with the least activity, in order to reduce the level of interference. It is possible to limit the channels scanned, for example excluding those frequencies ranges used by the Wi-Fi network included in the proposed architecture. However, our experiments have shown that the average time taken to scan all the available channels is 9 seconds (to the nearest second). This scan time is relatively small and as the home coordinator is initialised infrequently this is an acceptable delay when contrasted with the performance increase possible through the use of a channel with less interference. The coordinator is pre-programmed with the PAN ID (Personal Area Network Identifier), although it is possible for the coordinator to dynamically scan for existing network PAN IDs in the same frequency and generate a PAN ID that does not conflict. All home devices connected to the ZigBee home automation network are assigned a fixed 64 bit MAC address. Additionally, each device is assigned a dynamic 16 bit short address that is fixed for the lifetime of the network. At this stage of the network initialisation, the coordinator assigns itself the short address 0x0000. After the coordinator's initialisation phase the coordinator enters "coordinator mode", during this phase it awaits requests from ZigBee devices to join the network.

The ZigBee devices developed for the home network, as mentioned, includes a light switch, radiator valve, safety sensor and ZigBee remote control. A ZigBee end node has been integrated with these devices. As the devices are started, during their respective initialisation stage, the node scans for available channels to identify the network it wishes to join. There may be multiple networks in the same channel, these networks are normally distinguished by their PAN ID. The node selects which network to join based on the PAN ID. The node sends a request to the network coordinator to join the network. The request is sent to the coordinator directly or through a neighbouring router on the desired network with which the node shares the best signal. On receipt of the request the coordinator judges whether the requesting device is permitted to connect to the home automation network. The standard implementation of most ZigBee networks prevents unauthorised devices joining the network by providing a short user defined period where device may join. This, in our opinion, does not on its own provide sufficient network security. To enhance the systems security the proposed system encrypts all device communications including the requests to join the home network with a private key. Only those devices that are in possession of the correct private key can successfully connect to the home network. The devices that are permitted to join the network are recorded in the device database and stored on the network coordinator. A partially connected mesh topology was adopted for the ZigBee home automation network. Due to the nature of the home environment where communication interference is constantly fluctuating, the advantage of increased communication routes available through the adoption of a mesh topology outweighs the added routing complexity.

B. Wi-Fi Network

The homes Wi-Fi network was implemented through a standard Wireless (802.11b and 802.11g) ADSL Modem Router, with a 4 port switch. The modem provides two primary functions. Firstly, the modem provides the connection between the Internet and local Wi-Fi network; hence extending access to the Wi-Fi enabled home gateway to any location with Internet access. Secondly, any local Wi-Fi enabled device within range of the home's Wi-Fi network can directly access the home gateway. This provides a low cost communication method with the home network, reduced infrastructure costs where Wi-Fi devices are already in use. Moreover, home owners can monitor and control the home automation network, using familiar technology and devices.

C. Home Gateway

A thorough review of existing home gateway technologies revealed that no off-the-shelf solution exists that provides the functionality specified in the requirements for the home gateway, as previously discussed. This included the provision of interoperability between the Internet, Wi-Fi and ZigBee networks. Hence, it was necessary to develop a bespoke home gateway, as shown in Figure 4. The home gateway consists of a Wi-Fi module, a ZigBee Microcontroller and a power supply. The Wi-Fi module provides low cost and embedded serial to Wi-Fi connectivity. The ZigBee Microcontroller provides the connection to the ZigBee network. The Wi-Fi module connects to the home's local Wi-Fi network and the ZigBee microcontroller connects to the ZigBee home network as an end device. The home gateway once started enters the configuration stage. During the configuration stage the embedded Wi-Fi module establishes a connection with a local Wi-Fi network.

Fig. 4. Home Gateway.

The parameters for the Wi-Fi connection such as network SSID and security parameters are preconfigured. Simultaneously, the ZigBee microcontroller searches for a ZigBee home network and, as discussed, establishes a connection. As with the Wi-Fi module, the ZigBee microcontroller's connection parameters are preconfigured. This concludes the configuration stage.

Once the home gateway has been initialised, an idle state is entered into until input is received. Input can originate from both the Wi-Fi network for input to the ZigBee network, or conversely from the ZigBee network for output to the Wi-Fi network. Input from the Wi-Fi network normally takes the form of commands from user interface devices. The input from the ZigBee network normally takes the form of responses to commands received earlier from user interface devices.

D. Virtual Home

The virtual home is a software construct developed in C. The virtual home is implemented on the home gateway. All communication and instructions are checked, as illustrated in Figure 5, for security and safety, in the virtual environment, before implementation in the real home environment. The virtual home waits for input from an external source. All devices on the ZigBee network incorporate the ZigBee microcontroller and a dedicated AES Coprocessor. Sensitive communications on the home network are encrypted. Hence, the message payload of sensitive communications received by the virtual home from legitimate sources will be encrypted with a valid symmetric key. Once the security of messages has been established, the virtual home checks the safety implications of the messages. After decryption the destination device address is extracted from the message and checked in the device database for its existence. Once the device's existence on the network has been established, the command and parameters included in the message are extracted. The existence of the command for the respective device is checked to ensure the real device offers the requested functionality. The extracted parameters are compared against predefined safe ranges for the respective device and command. Only after the message has been processed by the virtual home algorithm for security and safety and declared safe is the message is re-encrypted and forwarded to the real home network device.

E. User Interface Devices

To evaluate the effectiveness of the system architecture for the provision of easy to implement, and flexible modes of control; three control modes were developed.

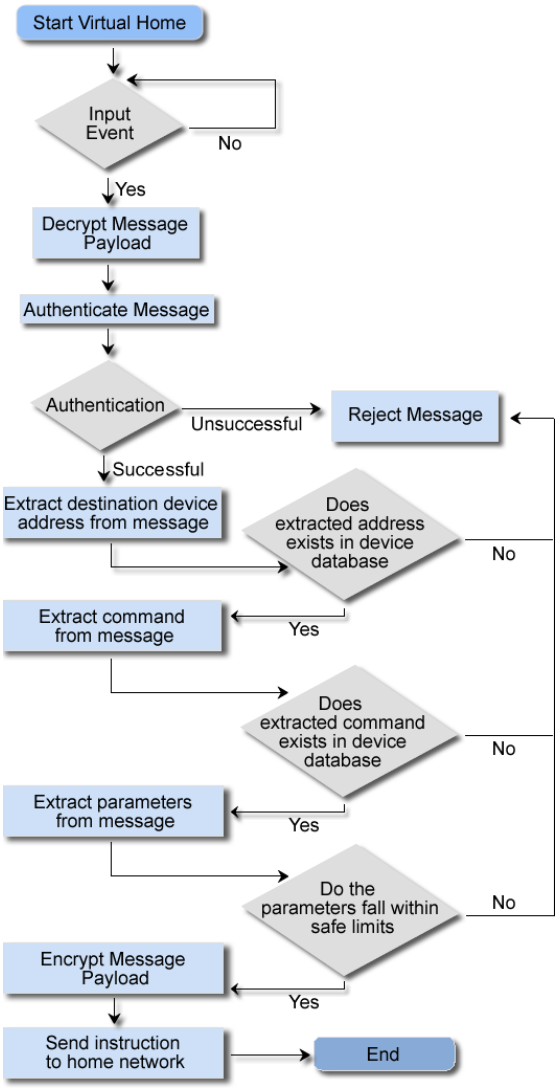

Fig. 5. Virtual Home Flow Chart.

ZigBee Remote Control: A low cost, simple-to-use remote controller, for the local monitoring and control of devices was developed. The controller board includes a ZigBee microcontroller, LCD display, four push button switches, and is powered by four AA batteries. Instructions from the remote control traverse the home network until received by the destination device.

Remote Access Device and Wi-Fi Remote Control: A standard mobile phone with built in support for Wi-Fi and J2ME was used to access and control the system. While locally accessing the system the mobile used Wi-Fi to freely access and control the system. When a Wi-Fi connection was not available the mobile established an Internet connection to access and control the system. In both scenarios the instructions sent from the mobile phone are received by the home gateway, which

translates the communication and forwards it to the virtual home, as discussed, before being sent to the destination device.

F. Home Automation Devices

To demonstrate the feasibility and effectiveness of the proposed system three devices; a light switch, radiator valve, and safety sensor, were developed. These devices are depicted in figures 6 (a), (b), and (c) respectively.

a. b. c.

Fig. 6. (a) ZigBee operated light bulb in the off state; (b) ZigBee based automatic radiator valve; (c) ZigBee safety sensor.

Light Switch: A conventional light switch was integrated with a ZigBee microcontroller, as shown in Figure 6 (a). In this prototype the user could access the light switch, detect the lights current state ("On" or "Off"), and adjust the state accordingly.

Radiator Valve: A prototype automatic radiator valve was developed and integrated with a ZigBee microcontroller, as shown in Figure 6 (b). The valve can be manually controlled as are conventional valves, but also remotely monitored and controlled.

Safety Sensor: The safety sensor has special characteristics of interest. For instance, unlike most devices, the safety sensor has to continuously monitor its environment and provide feedback. This reduces the time the device can operate in sleep mode, hence considerably reducing the battery life. A safety sensor was developed (see Figure 6 (c)) to investigate the potential viability of the system with a mass market end device that places a large demand on system resources. The safety sensor developed incorporated temperature, carbon monoxide, flame, and smoke sensors.

G.System Configuration

This section has described in detail the individual elements that combine to implement the proposed system architecture. A user can login to monitor and control the home automation systems end devices, using one of three user interface devices (ZigBee remote control, Wi-Fi remote control, and Remote access device). All messages from the devices using the Internet for communication are sent to the home's IP address. The messages are forwarded to the home gateway's IP address on the local Wi-Fi network, through a Wi-Fi enabled ADSL modem. Similarly, communications from the devices using the Wi-Fi network for communications are forwarded to the home gateway's IP address. Once the home gateway has received the messages they are forwarded to the virtual home. Messages from the ZigBee controller are sent directly to the end devices, over the ZigBee network. The virtual home checks the security and safety of all received messages. Those messages that fail to validate are rejected, the validated messages are forwarded to the destination device on the real home network. All responses from the device (i.e. acknowledgments, device status notifications, sensor readings) are relayed from the device, through the ZigBee network to the virtual home, through the home gateway, across the Wi-Fi network and, where appropriate, across the Internet to the user interface device.

IV. Evaluation

The implemented system was evaluated both quantitatively and qualitatively. To demonstrate the feasibility and effectiveness of the proposed system, four devices, a light switch, radiator valve, safety sensor and ZigBee remote control have been developed and integrated with the home automation system. These systems were subjected to a cycle of strenuous operations to simulate a high level of everyday usage. The light state was changed 20 times using the ZigBee remote control and 20 times using the Wi-Fi controller. Similarly the radiator valve state was changed 20 times using the ZigBee controller and 20 times using the Wi-Fi controller. The experiments showed the correct functionality of the devices 100% of the time. Table 1 provides a summary of the average delay between request and implementation of the requested change using the Zigbee and Wi-Fi controllers.

TABLE 1
ZIGBEE AND WI-FI CONTROLLER ACCESS DELAY

	Light Switch	Radiator Valve
ZigBee Controller access delay in ms	670	*N/A
Wi-Fi Controller access delay in ms	1337	613

*N/A indicates that the time delay was too short to be recorded by the test equipment.

As Table 1 indicates, the average access delay was greater for the Wi-Fi controller than for the ZigBee controller. However, the ZigBee controller had an average access delay of 670 ms while controlling the light switch, whereas the access delay incurred for controlling the radiator valve was small and subsequently could not be measured with our recording instruments. This implies that the majority of the access delay lies in the actuation of the light switch and subsequent bulb state change and is not attributable to the method of control. This is shown with a N/A in Table 1. Taking this into account the access delay for the light bulb (1337 ms) can be adjusted by removing the 670 ms access delay attributed to the switch actuation to provide a more realistic access time for the Wi-Fi controller for the light switch of 667 ms. This average access delay is supported by the access delay recorded for the radiator valve of 613 ms.

The viability of the home automation architecture was evaluated through real world testing of the proposed system with the developed radiator valve. The radiator valve, as depicted in Figure 6 (b), was tested in a real house. The radiator valve was located in the test house's living room, on

the ground floor as depicted in Figure 7. The radiators existing TRV valve was replaced with the prototype automatic radiator valve. The local controller was put on a desk 2m away from the radiator and connected to a laptop. This configuration allowed test software running on the local controller to print out the desired temperature set by the user, current temperature around the radiator and time taken to reach the desired temperature by the automatic radiator valve. Figure 8 shows the experimental environment.

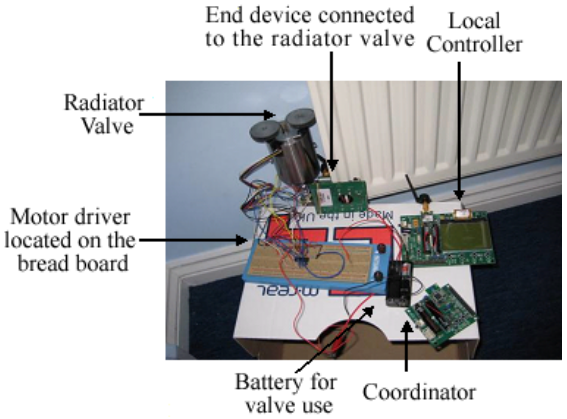

Fig. 7. Radiator Valve Replacement

The results of the experiments are summarised in Figure 9. The graph shows the desired temperature set by the user (Set Point) against the actual temperature (Measured Value) of the radiator at a regular interval of 15 minutes. As depicted, the actual temperature of the radiator quickly adjusted to the desired temperature set by the user, and this holds true for most temperature ranges set by the user. However, the actual temperature could not reach $25^{o}C$, it was surmised that the radiator was too small to heat such a large room to this temperature. The evaluation of the radiator valve shows the applicability of the proposed system with a real world end product. The experimentation highlighted that a radiator valve could successfully be implemented using the ZigBee communication standard and monitored and controlled using the proposed system. This successful evaluation supports and demonstrates the potential of the proposed system to be easily adaptable from the lab environment to the commercial market.

Fig. 8. Experimental Environment

For the qualitative analysis of the proposed system, a focus group was conducted on the 4th of March 2008 to evaluate end user's perspectives of the proposed architecture and obtain feedback as to areas for further work. The focus group consisted of ten members from a UK Housing Association (HA) who were chosen to reflect the views of the end customers. From the comments made the majority of participants felt that the proposed system's ability to remotely diagnose and check potential errors with systems such as

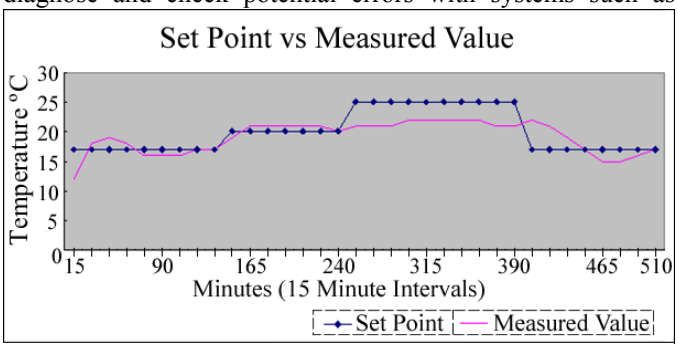

Fig. 9. Set Temperature and Measured Temperature

communal lighting was an attractive feature. Currently the HA spends approximately £100k on monitoring and maintaining communal lighting. The ability to detect when lighting has malfunctioned without physical human monitoring would make significant savings and incentivise the investment and adoption of such a system. Additionally, the flexible and extensive range of interfaces offered for the control and monitoring of devices connected to the home automation network was felt to be an attractive feature. It was felt that this feature would benefit people with mobility problems the most. One area for improvement that was highlighted by a participant and received widespread acceptance by the group was the suggestion to allow users to directly access the home automation system from a mobile phone without the need for a physical Internet connection to the home.

V. Conclusion

This paper has reviewed the existing state of home automation systems, and identified and discussed five areas that have hindered consumer adoption of such technologies. Briefly, the areas include: the complexity and expense of the architectures adopted by existing systems, the intrusiveness of the system installations, the lack of interoperability between different home automation technologies, and the lack of interoperability between systems developed by different manufacturers that utilise the same technology. Interface inflexibility and the inconsistent approaches adopted towards security and safety are also problems. A novel architecture for a home automation system is proposed and implemented, using the relatively new communication technology ZigBee. The use of ZigBee communications technology helps lower the expense of the system and the intrusiveness of the respective system installation. The incorporation of the virtual home concept coordinates the systems security and safety efforts in a clear and consistent manor. The inclusion of a

home gateway helps overcome the problems of network interoperability. The home gateway in our implementation provides interoperability between the local ZigBee and Wi-Fi networks and the Internet. Moreover the home gateway offers the potential to be easily extended to include interoperability for other communication standards. Furthermore, the home gateway unifies the interface offered by the system across the different networks and devices used to access the system. The feasibility and appropriateness of the proposed architecture and technologies in the creation of a low cost, flexible and secure system has been successfully evaluated both through experimentation and user trials. Experimentation has highlighted the stability of the novel architecture adopted, including the minimal impact of the inclusion of the virtual home on system's performance. The potential for successful co-existence and interoperability of Wi-Fi and ZigBee has been practically proven with implementation with a real home automation system. Focus group sessions have shown a positive attitude towards the developed system and significant support for the diverse modes of control, monitoring, and integration with existing home networks such as Wi-Fi.

ACKNOWLEDGMENT

The authors wish to thank colleagues from the network and control research group at Loughborough University for their continued support and feedback.

REFERENCES

[1] K. Bromley, M. Perry, and G. Webb. "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*, vol. 50, no. 2, pp. 498-504, 2004.

[3] N. Sriskanthan, F. Tan and A. Karande, "Bluetooth based home automation system", *Microprocessors and Microsystems*, Vol. 26, no. 6, pp. 281-289, 2002.

[4] H. Ardam and I. Coskun, "A remote controller for home and office appliances by telephone", *IEEE Transactions on Consumer Electronics*, vol. 44, no. 4, pp. 1291-1297, 1998.

[5] T. Baudel and M. Beaudouin-Lafon, "Charade: remote control of objects using free-hand gestures", *Communications of the ACM*, vol. 36, no. 7, pp. 28-35, 1993.

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

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

[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*, pp. 1517-1520, 2006.

[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*, pp. 1583-1586, 2007.

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

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

Khusvinder Gill is a PhD student in the Computer Science Department at Loughborough University. His research interests include security of remote communications, and wireless sensor networks. He is a student member of the IEEE. He received his B.Sc. degree from Loughborough University, UK in 2006.

Shuang-Hua Yang, Professor of Networks and Control, is the director of the Networks and Control Research Group in the Computer Science Department at Loughborough University. He is also an overseas professor in Central China Normal University and a guest professor in Huazhong University of Science and Technology, Petroleum University China, and Liaoning University of Petroleum and Chemical Technology. His research interests include wireless sensor networks, networked control, safety critical systems, and real time software maintenance. He is a fellow of the Institute of Measurement & Control (FInstMC), a senior member of IEEE (SMIEEE), and a Chartered Engineer (CEng) in the UK. He is an associate editor of the nternational Journal of Systems Science, and the International Journal of Automation and Computing. He is also serving as a member of the editorial advisory board for the International Journal of Information and Computer Security, Journal of Measurement and Control, International Journal of Advanced Mechatronic Systems, and International Journal of Process System Engineering. Professor Yang received his B.Sc. degree in instrument and automation, M.Sc. degrees in process control from Petroleum University China in 1983 and 1986 respectively, and his Ph.D. degree in intelligent systems from Zhejiang University in 1991.

Fang Yao is a PhD student in the Computer Science Department at Loughborough University. His research interests include interference of wireless networks and routing protocols for wireless sensor networks. He received his B.Sc. degree from Tianjin Science and Technology University, China in 2003 and his M.Sc. degree from Loughborough University, UK in 2005.

Xin Lu is a PhD student in the Computer Science Department at Loughborough University. His research interests include energy harvesting devices for ZigBee electronics. He received his B.Sc. degree from Beijing Institute of Technology, China in 2004 and his M.Sc. degree from Loughborough University, UK in 2005.