

We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900

Open access books available

186,000

International authors and editors

200M

Downloads

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.

For more information visit www.intechopen.com



Integrated Wireless Technologies for Smart Homes Applications

Mahmoud A. Al-Qutayri and Jeedella S. Jeedella

*Khalifa University of Science, Technology, and Research
United Arab Emirates*

1. Introduction

Due to the rapid advances in wireless communication and information technologies it is now possible to embed various levels of smartness in the home. These smart homes are ones that can interact intelligently with their inhibitors to provide comfort and safe living. This interaction may range from simple control of ambient temperature to context-aware and mobile agent based services. An example of that is delivery of particular information content based on the smart home inhibitor location inside the home and the activities that he or she is engaged with.

Wireless networks and sensors are seen to play an increasingly important role as key enablers in emerging pervasive computing technologies that are required for the realization of smart homes. The wide spread of wireless networks in our daily life is enabled by the communication standards such as WiFi, Bluetooth, Zigbee, RFID, and cellular technologies. A combination of these standards is envisaged to be used to construct the smart home. Effectively all wireless technologies that can support some form of remote data transfer, sensing and control are candidates for inclusion in the smart home portfolio.

A top level architecture of a smart home is illustrated in Fig. 1 (Al-Qutayri & Jeedella, 2010). It includes a server/gateway/router that can be used as the central point of connectivity for devices within the home as well as allowing connectivity to the outside world. The setup also includes smart sensors as well as appliances that have either wired or wireless connectivity. Communicating with the smart home from the outside can be done using one or a combination of the following external networks such as phone lines, xDSL lines, cable TV, GSM and power line networks.

Following this introduction, Section 2 reviews some of the major wireless communication technologies that can be used to realize a smart home. Section 3 describes briefly some of the smart sensors that can be used. Section 4 describes the major computing technologies, including ubiquitous and pervasive, context-aware, and agents computing which introduce smartness aspects to the home. Section 5 details some of the application that can be realized with smart homes. Section 6 describes the design and implementation of some smart home systems. In particular, the end-to-end realization of a secure system that enables monitoring and control of various devices with multiple levels of settings is described and the results

achieved are presented. Then Section 7 presents some conclusions and possible future directions in the area of smart homes.

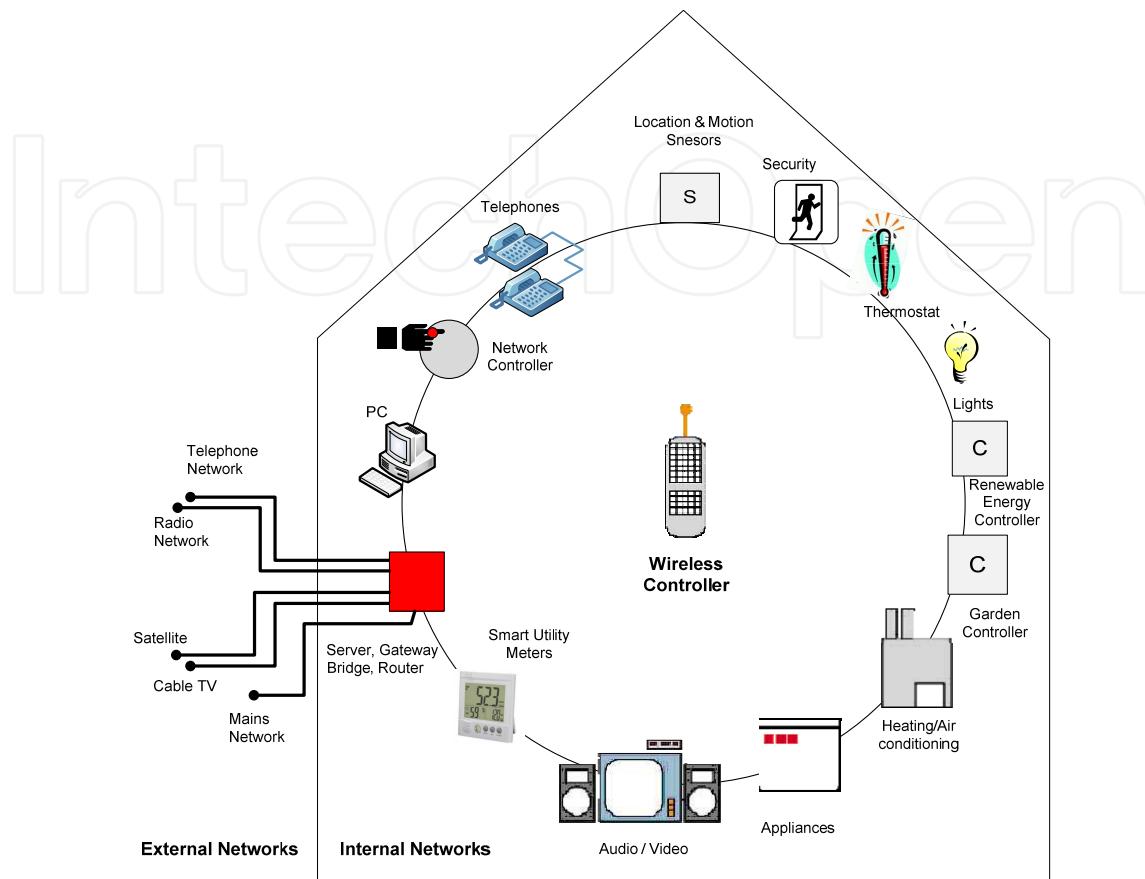


Fig. 1. Top Level Architecture of a Smart home

2. Wireless Technologies

The wireless technology standards are everywhere. Bluetooth, Zigbee, RFID, WiFi, and cellular technologies are the most well known standards. A combination of these standards is envisaged to be used to construct the smart home. Effectively all wireless technologies that can support some form of remote data transfer, sensing and control are candidates for inclusion in the smart home portfolio. This section discusses some of these key wireless technologies.

2.1 Bluetooth

Bluetooth is a universal radio interface that enables various electronic devices, including mobile phones, sensors... etc, to communicate wirelessly through a short range radio connection (Thompson et al., 2008). The introduction of this technology eliminated the requirement for wired connections, eased the connectivity process between devices, and enabled the formation of personal networks. The pervasiveness of Bluetooth enabled electronic devices is enabling ubiquitous connectivity and hence allowing the development of many applications.

A Bluetooth device uses a license-free frequency band at 2.45 GHz. This band is also known as the Industrial-Scientific-Medical (ISM) band and has a range of 2.4 GHz to 2.4835 GHz. As this band is a free one, and hence gets used by other applications such as cordless phones, Bluetooth radio transceivers use frequency-hopping spread-spectrum to avoid interference. Depending on the Bluetooth class, the communication range varies from 1 meter for Class 3 to 100 meters for Class 1. The most common range is 10 meters for Class 2. The data rate of devices in a Bluetooth network varies from 1 Mbps to 24 Mbps. In a Bluetooth network, there are two types of devices: a slave and a master. Each Bluetooth device has the ability to be either a slave or a master or both at the same time. In general, a Bluetooth network consists of small subnets or piconets. A piconet is formed by two or more connected devices sharing the same channel. In every piconet, there is only one master and up to 7 slaves. The communication between the slaves goes all time through the master. When two or more piconets are connected they form a scatternet. The connection between piconets can be done by having a device in common. This device may be a slave in one piconet and a master in another piconet as shown in Fig. 2. The protocol stack of Bluetooth is depicted in Fig. 3 and the details of its functionality are given in (Labiod et al., 2007).

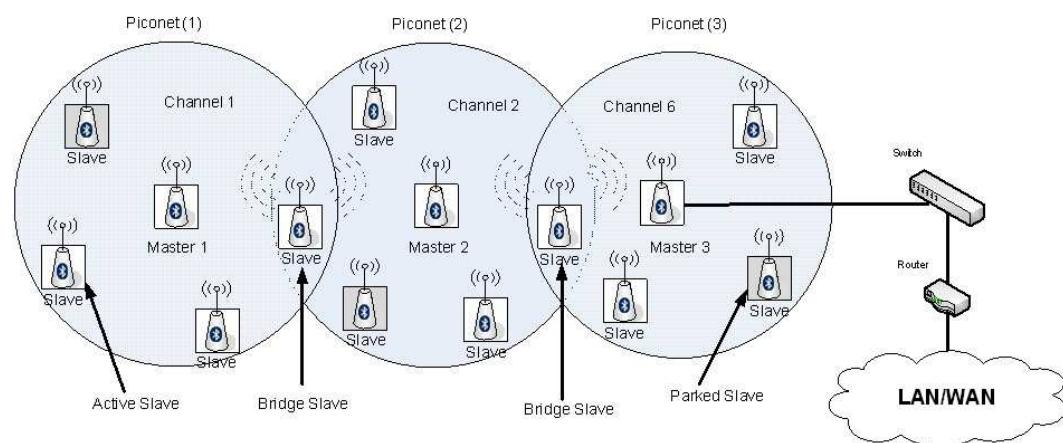


Fig. 2. An example of Bluetooth scatternet

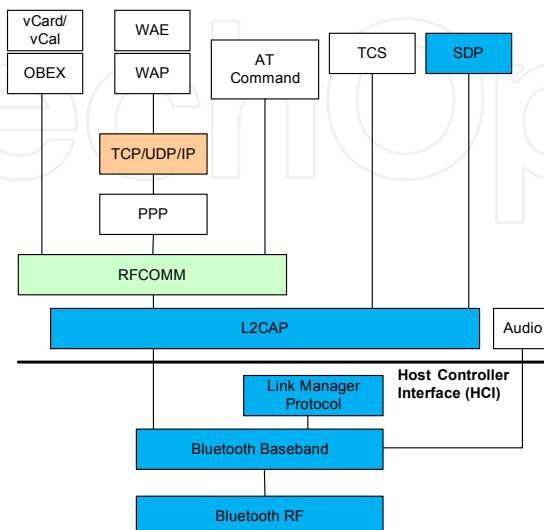


Fig. 3. General Bluetooth protocol stack

Smart homes can benefit from Bluetooth technology in a variety of ways. One possibility is to embed appliances with Bluetooth radio transceivers and use that technology to communicate with a home server that is accessible by the user. This enables monitoring and control operations to be conducted by the user. Another possible application is the establishments of Bluetooth enabled sensor networks that can track the well being of people with disabilities (Leopold et al., 2003).

The challenges that face the use of Bluetooth in a smart home environment are similar to those facing the technology in other environments. A primary concern of the use of Bluetooth is its security vulnerability. It has been shown that the security of Bluetooth devices can be compromised by adversaries. A number of solutions have been proposed in the literature to harden security and privacy of Bluetooth based communication (Carettoni et al., 2007).

2.2 ZigBee (IEEE 802.15.4)

IEEE 802.15.4 standard is a low cost low power wireless communication standard for Personal Area Network (PAN). The low cost makes it suitable for remote control and monitoring applications. The low power makes it suitable to operate on batteries for long life. It reduces the cost of hardware and consuming power by lowering its data rate. The specifications define only the lowest two layer of the OSI networking reference model: the physical and Media Access Control (MAC) layers. The data rate, operating frequency, and network size are defined by the standard. The achieved data rate between IEEE 802.15.4 compliant devices varies from 250 kbit/s to 20kb/s depending on the distance between devices and the transmission power. These devices may operate in one of the following three RF bands: 868 MHz (Europe), 915 MHz (North America), and 2400 MHz (worldwide). The 2.4 GMhz band is used more often than the other bands since it is available worldwide for unlicensed operation. In addition to that, the performance of products developed for that band is better when compared to the other bands with respect to data rate. The size of the network is not limited by the standard. However, network address are stored and sent using 16 bit or 64 bit numbers, which limits the network size to 2^{64} devices.

IEEE 802.15.4 standard defines Star, Cluster Tree and Mesh networks as possible topologies for the wireless network as shown

Fig. 4. However, mesh networks enable high levels of reliability and longer coverage range by providing more than one path through the network for any wireless link. Note that in any ZigBee network there are three types of ZigBee devices (Gislason, 2008):

- **PAN coordinator:** There is only one coordinator in a network that is responsible for starting the network, binding together devices. Also it routes data between different devices. It is a Full Function Device (FFD) and it is usually mains powered device.
- **A router:** It cannot start the network however it scans a network to join it. Once it is in the network it can route data between Reduced Function Devices (RFD). It is a FFD and it is usually mains powered device.
- **An end device:** It cannot start a network however it scans a network to join it. It can be either a RFD or FFD and it is usually battery powered device.

The protocol stack of Zigbee defines only some functionality in layers on top of the physical and MAC layers which are defined in the IEEE 802.15.4 standard. It provides the set of programming tools for the intended market. Furthermore, ZigBee technology defines a set of applications profiles to facilitate the development and deployment of ZigBee devices from different manufacturers as shown in Fig. 5 (Gislason, 2008).

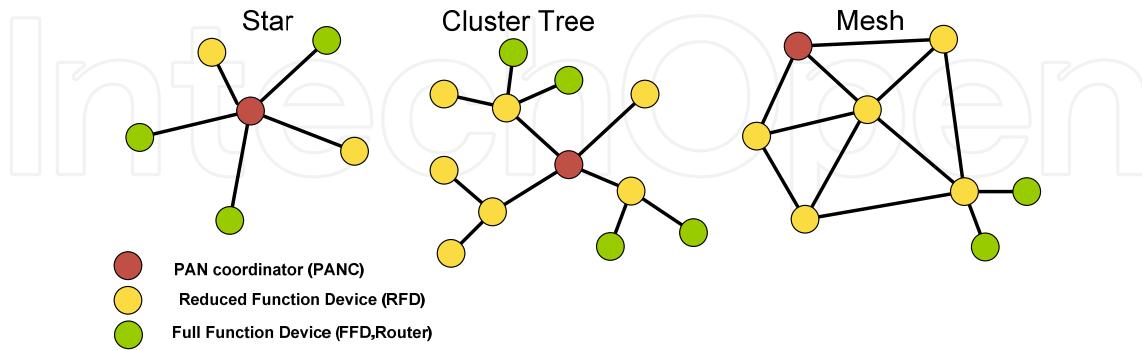


Fig. 4. Possible ZigBee networking topologies

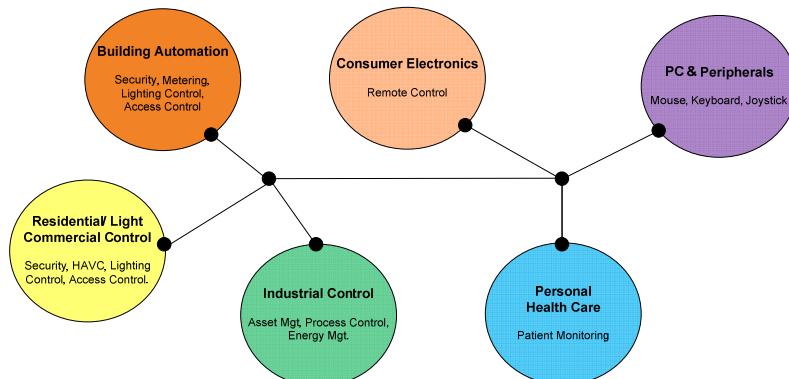


Fig. 5. ZigBee Applications Profiles

2.3 RFID

Radio Frequency Identification (RFID) describes a system that transmits the identity of an object wirelessly using radio waves (Want, 2006). It defines a RFID tag holding information about the object carrying the tag and a RFID reader. The RFID tag transmits signals containing its data when it is scanned by the reader. The RFID tag can be either active or passive where an active tag contains a battery and the passive tag does not have a battery. The passive tag uses the reader's magnetic field and converts it to DC voltage to power up its circuitry. Consequently, the passive tags are cheaper and have lower range when compared to active tags.

RFID systems can be categorized based on the used frequency ranges. The Low-Frequency (LF) systems use signals with a frequency between 124-135KHz. The High-Frequency (HF) systems use a 13.56MHz and the Ultra-High-Frequency (UHF) systems use a frequency between 860-960MHz. In general, the LF RFID systems have short reading ranges and lower system costs. In case longer reading range is required, HF RFID systems can be used however their cost is higher.

RFID systems can be used in smart homes where every single object can be connected to the Home Area Network (HAN) through a virtual wireless address and unique identifier (Darianian and Michael, 2008). This can be used to keep an updated database holding information about objects' locations. Accordingly, the smart home can be asked to provide information about a specific object that you are looking for such as your car's key or your remote control. Furthermore, RFID system can be used to track smart home occupants, where a number of studies have been reported in the literature that use RFID concept to track smart home occupants (Yamazaki, 2007). By the attachment of a RFID tag to each smart home user and the deployment of RFID readers at different places in the home, the location of each user can be identified. This information can be used to adapt services in the smart home based on each user preferences.

One of the problems of using RFID tags to track people in smart homes is that the readability of RFID tags is difficult near water or a sheet of metal. The human body consists primarily of liquid which makes it difficult to scan a RFID tag attached to human body (Juels, 2006). However, researchers are looking for new ways to improve the readability of RFID tags in these difficult environments.

2.4 GSM/GPRS

The GSM (Global System Mobile) is the technology that generated a revolution in the field of mobile communications. New generations of GSM were introduced over the past decade that includes GPRS, UMTS... etc in order to improve the transmission rates, and offer new types of services (Brand and Aghvami, 2002). The GSM which is also known as the cellular network is based on frequency reuse. To that effect a particular geographical area gets divided into cells. The size of the cell is normally dependent on the local traffic distribution and demand. A high level architectural view of GSM/GPRS is shown in Fig. 6.

The mobile wireless system such as GSM/GPRS is used to deliver both voice and data communications. One of the cost effective services that is delivered by the network and can be used for smart homes applications is the SMS (short message service). The SMS is a text message whose content can be processed using an appropriate program in order to execute commands for monitoring and control operations (Al-Qutayri et al., 2008). Such programs are normally written using Java language. The ability to use the GSM network basically means that remote access and control to a smart home is possible.

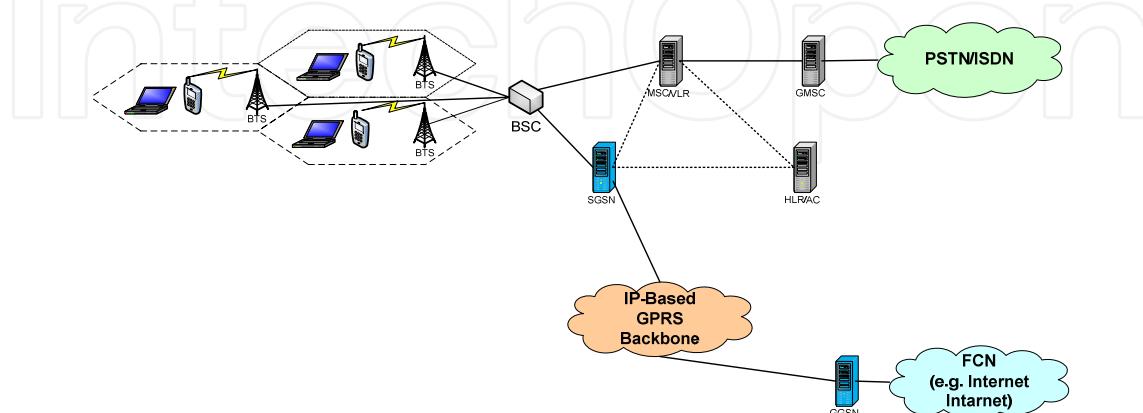


Fig. 6. GSM-GPRS System Architecture

2.5 WiFi (IEEE 802.11)

Wireless Fidelity (WiFi) is a common term that refers to the IEEE 802.11 wireless communication standard for wireless local area networks (WLAN) in the 2.4, 3.6 and 5 GHz frequency bands. Network users, when using WiFi technology, can move around without restriction and access the network from almost anywhere. Also it can provide a cost-effective network setup for hard-to-wire locations such as old buildings. Two types of devices are considered in the WiFi standard: an access point (AP) and a wireless device which could be a laptop equipped with a wireless network interface. The main function of an AP is to bridge the information between the fixed wired network and the wireless network. An AP can support up to 30 wireless devices and can cover a range of 33–50 meters indoors and up to 100 meters outdoors. The wireless devices can be possibly connected together using infrastructure topology or an ad hoc mode topology.

The infrastructure topology is sometime called an AP topology since the wireless network consists of at least an AP and a set of wireless devices. In this topology, the system is divided into basic cells, where each cell is controlled by an AP. To extend the coverage area, multiple basic cells can be used as shown in Fig. 7.

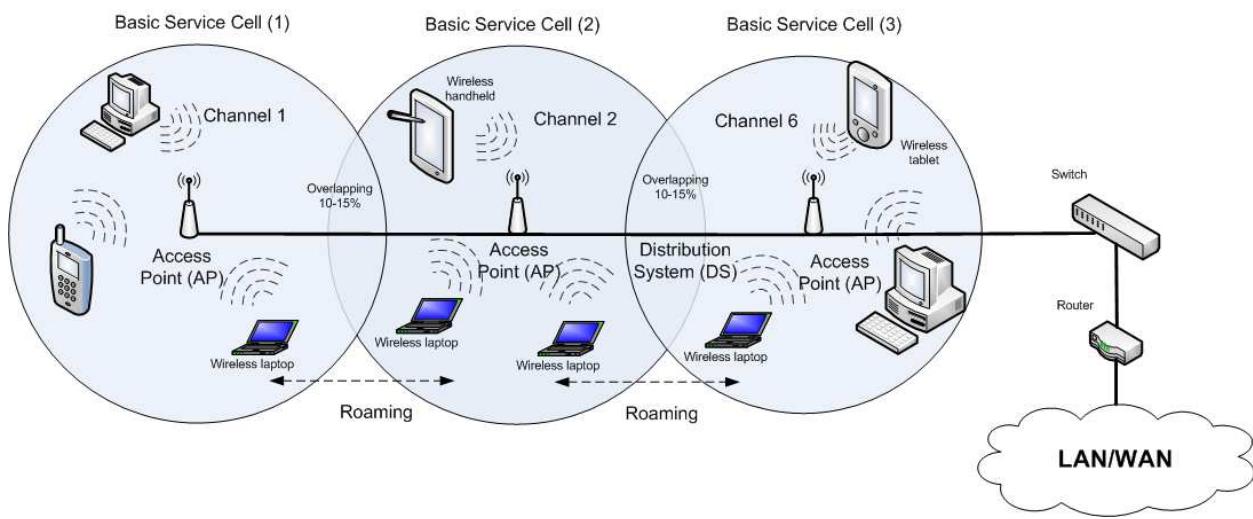


Fig. 7. A typical WLAN

In general, wireless networks should be able to reach fixed Local Area Network (LAN) services such as file servers, printers and Internet access. This is achieved by the distribution system (DS) connecting the different APs together. The connection between the APs can be done using either a cable connecting them together or using a wireless connection. The data transfer between wireless devices within a basic cell and the distribution system occur via an AP. The distribution system is responsible for transferring the data packets between various cells within the wireless network. It is also responsible for address mapping and internetworking functions. To cover an extended area, basic cells may sometimes partially overlap as shown in Fig. 7. On the other hand, the ad hoc topology represents a group of WiFi devices that have the ability to dynamically form connections with each other to create a network. This ad-hoc network does not require a connection to either an AP or to fixed network. It can grow, shrink and fragment without having to make any requests to a central authority. It is useful for setting up a wireless network quickly and easily.

IEEE 802.11 standard is similar to IEEE 802 standard that deals with LANs and metropolitan area networks (MAN). It focuses on the two lowest sub-layers of the Open System Interconnection (OSI) networking reference model. Namely, the physical layer (PHY) and a data link layer containing the MAC sublayer and the LLC and more details can be found in (Labiod et al., 2007).

The IEEE 802.11 standard has evolved over the past years where two types of systems were defined. Those operate in the band of 2.4 GHz such as IEEE 802.11b/g and those operate in the band of 5 GHz such as IEEE 802.11n. Since IEEE 802.11n standard supports high data rate approximately five times higher than the previous standard, it is expected that it will be used in consumer electronics applications, especially for streaming video in smart homes. The video signal can be displayed on the suitable display system based on the smart home inhibitors locations and preferences. Some companies such as Philips are demonstrating wireless video streaming for home entertainment system using this wireless technology. Since the existing 802.11a/b/g standards were created to serve the PC applications domain, they have substantial limitations for real-time and high bandwidth requirements from consumer electronics applications. Even though the 802.11g has a maximum data rate of 54Mb/s, in practice it achieves 20Mb/s with difficulty, especially when the signal has to penetrate walls. With the improvements in codec technologies such as MPEG4, H.264 and WMV9 the required bandwidth to stream video is reduced. However, other requirements are driving to increase the required streaming bandwidth such as high definition video, the Voice over Internet Protocol (VoIP), networked audio devices, etc.

3. Smart Sensors

A sensor is a device that converts a physical or biological quantity into electrical quantity. The measured electrical quantity should be calibrated, converted to digital format and sent to the microcontroller for further processing and control. Most of the sensors, irrespective of their types, can be included as part of a ubiquitous embedded system that has communication capabilities and backend connectivity. These types of sensors are called sometimes smart sensors. These enable software development and data analysis using embedded processing capabilities as well as sending remote processing by a computing system located at some other location. Examples of these types of integrated sensors include Particle Computer (Decker et al., 2005), Berkeley MOTES (Estrin, 2002)... etc.

The intelligent homes of the future are expected to be embedded with a network of heterogeneous low power wireless smart sensors that monitor the vast set of parameters necessary for building ambient intelligence. The smart sensors will have to function in an autonomous manner and maintain the privacy of the home inhabitants. The tasks that the network of sensors and actuators may perform in a smart environment can range from a simple one such as turning on and off the garden sprinkler system at regular intervals to supporting elderly people at home (Dengler et al., 2007).

The set of sensors and actuators that will be needed can be broadly classified as conventional and non-conventional types with reference to present state of sensors technology. The conventional sensors type includes temperature, humidity, light, motion and smoke detectors (Augusto and Nugent, 2006). A light sensor for example can be used to automatically differentiate between day light and nightfall and hence open or close the curtains using an appropriate actuator. Temperature and humidity sensors can be used in

conjunction with the heating and air-conditioning system to optimise the home atmosphere and give the same level of comfort throughout the home.

Non-conventional sensors types include location, posture, heartbeat and biosensors. These types of sensors enable monitoring various conditions including health oriented ones for elderly persons living on their own. The biosensors such as finger print, face and iris recognition can be used to grant physical access to the home. Accordingly, the house environment will be adapted to his or her needs.

In order to build the ambient intelligent environment for the smart home inhibitors different types of sensors should be deployed in the house. By the fusion of the data streams from different sensors the whereabouts of smart home users can be inferred. For example, the data coming from audiovisual sensors can be combined with the RFID tracking system to infer the location of smart home owner and his activity. In some cases the emotion of a smart home owner can be inferred using face recognition and the analysis of his or her voice.

4. Computing Technologies

The sensory information gathered by the distributed sensors in a smart environment needs to be processed in order to perform the required actions. These actions can occupy a wide spectrum that extends from simply toggling a device between on and off states to sophisticated personalized decisions. The level of sophistication and intelligence that needs to be used in interacting with devices depends on the complexity of the device and the type and level of functions it can perform. An air conditioning system for example has a reasonable level of complexity. For such a system, once it gets switched on the desired temperature and air flow levels need to be set.

Interacting with individual devices and appliances can introduce a basic level of intelligence to the home environment. However, the level of intelligence can be greatly enhanced once devices, be it simple sensors or complex appliances, can exchange information and effectively share the decision making process to offer a certain type of service to the occupant of an intelligent environment. This section reviews the major computing technologies that have been proposed in the literature to realize smart homes or more generally smart environments.

4.1 Ubiquitous and Pervasive Computing

Advances in integrated circuits design and miniaturization processes are resulting in computing devices with ever shrinking sizes. At present, such devices are being commercially produced using an approximately thirty nanometer process. This reduction in the computing devices size and cost has effectively led in recent years to the realization of the ubiquitous computing world envisaged by Mark Weizer (Weizer 1991). In that vision Weizer stated that "the most profound technologies are those that disappear, they weave themselves into the fabric of everyday life until they are indistinguishable from it."

In the ubiquitous world of computing, which was subsequently named by IBM as pervasive computing (Satyanarayanan, 2001, Garlan, 2002), the technology becomes unobtrusive as computers get pushed into the background and the focus shifts to the information and the people using the system. The major aspects of pervasive computing systems include (Haryanto, 2005):

- Computing devices are scattered everywhere in the environment or space of interest
- The devices can be interconnected and interact with each other
- The devices can work autonomously without active attention from the user
- Each device tends to be dedicated for a special task
- The devices integrate into the background in a seamless manner that makes them effectively invisible to the user.

Pervasive computing plays a major role along with other technologies, particularly computing ones, in supporting the realization of smart homes as well as the more general ambiance intelligence (Ma et al., 2005; Mann, 2005; Augusto, 2007). To that extent many researcher have attempted to use pervasive computing to introduce smartness to some aspect of the home while other built a complete smart home prototype with extensive devices and networking. The articles by (Al-Qutayri et al., 2008; Choi et al., 2005; Roduner et al, 2007) describe smart home systems in which some of the appliances are fitted with wireless sensors that enable remote monitoring and controlling of those devices. Other significant research work that resulted in smart home structures with extensive pervasive computing infrastructure include AwareHome (GATECH) (Kientz et al., 2008) and Adaptive House (University of Colorado) (Mozer, 2005) as well as other projects (Helal et al., 2005).

4.2 Context-Aware Computing

Context-aware computing and pervasive computing go hand in hand and complement each other. Having pervasive computing environment provides the infrastructure that supports advancements in context-aware computing. Conversely, the enhanced capabilities of context-aware computing are placing demand on building responsive pervasive computing environments (Baldauf, 2007; Dargie, 2009). Computing systems that are context-aware have smart or cognitive characteristics that enable them to adapt to changes in the environment and user requirements (Schaefer, 2006). This dynamic adaptation provides the system with the autonomy needed to take decisions without the user direct intervention and hence make computing an unobtrusive task that blends into the fabric of the environment. Extensive research has been conducted to date to enable the design of context-aware computing system. All such systems tend to have architecture with a middleware layer that interfaces the application to the system software. The middleware supports integration between disparate products and platforms while maintaining the integrity, reliability and robustness of the overall solution.

The application of context-aware computing in the field of smart homes continues to be of interest to many researchers. It creates the required smart features that allow flexible interaction between the user and the environment. The article by (Oh and Woo, 2005) proposes a unified ubiHome application service model that provides personalized environment to each user. Application of context-awareness in the control of smart home appliances is described in (Choi et al., 2005). The system utilizes six parameters for learning and predicting the user's preference: the pulse, the body temperature, the facial expression, the room temperature, the time and the location. The application of context-aware computing in a smart home environment to support independent living and provide health care services is the subject of extensive research given the importance of this field (Haryanto, 2005; Cook, 2006; Bricon-Souf and Newman, 2007).

4.3 Agent Based Computing

Agent based computing is a powerful technology for the development of complex software systems. It draws on knowledge from different areas including software engineering, artificial intelligence, robotic and distributed computing. An agent is characterized by autonomy, social ability, reactivity, and pro-activeness. These characteristics enable the development of proactive and intelligent applications that can interact with one another (Zambonelli et al., 2000).

A multi-agent system can be considered an ensemble of autonomous agents. The agents work independently from each other. However, as each agent tries to achieve its task it typically needs to interact with other agents as well as the surrounding environment in order to obtain information and/or services that it does not have or coordinate its activities in such a way to achieve its goals.

Multi-agent systems tend to be static and hence execute on the system on which they are running. However, by their very nature mobile agents are programs that can autonomously move from one computing machine in a network to another. The dynamic movement ability of a mobile agent enables it to move to a computing system on the network that contains the object it wants to interact with (Ilarri et al., 2008).

Agent based computing technology, be it static or mobile, lends itself well to smart homes research. The article by (Cook et al., 2003) describes the "MavHome" project whose goal is to create a home that acts as intelligent agent. The study by (Velasco et al., 2005) proposes a multi-agent based architecture which enables multimedia contents to follow the user movements throughout the smart home environment. The article by (Marsa-Maestre et al., 2008) proposes a service oriented architecture implementation based on mobile agent systems. This is then used for service personalization using mobile agents that follow the system users as they move from one location to another within a smart space.

5. Applications

The opportunities that are primarily envisaged in a home that can be classified as smart are numerous and can be classified as services or monitoring and control. The sub-sections below explore some of those smart home applications.

5.1 Appliance monitoring and control

By exploiting sensors in smart home appliances and connecting them in smart home network, they can operate in a much more sophisticated and intelligent ways. They could be controlled easily from any place in the house by switching them ON or OFF from rooms in the house (Balasubramanian, 2008). The remote control and monitoring of these appliances can be performed remotely via the Internet or GSM mobile phones. Furthermore, some machine can act smartly by reporting their problems to the service company. For example, the refrigerator might report a cooling problem to the maintenance company; this is much needed in case smart home inhibitors are in holiday.

Furthermore, by exploiting electronic tags in food's packages, clothes, dishes, etc smart home appliance can operate in intelligent ways. White goods companies such as Merloni Elettrodomestici, are introducing appliances that communicates with objects using RFID (Merloni, 2003). Washing machine can scan the load in it to adjust the wash cycle to be suitable for the fabrics used. The refrigerator also might warn the user about the expiry

dates of some of the products inside it. In addition to that it can send automatically a shopping list to some home delivery services.

5.2 Safety and Security

Safety and security are important aspects of human life. Therefore, incorporating safety issues in smart home is an important requirement for most of the smart home occupants.

A number of products are available in the market that implements some of smart home concepts to deliver various aspects of safety, alarm and security. It is expected that the number of these products will grow in the nearby future. The general architecture of these systems consists of an appropriate set of interconnected sensors that monitors specific conditions or situations and communicates them to a local server which then transmits them to the concerned parties. These sensors could include smoke detectors, water leakage detectors, intruder detectors, power outage detectors, etc. In case of an alarm, both the home owner and the security company will be informed about the existence of the alarm. Having a smart system installed in the home, it will transmit detailed information specifying the exact location and the cause of the alarm. Furthermore, the system will allow the user to control some utilities of his home remotely. For example, in case that the home owner is expecting a home delivery and he cannot be in his house, the main gate can be opened to allow the postman to deliver the package. He can also close the doors and the main gate after the postman leaves the house. Via the Internet or his mobile phone, he could also switch on or off the heating/cooling system for a specific part of his home. In case the smart home occupants are in holiday, they could program the system to simulate the owner presence inside the home by switching on the home lights and switching them off at regular times.

5.3 Tele-health Care

The cost of providing health care particularly in developed countries continues to rise. This is attributed to many factors that include an increase in peoples' life expectancy coupled with a decline in birth rates which are resulting in an aging population. Add to this is the general increase in the salaries of health professionals and the cost of medication and diagnostic equipment. All these costs are putting a huge strain on the health budgets of the various government departments and agencies.

This means that the provisions for long-term health care within hospitals and clinics are severely restricted. However, those patients who may need long-term health care, such as elderly persons with heart problems, may not have people to look after them once they go home or they may simply prefer to live within their own normal environment for psychological, social or other similar reasons. The availability of a smart living environment, in the form of a smart home, will help alleviate some aspects of this problem and hence release resources that would otherwise go to long-term health support of an individual patient to other patients, enable early diagnosis of chronic health conditions, and make clinical visits more efficient due to the availability of objective information prior to the such visits (Botsis and Hartvigsen, 2008; Friedewald et al., 2005).

A number of studies have been reported in the literature that applies the smart home concept to deliver various aspects of telemedicine or tele-health (Liu et al., 2007). The general architecture of a system that delivers the required health-care services would consist

of an appropriate set of sensors that monitor specific medical conditions or situations and communicates it to a local server and then transmits it to the entity assigned to look after the patient. Many of the proposed telehealth system use multi-agent technology to arrive at an intelligent decision regarding the health state of the person being monitored (Rammal et al., 2008). The system described in (Tabar et al., 2006) uses a set of cameras to form a distributed vision processing setup. Analysis of the occupant's posture is then used to detect if the person suffered a fall. The assessment is based on a set of rules and once a fall situation is asserted an alarm gets sent to a call centre. A voice link can then be established between the occupant and the care centre.

5.4 Energy Metering

Environmental awareness is a major trend that has impacts on all businesses especially in the developed countries. The driving forces for this interest are rising energy costs and reducing greenhouse gas emissions. These factors are pushing to reduce energy usage and or optimize its usage in homes and commercial building through smart energy products. In general, energy cost can be one fifth of building's operating costs, with lighting and heating or cooling using most of it in both residential and commercial buildings. Consequently, they are the main targets for energy reduction through smart energy usage. Utility companies are interested in smart ways to control the rising energy usage with minimum costs. They are reluctant to implement and deploy both load control and time-of-use (TOU) rates to help managing the load during peak demands. They would like to have the possibility, through load control, turn off some non-critical customer loads, such as HVAC, for short period of time, during peak demands. Also, they can use demand response mechanism where customers are informed about TOU rates. This will encourage the customers to manage their energy usage efficiently. These actions will help utility companies in reducing their peak demands and users to reduce their utility bills.

The use of smart electricity meters in smart homes will definitely be able to communicate with utility companies for the purpose of load control and demand response (Venables, 2007). Through Home Area Network (HAN), smart meters can communicate and control other appliances in the smart home, such as the HVAC system. In addition to that the smart home owner can take voluntary actions during demand/response periods to reduce his/her home consumption by turning off appliances, lights, etc. Having the household appliances interconnected will facilitate load control and demand response. For example, a dishwasher can be given the command to delay its start time to a time that has lower utility rate.

5.5 Environmental Control

Heating and cooling a house is the major post in the houses' utility bill, therefore, they deserve special attention when designing smart homes. Choosing good isolation materials for constructing homes that are suitable for their environment is the foundation to reduce these costs. By the deployment of smart sensors inside and outside the house, the houses' energy consumption can be managed efficiently. By collecting information from the distributed sensors inside the house such as thermostats, humidity, airflow, etc and from sensors outside the house such as thermostats, humidity, sunshine, wind speed meter etc, these information can be processed to control HVAC units and blinds/shades/rollers/windows. For example, in case that a window is opened for a pre-specified period

while the HVAC unit was on for that specific room, a decision can be made to stop that unit or to alarm user about this inefficient use of energy. In addition to that, an advice can be given to the user to shut the curtains in the night when the temperature outside is much lower than the one inside the house while the heating system was on.

The renewable sources of energy available to smart homes depend on their geographical locations. For example, in locations where the sun shines most of the year, it is advisable to have solar panels installed on its roof. In other locations where you have windy climate, it is advisable to have wind turbines installed in garden (Balasubramanian, 2008). By monitoring the environmental conditions inside and outside the house and the current home load condition, decisions can be made how to use the generated electricity. In case that the house is connected to smart electricity grid, the extra electricity can be fed back to the grid.

5.6 Information Access

The smart home should respond to the inhibitor's needs and the change of these needs in unobtrusive and invisible way while remaining under the control of the users (Friedewald et al. 2005). By identifying the location of a person inside the house and by sensing his activity the environment can be adapted to suit his wishes. In case the person requires information it will be forwarded to the nearest display based on his location. Also his preferences and the accessed information should move with him when he changes his location. In case the smart home inhibitor was watching the news while he was shaving in the bath room, the same news channel will be displayed in the kitchen when he moved there to drink his coffee. In case the smart home inhibitor is reading a novel, the information related to novel could be retrieved from the Internet and displayed on the nearest display screen (Friedewald et al., 2005).

5.7 Smart Space for Kids

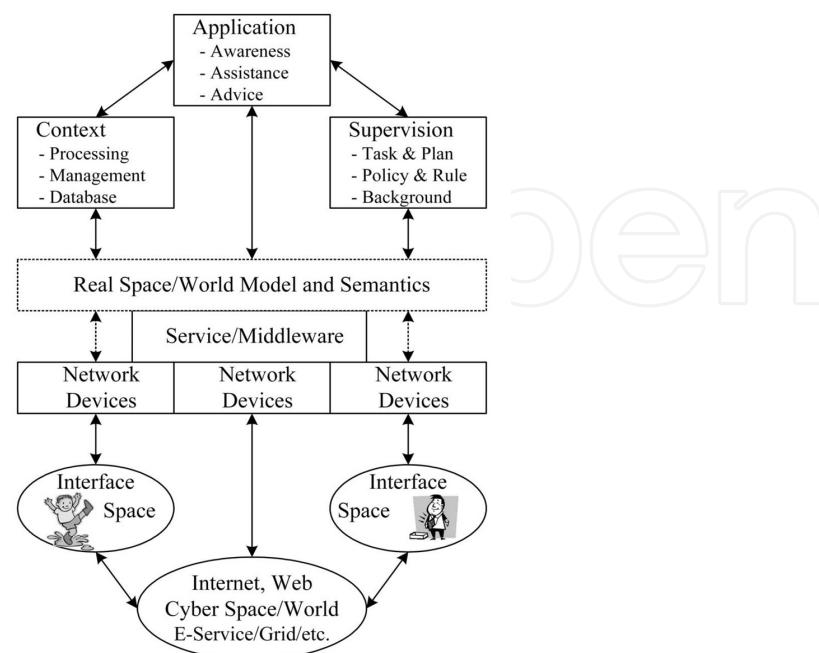


Fig. 8. System Architecture of UbicKids

The UbiKids system proposed by (Ma et al., 2005) aims at creating a smart hyperspace environment of ubiquitous care for kids. The system caters for both kids and parents. The main objectives of UbiKids are: (1) to develop a set of ubiquitous applications that help parents to take care of their kids through efficient, user friendly, reliable, secure and trustworthy services; (2) to study the social and psychological impact of ubiquitous kids care applications on the families; (3) to build a prototype smart hyperspace environment. The system architecture of UbiKids is illustrated in Fig. 8 (Ma et al., 2005).

6. Case Study

This section describes the architecture and design of a prototype smart home system that integrates a variety of wireless information and communication technologies with a variety of sensors and appliances. The prototype system enables an authorized user to monitor and control home devices equipped with a smart interface structure using a mobile phone. The system is embedded with authentication and verification mechanisms that provide secure end-to-end processing. The system is scalable through a flexible architecture that easily expands the portfolio of devices to be monitored and controlled. This system uses the mobile GSM/GPRS network for the external network. Where a mobile phone application using J2ME is designed to control and monitor various types of devices. It communicates with the home computer server which is connected wirelessly to the microcontrollers of the devices, being monitored or controlled, via a Bluetooth network. Although the Bluetooth technology used for the internal network has some limitations in terms of high cost and short range, and security concerns, its hardware size is small (Pooter, 2006). This technology can be replaced with the Zigbee technology since it is more suited for this type of application. Furthermore, it is cheaper, has better security and battery powered Zigbee devices require less power.

6.1 Smart Home Architecture

The architecture and the various technologies used in the design of the prototype system are described in Fig. 9. A comprehensive description of the system, its functionality, and services is given by (Al-Qutayri et al., 2010). The system consists of a Java-enabled mobile phone with a mobile application, a computer server with a Java application, a GSM modem connecting the server to the external network, a PIC microcontroller with a hardwired application connected to the devices, and Bluetooth adapters connecting the server and the microcontrollers to the internal Bluetooth network.

The system is connected to the external network using GSM network. A mobile phone communicates with the home server using Short Message Service (SMS). The mobile application which is written using Java 2 Micro Edition (J2ME) technology includes a friendly menu-driven Graphic User Interface (GUI). The GUI is used by the user to input all information to the system. It has a list to display the main system services, buttons to turn on, turn off or monitor a device, text fields to get the configuration information, and commands to move from menu to sub-menus. The system uses the Bluetooth P-to-P (Point-to-Point) protocol as the wireless internal network to connect the home devices' microcontrollers to the home server.

The home server is the core of the smart home system. It is connected to the GSM network via a GSM modem to send/receive SMS messages to/from the mobile phone. It also

connects to home devices through the Bluetooth connection. Fig. 10 show the software architecture of the home server. The server application is written using the Java programming language.

Smartness is introduced to the devices in the prototype system by including a PIC microcontroller in each device in order to monitor and/or control it at the hardware level. It is also connected to a Bluetooth adapter to establish the Bluetooth P-to-P connection with the home server. An application program, which is written in C and downloaded to the PIC microcontroller, receives commands from the server, interprets them and sends the information to the devices. It also reads the status of devices and sends it to the server. The presence of the microcontrollers enables the introduction of smart control and monitoring functionality to the home devices. The level and sophistication of the smartness depends on the functions the device can perform.

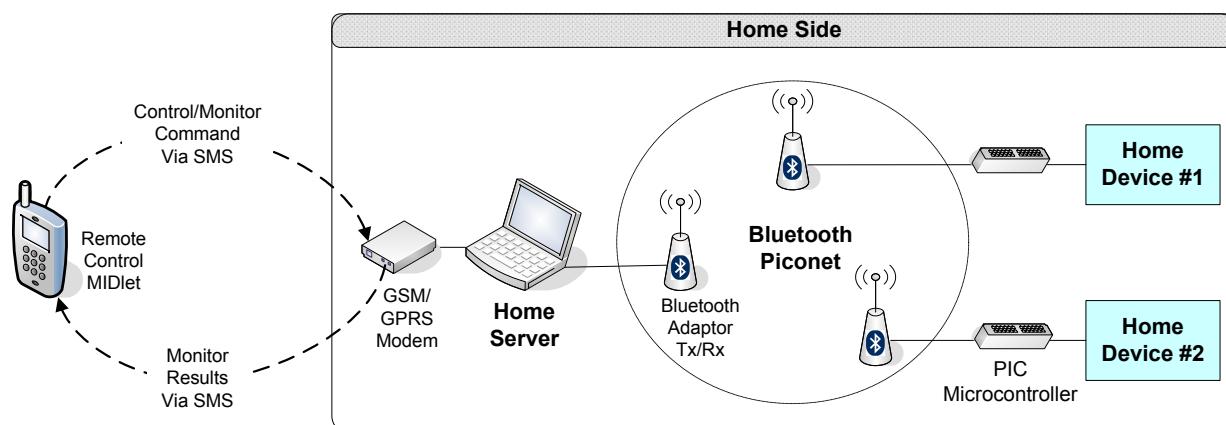


Fig. 9. Smart Home System Architecture and Technologies

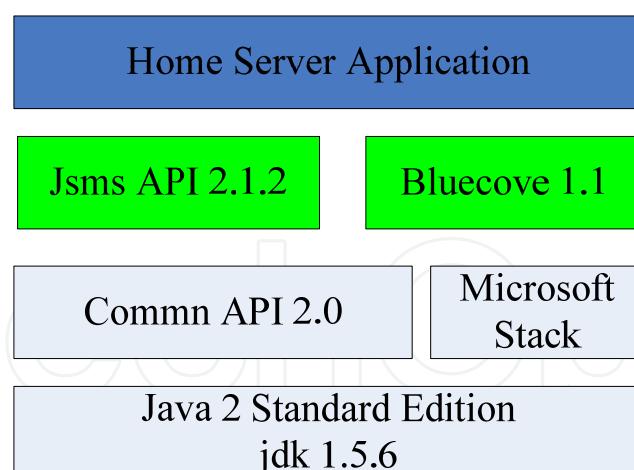


Fig. 10. Software Architecture of Home Server

6.2 System Services

The system provides three main services: monitor the settings of home devices and appliances, control the settings of home devices, and get status of devices periodically. Some additional minor services provided by the system are events and problems logging and notification of connections problems. Monitoring home devices consists of checking the setting of the devices. The monitoring command is sent via an SMS as illustrated in Fig. 11.

Controlling a home device includes changing the setting of the device by sending a command via an SMS containing the name of the device to be controlled and the control command as illustrated in Fig. 12. The control commands currently implemented are: turn off device, turn on device to a certain level, and change the level of device.

Instead of running the J2ME application in the mobile phone every time to get the device status, an SMS message is generated by the home server that periodically shows all devices status. The SMS message is sent according to a pre-programmed time interval. This time interval can be changed by the mobile phone application by sending a special command to the server.

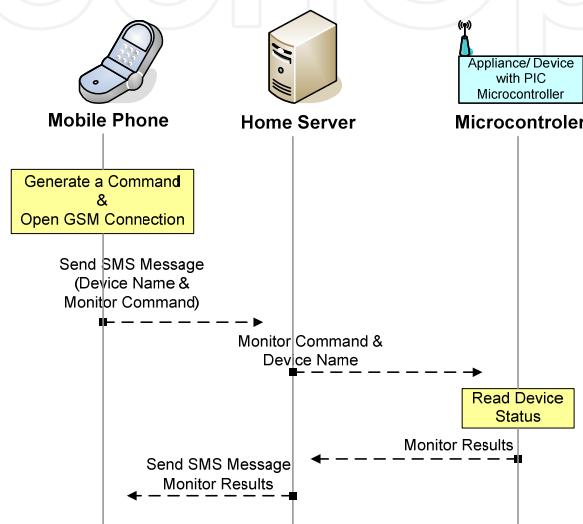


Fig. 11. Home Device Monitoring Process

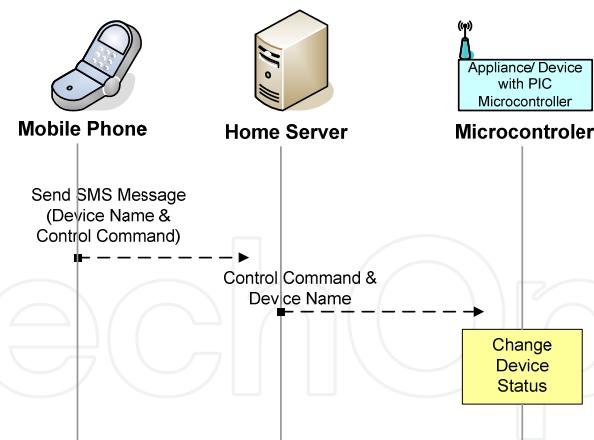


Fig. 12. Home Device Controlling Process

6.2 System Software Application Design

The system that enables monitoring and control of home appliances consists of three major software applications: mobile or hand-set, home server, and appliance controller.

The data flow diagram of the mobile application is depicted in Fig. 13. This application gets/sends data from/to two terminals. First time, the user configures the mobile application with two parameters: Home Server SIM card Number and Periodic time for SMS

notification. The Home Server connects to the GSM network using GSM modem and that has a SIM card Number.

The user controls the mobile application using the following set of commands:

- Set Level: select a level for a specific device
- Back and Select: enable the user to move from one category to another (Monitor a Device, Control a Device, and Configuration)
- Turn-on/Turn-off and Monitor: the command like buttons used by the user to send the command by pressing the button

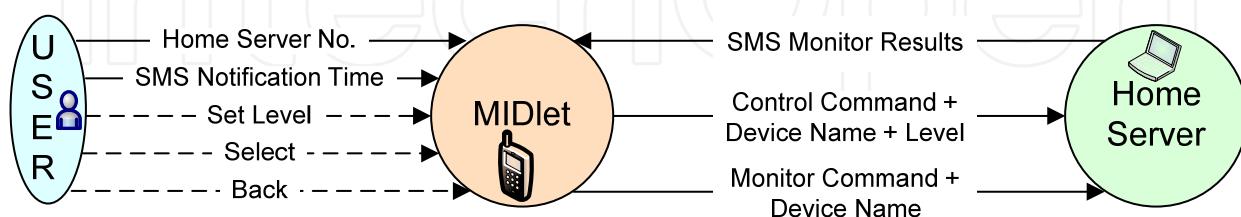


Fig. 13. Mobile Application Data Flow Diagram

The behaviour model of the mobile application is illustrated in Fig. 14. As can be seen in figure, the application moves or passes through four states to send a SMS message which contains the commands for home appliances.

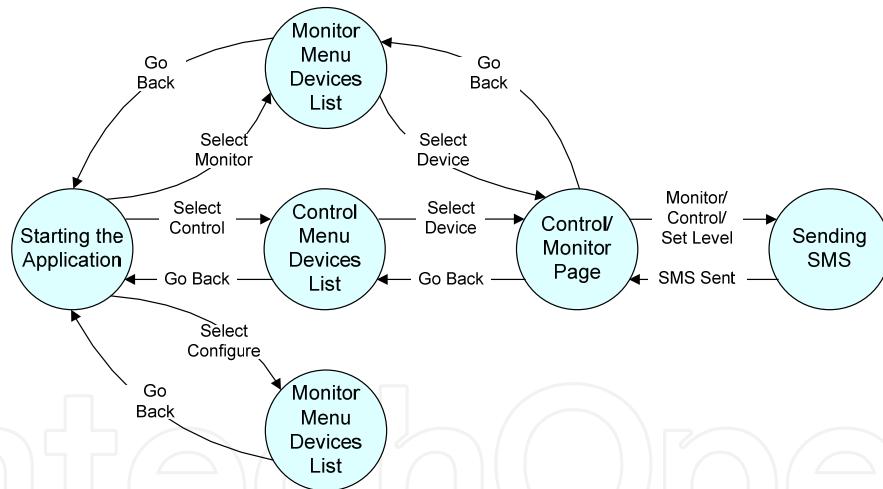


Fig. 14. Mobile Application Behavior Model

Fig. 15 show the data flow diagram model representing interaction between the home server and two appliances controlled by PIC microcontrollers. The home server communicates with each PIC microcontroller through a Bluetooth wireless connection. When the home server receives SMS message from a mobile phone, it extracts the message and checks its contents if the sender is an authorized one, otherwise it disregard the received message. The message could contain only three possibilities: Control a device, Monitor a device, or Set SMS notification time.

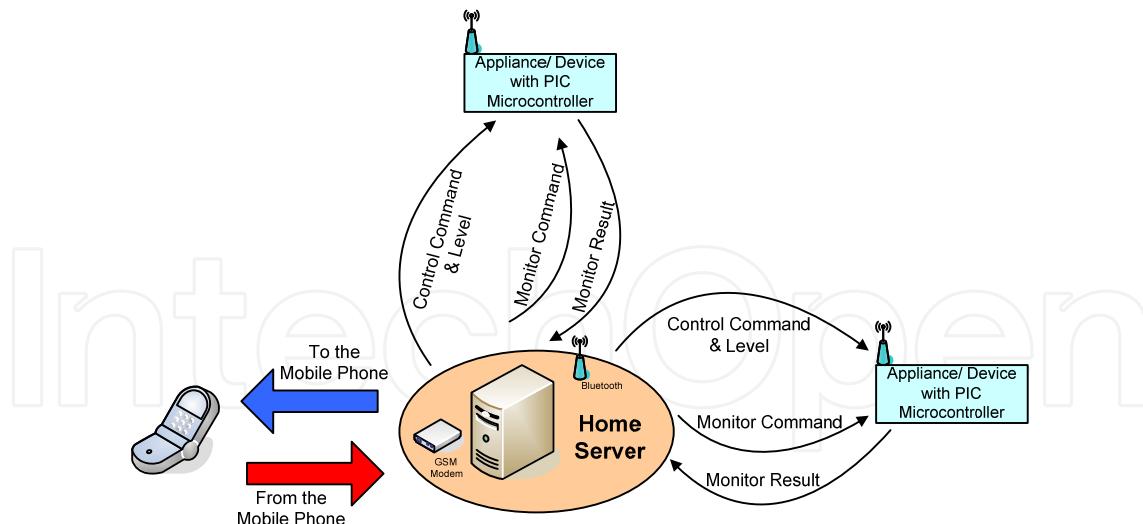


Fig. 15. Home Server Data Flow Model

If the message content is SMS notification time, the home server will set the new time. If the content is controlling a device the home server will look for the device. It assumes that each device at home has a smart interface, using a PIC microcontroller or another processor, and a Bluetooth MAC address. The server will open Bluetooth connection and then will send the control command (on/off) plus the level if the device has more than two control levels. After sending the command the connection will be closed by the server. In case of monitoring, the home server will open the Bluetooth connection and keeps it open until the PIC microcontroller replies with the device status. The SMS notification service can't be noticed from the data flow diagram therefore it is shown in the home server behavioural model in Fig. 16.

The behavioural model of the appliance controller application is shown in Fig. 17. The appliance is controlled via a PIC microcontroller. At the beginning, the PIC forces the Bluetooth adapter to change its mode to discoverable mode. In this mode the home server that acts as a master in the Bluetooth network scan and find the PIC Bluetooth adapter. The Bluetooth adapter accepts to open a connection with home server at the server request. The PIC microcontroller reads the sent command from the home server. For control command the PIC executes the command by setting the correct output at its output pins according to the sent command. For monitor command the PIC sends the status to home server.

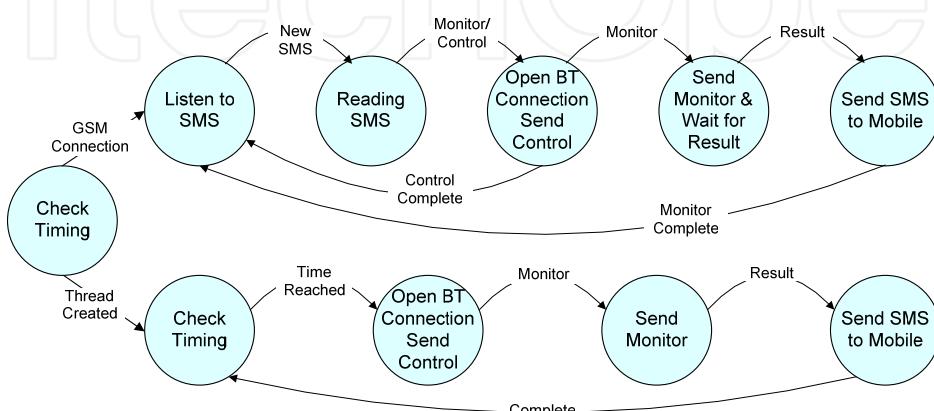


Fig. 16. Home Server Behavioural Model

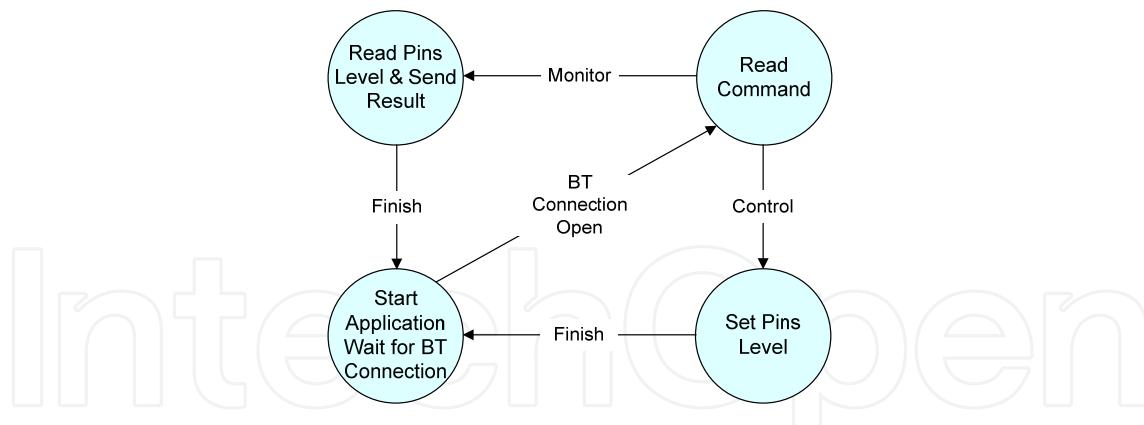


Fig. 17. Behavioural Model of Appliance Controller

6.2 System Security

Securing the complete system requires the incorporation of authentication as well as encryption layers. The authentication process is initiated through the GUI of the mobile phone once the application is enabled. The user is required to enter a username and a password. This information is then sent via SMS to the home server in order to establish the authenticity of the user through comparison with registered entries in the database. Once a valid user is identified the home server initiates a session that includes the phone number being used and a randomly generated number. The later number is used as an additional level of authentication and will expire once the session ends.

In this system, users are assigned access levels that define the actions they are allowed to perform. Security of the communication between the mobile station and the GSM/GPRS modem connected to the home server is achieved by the GSM encryption standard implemented at both ends. This is a highly robust method and hence additional security is not needed.

The most vulnerable part of the system is the connection between the home server and the various devices in the home. This is due to the use of Bluetooth to achieve connectivity and hence device monitoring and control. Bluetooth has inherent security problems that will expose the system to hacking should they be not addressed (Ferro and Potorti, 2005). Therefore, securing Bluetooth P-to-P communication required the implementation of an encryption/decryption process between the home server and the smart home devices that use Bluetooth wireless technology. This was implemented using a simplified form of AES (advanced encryption standard) algorithm. AES is a well known robust encryption standard that is widely used in various applications. This block cipher is relatively easy to implement, and does not require large amount of memory (Daemen and Rijmen, 2002).

6.3 Complete System Results

The system functionality and services were tested through verification and validation at all levels. This process included testing the user login and authentication, and remote monitoring and controlling devices/appliances at the home. The security features implemented to secure the communication between the home server and the remote devices were also tested in the process. The prototype system was evaluated by connecting the home server to a two-level device and a multiple-level device. The following paragraphs

demonstrate the security aspects discussed earlier and the use of a three-speed DC Fan as an example of a multiple-level device to be monitored and controlled.

As soon as the user starts the application on the mobile hand-set the MIDlet main login page appears as shown in Fig. 18(a). Under the Menu button page shown in Fig. 18(b) the user can select to either Register or Login. Selecting the Register option enables the user to register new users and add them to the database with the appropriate privilege level as shown in Fig. 18(c) below. If the user chooses the Login command the username and password get added to the URL and the http request is initiated to access the web server. An alert appears to notify the user that it is going to start an http request then a waiting page will appear. Depending on the user privilege that is stored in the database the appropriate list of commands appear. Should the login not be successful the process will go back to the initial login page.

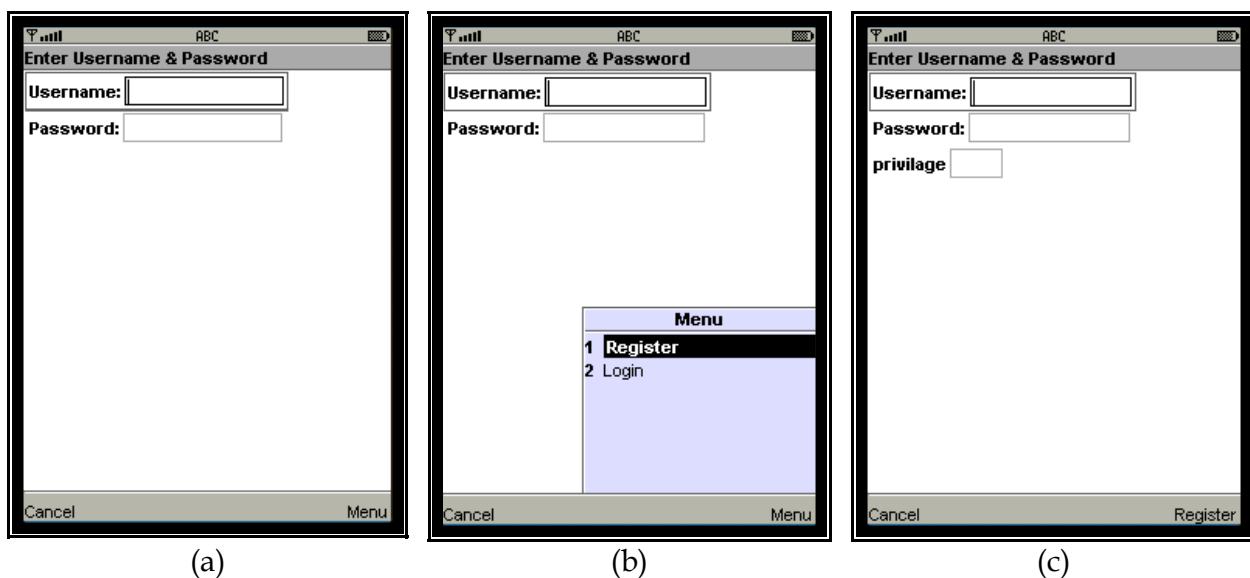


Fig. 18. (a) Main Page (b) List of Commands (c) Registration Page

The home device monitoring and control is illustrated in Fig. 19. To control the Fan the user chooses control a device from the main menu of the mobile application as shown in Fig. 19(a). The main menu also includes: monitor a device to check the status of a device and configuration to set the time interval for periodic notification of all devices' status. When the user selects the control mode, all connected home devices will be listed as shown in Fig. 19(b). Selecting a device will result in displaying a control page which has two buttons as shown in Fig. 19(c). Pressing Turn-Off will result in sending an SMS message to the home Server to turn-off the selected device. Clicking on Turn-On opens a new page as shown in Fig. 20(a). If the device to be controlled is a two-level (ON or OFF) device, this page will not be displayed. The next step is to select one of the three speeds for the Fan. An SMS is then automatically sent to the home server. The SMS includes the Fan name, the turn-On control command and the level information (speed two in Fig. 20). The home server would then open a Bluetooth connection with the PIC microcontroller of the Fan device on a certain MAC address. When the Bluetooth adapter on the device side accepts the connection, the home server sends setting the speed command. The Fan receives the command and changes its state to the appropriate speed.



Fig. 19. (a) Main Menu (b) Control Menu (c) Control Page



Fig. 20. Set the Speed for Fan (a) Set Level (b) Send Control Message

In this study the impact of overall system delay and failure of SMS delivery due to various communication and processing aspects was not tested directly. The rational for not implementing that is that the system is a prototype one and through assessment of its reliability and hardening of its security are not necessary. Having said this, the system has a regular update mode that can be used to check the operating status of the various appliances. This is not envisaged as a replacement for a proper mechanism to take care of delays and failure issues.

7. Conclusions

This chapter presented some of the state of the art technologies and associated applications in the field of smart homes. It gave an overview of the major wireless communication technologies that form a fundamental part of the infrastructure of modern smart homes. Some of those technologies are integrated within sensing and networking devices such as Zigbee, Bluetooth, RFID, and WiFi. Other wireless technologies, such as the GSM, are more of a wider format that can form large network and yet can integrate with the other ones dedicated for short range. The paper also briefly discussed some of the modern sensors that can be used in smart homes. Many of them are of the embedded ubiquitous type that is equipped with wireless communication capabilities and can connect to other devices. The application areas discussed include appliances monitoring and control, safety and security, telehealth care, energy saving, environmental control, and information access.

Some of these areas are more developed than others, however, all those areas are either already available or they are expected to be deployed in the near future. The chapter included a case study of a complete end-to-end smart home system that is used to monitor and control home appliances using a mobile phone. The prototype system used GSM as the external network and Bluetooth as an internal network. However, other suitable wireless technologies can be used on the same architecture. The system enables two way control and has automatic updating service that informs the user about the status of the devices at regular intervals.

Given the advanced status of the constituents of smart homes, it is expected that many of the existing homes will be turned smart in the not too distant future. So, the future vision of the smart home is getting closer, but the designers need to spend more time to learn how people live within the bounds of their homes.

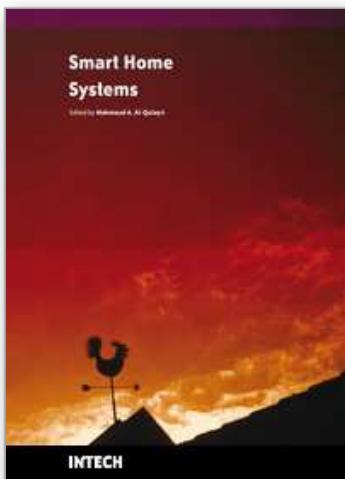
8. References

- Al-Qutayri, M., Barada, H., Al-Mehairi, S., and Nuaimi, J. (2008) "A Framework for an End-to-End Secure Wireless Smart Home System," IEEE Systems Conf., pp. 1-7
- Al-Qutayri, M., Barada, H., and Al-Mehairi, S. (2010) "Integrated Secure Wireless System for Smart Home Monitoring and Control," Int. Journal of Computer Aided Engineering and Technology, Vol. 2, Nos. 2/3, pp. 181-198
- Al-Qutayri, M.A. and Jeedella, J.S. (2010) "Smart Homes: Technologies and Challenges," Int. Journal of Computer Aided Engineering and Technology, Vol. 2, Nos. 2/3, pp. 125-144.
- Augusto, J. (2007) "Ambient Intelligence: the Confluence of Ubiquitous/Pervasive Computing and Artificial Intelligence," In Intelligent Computing Everywhere, Springer, pp. 213-234
- Augusto, J. C. and Nugent, C. D. (2006) "Smart Homes Can Be Smarter," In Designing Smart Homes - The Role of Artificial Intelligence, pp. 1-15.
- Balasubramanian, K. and Cellatoglu, A. (2008) "Improvements in Home Automation Strategies for Designing Apparatus for Efficient Smart Home," IEEE Transactions on Consumer Electronics, Vol. 54, No. 4, pp. 1681-1687.
- Baldauf, M., Dustdar, S., and Rosenberg, F. (2007) "A Survey on Context-Aware Systems," Int. Journal of Ad Hoc and Ubiquitous Computing, vol. 2, no. 4, pp. 263-277
- Botsis, T. and Hartvigsen, G. (2008) "Current Status and Future Perspectives in Telecare for Elderly People Suffering from Chronic Diseases," Journal of Telemedicine and Telecare, Vol. 14, No. 4, pp. 195-203
- Brand, A. and Aghvami, H. (2002) Multiple Access Protocols for Mobile Communications: GPRS, UMTS and Beyond, Wiley
- Bricon-Souf, N. and Newman, C. R. (2007) "Context awareness in health care: A review," Int. Journal of Medical Informatics, vol. 76, no. 1, pp. 2-12
- Carettoni, L., Merloni, C., and Zanero, S. (2007) "Studying Bluetooth Malware Propagation: The BlueBag Project," IEEE Security & Privacy, vol. 5, no. 2, pp. 17-25
- Chan, H. and Perrig, A., (2003) "Security and Privacy in Sensor Networks," IEEE Computer, Vol. 36, Issue 10, pp. 99-101.

- Choi, J., Shin, D., and Shin, D. (2005) "Research and Implementation of the Context-Aware Middleware for Controlling Home Appliances," *IEEE Trans. on Consumer Electronics*, vol. 51, no. 1, pp. 301-306
- Cook, D. J. (2006) "Health Monitoring and Assistance to Support Aging in Place," *Journal of Universal Computer Science*, vol. 12, no. 1, 2006, pp. 15-29
- Cook, D.J., Youngblood, M., Heierman, E., Gopalratnam, K., Rao, S., Litvin, A., and Khawaja, F. (2003) "MavHome: An agent-based smart home," First IEEE Int. Conf. on Pervasive Computing and Communications (PerCom'03), pp. 521-524.
- Daemen, J. And Rijmen, V. (2002) *The Design of Rijndael: AES - The Advanced Encryption Standard (Information Security and Cryptography)*, Springer
- Dargie, W. (2009) *Context-Aware Computing and Self-Managing Systems*, Chapman & Hall
- Darianian, M. and M. P. Michael (2008) "Smart Home Mobile RFID-Based Internet-of-Things Systems and Services" *Int. Conf. on Advanced Computer Theory and Engineering (ICACTE08)*, pp. 116-120
- Decker, C., Krohn, A., Beigl, M., and Zimmer, T. (2005) "The Particle Computer System," *Int. Symp. on Information Processing in Sensor Networks*, pp. 443-448.
- Dengler, S., Awad, A., and Dressler, F. (2007) "Sensor/Actuator Networks in Smart Homes for Supporting Elderly and Handicapped People," *Int. Conf. on Advanced Information Networking and Applications Workshops*, pp. 863-868
- Estrin, D. Culler, D. Pister, K. and Sukhatme, G. (2002) "Connecting the physical world with pervasive networks," *IEEE Pervasive Computing*, Vol.1, Issue 1, pp.59-69.
- Ferro, E. And Potorti, F. (2005) "Bluetooth and Wi-Fi wireless protocols: a survey and a comparison," *IEEE Wireless Communications*, Vol. 12, Issue 1, pp. 12-26
- Friedewald, M., Da Costa, O., Punie, Y., Alahuhta, P., and Heinonen, S. (2005) "Perspectives of ambient intelligence in the home environment," *Telematics and Informatics* Vol. 22, pp. 221-238.
- Garlan, D., Siewiorek, P.D., Smailagic, A., and Steenkiste, P. (2002) "Project Aura: Toward Distraction-Free Pervasive Computing," *IEEE Pervasive Computing*, Vol. 1, No. 2, pp. 22-31.
- Gislason, D. (2008). *Zigbee Wireless Networking*, Newnes
- Haryanto, R. (2005) *Context Awareness in Smart Homes to Support Independent Living*, MSc Thesis, University of Technology, Sydney, Australia, 2005
- Helal, S., Mann, W., El-Zabadani, H., King, J., Kaddoura, Y., and Jansen, E. (2005) "The Gator Tech Smart House: A Programmable Pervasive Space," *IEEE Computer Magazine*, no. 3, pp. 64-74
- Ilarri, S., Mena, E., and Illarramendi, A. (2008) "Using Cooperative Mobile Agents to Monitor Distributed and Dynamic Environments," *Information Sciences*, vol. 178, no. 9, pp. 2105-2127
- Juels, A. (2006) "RFID Security and Privacy: A Research Survey," *IEEE Journal on Selected Areas in Communications* Vol. 24, Issue 2, pp. 381-394.
- Kientz, J., Patel, S., Jones, B., Price, E., Mynatt, E., and Abowd, G. (2008) "The Georgia Tech Aware Home," *ACM Conference on Human Factors in Computing Systems*, pp. 3675-3680
- Labiod, H., Afifi, H. and De Santis, C. (2007), *WI-Fi, Bluetooth, Zigbee and Wimax*, Springer.
- Leopold, M., Dydensborg, M., and Bonnet, P. (2003) "Bluetooth and Sensor Networks: A Reality Check," *Int. Conf. on Embedded Networked Sensor Systems*, pp.103-113

- Liu, Y., Bacon, J., and Wilson-Hinds, R. (2007) "On Smart-Care Services: Studies of Visually Impaired Users in Living Contexts" Int. Conf. on Digital Society (ICDS), 2007
- Ma, J., Yang, L., Apduhan, B., Huang, R., Barolli, L., and Takizawa, M. (2005) "Towards a Smart World and Ubiquitous Intelligence: A Walkthrough from Smart Things to Smart Hyperspaces and UbiKids," Journal of Pervasive Computing and Communications, Vol.1, No.1, pp. 53-68
- Mann, W., El-Zabadani, H., King, J., Kaddoura, Y., and Jansen, E. (2005) "The Gator Tech Smart House: A Programmable Pervasive Space," IEEE Computer, Vol. 38, Issue 3, pp. 64-74
- Marsa-Maestre, I., Lopez-Carmona, M., Velasco, J., and Navarro, A. (2008) "Mobile Agents for Service Personalization in Smart Environments," Journal of Networks, Vol. 3, No. 5, pp. 30-41.
- Merloni (2003). "Merloni Unveils RFID Appliances," RFID Journal
- Mozer, M. C. (2005) "Lessons from an Adaptive House," In D. Cook & R. Das (Eds.), Smart environments: Technologies, protocols, and applications, (pp. 273-294), Wiley & Sons
- Oh, Y., and Woo, W. (2004), "A Unified Application Service Model for ubiHome by Exploiting Intelligent Context-Awareness," Int. Symp. Ubiquitous Computing Systems, LNCS, pp. 192-202
- Oh, Y. and Woo, W. (2005) "A Unified Application Service Model for ubiHome by Exploiting Intelligent Context-Awareness," In Ubiquitous Computing Systems, Springer, pp. 192-202
- Pooter, B. (2006) "Bluetooth Security Moves," Network Security, Vol. 2006, Issue 3, pp.19-20.
- Rammal, A., Trouilhet, S., Singer, N., and Pécatte, J.M. (2008) "An Adaptive System for Home Monitoring Using a Multiagent Classification of Patterns," Int.1 Journal of Telemedicine and Applications, Vol. 2008, Article ID 136054
- Roduner, C., Langheinrich, M., Floerkemeier, C., and Schwarzentrub, B. (2007) "Operating Appliances with Mobile Phones – Strengths and Limits of a Universal Interaction Device," in Pervasive Computing, LNCS, Springer, pp. 198-215
- Satyanarayanan, M. (2001). "Pervasive Computing: Vision and Challenges," IEEE Personal Communications, vol. 6, no. 8, pp. 10-17
- Schaefer, R., Mueller, W., and Groppe, J. (2006) "Profile Processing and Evolution for Smart Environments," Proceedings of 3rd Int. Conf. on Ubiquitous Intelligence and Computing (UIC-06), LNC, pp. 746-755
- Tabar, A. M., Keshavarz, A., and Aghajan, H. (2006) "Smart Home Care Network using Sensor Fusion and Distributed Vision-based Reasoning," Proceedings of the 4th ACM Int. workshop on Video surveillance and sensor networks, pp. 145-154.
- Thompson, T. J., Kumar, C. B., and Kline, P. J. (2008), Bluetooth Application Programming with the Java APIs, Morgan Kaufmann
- Velasco, J., Marsá-Maestre, I., Navarro, A., López, M., Vicente, A., Hoz, E., Paricio, A., and Machuca, M. (2005) "Location aware services and interfaces in smart homes using multiagent systems," Proc. Int. Conference on Pervasive Systems and Computing (PSC'05), USA
- Venables, M. (2007). "Smart Meters Make Smart Consumers [Analysis]." Engineering & Technology 2(4): 23-23.

- Weiser, M. (1991) "The Computer for the 21st Century", *Scientific American*, vol. 165, pp. 94-104
- Want, R. (2006). "An Introduction to RFID Technology," *IEEE Pervasive Computing*, Vol. 5, Issue 1, pp.25-33.
- Yamazaki, T., (2007) "The Ubiquitous Home," *Int. Journal of Smart Homes*, Vol. 1, No. 1, pp. 17-22
- Zambonelli, F., Jennings, N., Omicini, A., and Wooldridge, M. (2000) "Agent Oriented Software Engineering for Internet Applications," In *Coordination of Internet Agents: Models, Technologies and Applications*, Springer



Smart Home Systems

Edited by Mahmoud A. Al-Qutayri

ISBN 978-953-307-050-6

Hard cover, 194 pages

Publisher InTech

Published online 01, February, 2010

Published in print edition February, 2010

Smart homes are intelligent environments that interact dynamically and respond readily in an adaptive manner to the needs of the occupants and changes in the ambient conditions. The realization of systems that support the smart homes concept requires integration of technologies from different fields. Among the challenges that the designers face is to make all the components of the system interact in a seamless, reliable and secure manner. Another major challenge is to design the smart home in a way that takes into account the way humans live and interact. This later aspect requires input from the humanities and social sciences fields. The need for input from diverse fields of knowledge reflects the multidisciplinary nature of the research and development effort required to realize smart homes that are acceptable to the general public. The applications that can be supported by a smart home are very wide and their degree of sophistication depends on the underlying technology used. Some of the application areas include monitoring and control of appliances, security, telemedicine, entertainment, location based services, care for children and the elderly... etc. This book consists of eleven chapters that cover various aspects of smart home systems.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Mahmoud A. Al-Qutayri and Jeedella S. Jeedella (2010). Integrated Wireless Technologies for Smart Homes Applications, Smart Home Systems, Mahmoud A. Al-Qutayri (Ed.), ISBN: 978-953-307-050-6, InTech, Available from: <http://www.intechopen.com/books/smart-home-systems/integrated-wireless-technologies-for-smart-homes-applications>



InTech Europe

University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China

Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

© 2010 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the [Creative Commons Attribution-NonCommercial-ShareAlike-3.0 License](#), which permits use, distribution and reproduction for non-commercial purposes, provided the original is properly cited and derivative works building on this content are distributed under the same license.

IntechOpen

IntechOpen