Technical University of Crete

Department of Production Engineering and Management

Integration of Smart technologies in buildings

Diploma thesis by **Eleftheria Ntalla**

Supervisor: Professor Anastasios Pouliezos

Chania 2016

ABSTRACT

Smart home is the integration of advanced technology and services through home networking, which allows owners to have advanced monitoring of building functions for better quality of living. This thesis presents and analyzes the parameters of this technology, as the means of disseminating information, the system components and their functions, as well as the communication protocols of the systems that constitute the "smart" network. It describes collective information about sensors, multimedia devices and communication protocols which are widely used in smart home implementation.

ΠΕΡΙΛΗΨΗ

Έξυπνη κατοικία ή έξυπνο κτήριο είναι το κτήριο το οποίο ενσωματώνει εξελιγμένα συστήματα που επιτρέπουν στους ιδιοκτήτες προηγμένη παρακολούθηση και έλεγχο των λειτουργιών του κτηρίου. Στην παρούσα διπλωματική αναλύονται οι παράμετροι της εν λόγω τεχνολογίας, όπως τα μέσα διάδοσης πληροφορίας, τα στοιχεία του συστήματος και οι λειτουργίες τους, όπως επίσης και τα πρωτόκολλα επικοινωνίας των συστημάτων που στοιχειοθετούν το «έξυπνο» δίκτυο. Περιγράφει με συλλογικές πληροφορίες τους αισθητήρες, τις συσκευές πολυμέσων και τα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται ευρέως στην εκτέλεση των εργασιών του έξυπνου κτηρίου.

Contents

1. Introduction

When you're not home, nagging little doubts can start to crowd your mind. Did I turn the coffee maker off? Did I set the security alarm? Did I turn the heater off?

With a smart home, you could quiet all of these worries with a quick glance at your smartphone or tablet. You could connect the devices and appliances in your home so they can communicate with each other and with you.

Any device in your home that uses electricity can be put on your home network and at your command. Whether you give that command by voice, remote control, tablet or smartphone, the home reacts. Most applications relate to lighting, home security and thermostat regulation.

"A smart home, or smart house, is a home that incorporates advanced automation systems to provide the inhabitants with sophisticated monitoring and control over the building's functions."

Much of this is due to the jaw-dropping success of smartphones and tablet computers. These ultra-portable computers are everywhere, and their constant Internet connection means can be configured to control myriad other online devices. It's all about the Internet of Things.

"The Internet of Things" is a phrase that refers to the objects and products that are interconnected and identifiable through digital networks. This web-like sprawl of products is getting bigger and better every day. All of the electronics in your home are fair game for this tech revolution, from your fridge to your furnace.

1.1 Historical evolution

Although the term "smart home" was first used in 1980s, the concept is far from new. The early documented attempt to envisage something very similar dates back to the 1960s, with Walt Disney's Experimental Prototype Community of Tomorrow (EPCOT), presented in 1966.

Disney announced plans to develop another theme park to be called Disney World a few miles southwest of Orlando. Disney World was to include "the Magic Kingdom", a larger, more elaborate version of Disneyland. It would also feature a number of golf courses and resort hotels. The heart of Disney World, however, was to be the Experimental Prototype City (or Community) of Tomorrow, known as EPCOT for short.

An elaborated definition of a smart home was published by Intertek[1] in 2003, which was involved with the Department of Trade and Industry smart home project in the UK. According to Intertek, a smart home is a dwelling incorporating a communications network that connects key electrical appliances and services and allows them to be remotely controlled, monitored, or accessed.

A recent definition by Lalatendu Satpathy, UX Architect at SAP Ariba, provides a more appropriate concept of smart homes. According to Satpathy, "a home which is smart enough to assist the inhabitants to live independently and comfortably with the help of technology is termed as smart home. In a smart home, all the mechanical and digital devices are interconnected to form a network, which can communicate with each other and with the user to create an interactive space". The author does not include remote access in the definition.

Considering the current trends in smart home research, we can define the smart home as an application of ubiquitous computing that is able to provide user context-aware automated or assistive services in the form of ambient intelligence, remote home control, or home automation.

1.2 Benefits

Smart home projects have been conducted over the last several decades; they convey different ideas, functions, and utilities. Smart homes are extending into different branches of specialization focusing on the interests of researchers and user requirements and expectations. Smart homes provide comfort, healthcare, and security services to their inhabitants. Comfort and healthcare services can be provided locally as well as remotely. Security measures not only provide authentication services to the user but also restrict unauthorized access to the household devices.

Smart buildings are not just about installing and operating technology or technology advancements. Technology and the systems in buildings are simply enablers, a means to an end. The technology allows us to operate the building more efficiently; to construct the buildings in a more efficient way, to provide productive and healthy spaces for the occupants and visitors, to provide a safe environment, to provide an energy-efficient and sustainable environment and to differentiate and improve the marketability of the building.

Smart homes enable users to connect, control and monitor all appliances and information in the home through simple and intuitive user interfaces. There are numerous different use cases that can be identified around four main application areas: Security, Energy, Comfort and Healthcare.

1.2.1. 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.

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. Having a smart system installed in the home, it will transmit detailed information specifying the exact location and the cause of the alarm.

1.2.2. Home Energy Management

Home energy management is mainly about monitoring and controlling home energy consumption. The main sources of power consumption in the house are heating systems, water pumps, cooling, lighting and large electrical appliances. The three main actors in this market are utilities, regulators and consumers themselves.

The consumer's interest is in reducing the monthly bill or increasingly become a green citizen, encouraging measures that reduce power consumption and one's carbon footprint.

The utilities' interest is in reducing the level and duration of peak consumption and optimizing production capacity by being able to plan power generation on the basis of predicted customer demand.

Regulators in many countries are pushing for the installation of smart meters to reduce power consumption. The energy saving is one of the main reasons for the emergence of smart home automation concept. Most wireless autonomous devices are usually battery-powered. Therefore it's essential to manage the smart devices to best utilize the scarce power resources over long time.
Some of the techniques employed to reduce power consumption includes;

Ability to enable sleep mode: The device is shutdown (sleep mode) when not transmitting or receiving.

Keep low duty cycle:

$$T_{duty\_cycle} = \frac{T_{tx/rx}}{T_{cycle}}$$

Equation 1: Duty cycle

T_{duty_cycle} : Duty time; Device's active time

$T_{tx/rx}$: Transmission or reception time; A fraction of the time gap between activities

T_{cycle} : Total cycle time between transmission and reception.

With low duty cycles, the smart node is active for a small time period, making power optimization. This can be achieved using short transmission or reception time and long time interval between transmission and reception.

1.2.3. Comfort

The comfort market embraces solutions enabling control of the home’s environmental conditions. These include Heating, Ventilation and Air Conditioning (HVAC), lighting control, shutters control and garden watering. The objective is to enable centralized control of the home environment as simply as possible from a single platform. For example if a kid’s movie is ordered in a Smart Home, the lighting could automatically be set at medium with shutters open, but for a horror movie, shutters would be lowered and all lights extinguished.

1.2.4. Healthcare

The rising cost of healthcare in the developed world has driven the governments to make efforts in order to manage and reduce it. A variety of remote services have been tested and deployed on a limited basis, including transmission of biometric data such as blood pressure, glucose level and heart rate to medical centers, as well as remote surveillance and detection of falls for the elderly. It is noticeable that it is more cost-effective for older adults and persons with disabilities to remain living at home for as long as possible, with assistive, supportive and health-monitoring devices than to be placed in healthcare institutions.

1.3 Design

Smart buildings recognize and reflect the technological advancements and convergence of building systems, the common elements of the systems and the additional functionality that integrated systems provide. Smart buildings provide information about a building or space within a building to allow the owner or occupant to manage the building or space.

They provide the most cost effective approach to the design and the deployment of building technology systems. The traditional way to design and construct a building is to design, install, and operate each system separately.

The smart building takes a different approach to designing the systems. Essentially, one designer designs or coordinates the design of all the building technology systems into a unified and consistent construction document. The construction document specifies each system and addresses the common system elements or integration foundation for the systems. These include cabling, cable pathways, equipment rooms, system databases, and communication protocols between devices. The one consolidated design is then installed by a contractor, referred to as a Technology Contractor or as a Master System Integrator.

This process reduces the inefficiencies in the design and construction process saving time and money. During the operation of the building, the building technology systems are integrated horizontally among all subsystems as well as vertically—that is subsystems to facility management systems to business systems—allowing information and data about the building’s operation to be used by multiple individuals occupying and managing the building.

Smart buildings are also a critical component regarding energy usage and sustainability of buildings and the smart electrical grid. The building automation systems, such as HVAC control, lighting control, power management, and metering play a major role in determining the operational energy efficiency of a building. The smart electrical grid is dependent on smart buildings.

The driving forces for smart buildings are economics, energy, and technology. Smart buildings leverage mainstream information technology infrastructure and take advantage of existing and emerging technology.

For developers and owners, smart buildings increase the value of a property. For property and facility managers, smart buildings provide more effective subsystems and more efficient management options, such as the consolidation of system management. For architects, engineers, and construction contractors, it means combining portions of the design and construction with the resulting savings and efficiencies in project management and project scheduling.

[1] **Intertek Group plc** is a multinational inspection, product testing and certification company headquartered in London, United Kingdom. It is listed on the London Stock Exchange and is a constituent of the FTSE 100 Index.

2. Basic Structure of a Smart Home System

The smart home integration consists of three major areas. The physical components (electronic devices-sensors-actuators), the control system (artificial intelligence/expert system) and the communication system (wired/wireless network) which connects physical components and control system.

The control system can access from home exterior through external home network like mobile network or Internet. In a smart home system the physical components sense the environment and pass to home control system through home sub networks and home network. Home control system takes the decision and passes the control information to the actuators through home network.

For example, gas sensor detects the gas leakage in a smart home and passes this message to the home control system through ZigBee, a wireless network. Control system decides to switch off the gas valve and pass this to actuator, which will close the gas valve.

The basic structure of a smart home system is depicted in *Figure 1*

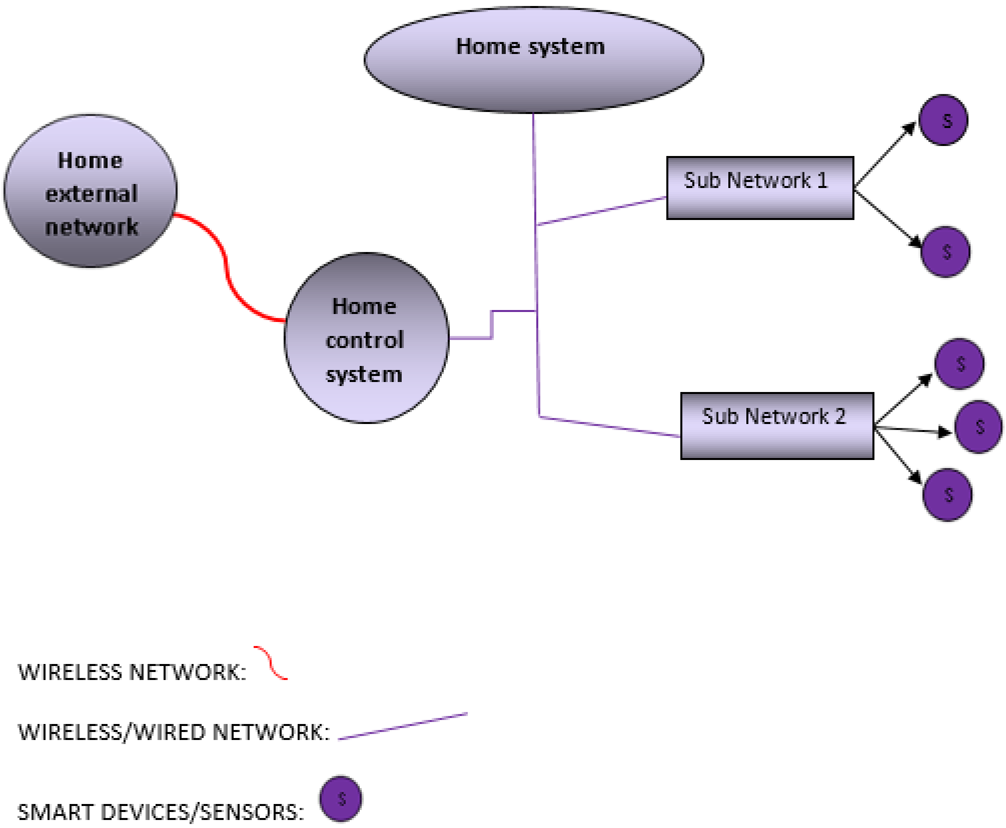


Figure 1: Basic Structure of a Smart Home System

2.1 Physical Components

The role of physical components is quite important as they measure and collect the information and share with the control system through network. Sensors, microcontroller, actuator and smart devices are used as physical components. Different applications use different sensors. They observe the smart home resident's interaction with objects such as doors, windows, keys and all home appliances.

2.1.1 Actuators

Actuators are electrical or electronic devices that can control a household appliance.

When they come as a separate device, they need to be electrically coupled with the appliance and can control it by executing some simple commands, such as switching it on or off. When they are embedded within the appliance itself, they can be more sophisticated and provide more value added to the user.

2.1.2 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, Berkeley MOTES… 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.

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. 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 optimize 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.

2.2 Control System

The control system is a critical part of a Smart Home as it determines usability, reliability and overall effectiveness of the solution provided. These systems are written as a piece of software that is run on a home computer or embedded in an electronic device. These software systems offer the ability to control a subset of the home appliances from a centralized location. Most of them also provide users with the option to store macro commands; that is, to combine a list of tasks together. These macros can be then invoked by the user when required or be automatically executed by the system at a pre-set scheduled date and time.

2.3 Communication System

The communication system is used to share the information between physical components and control system in the smart home system. It can be wired or wireless communication. The widely used wireless technologies are Bluetooth, WiFi and Zigbee. Bluetooth is the first and popular low bandwidth wireless interface for the smart home. In the last few years the bandwidth requirement of the smart home has increased dramatically which introduces WiFi – a wireless local area networks technology based on the IEEE 802.11.

3. Means of Information transmission

Information is a sequence of signals that are either recorded or transmitted. It is that from which data and knowledge can be derived, as data represents values attributed to parameters and knowledge signifies understanding of real things or abstract concepts. Information is often defined in relation to the meaning of data. In computer networks, the synonym for data transfer is bandwidth.

Bandwidth is the amount of data that can be carried from one point to another in a given time period (usually a second).

Network bandwidth is usually expressed in bits per second (bps); modern networks typically have speeds measured in the millions of bits per second (megabits per second, or Mbps) or billions of bits per second (gigabits per second, or Gbps).

Bandwidth is the range of frequencies -- the difference between the highest-frequency signal component and the lowest-frequency signal component -- an electronic signal used on a given transmission medium. Like the frequency of a signal, bandwidth is measured in hertz (cycles per second). This is the original meaning of bandwidth, although it is now used primarily in discussions about cellular networks and the spectrum of frequencies that operators license from various governments for use in mobile services.

Speed = frequency · wavelength

$$c = f \cdot \lambda$$

Equation 2: Speed

Frequency (f) is the number of occurrences of a repeating event per unit time. It is measured in Hz

Wavelength (λ) is the spatial period of the wave. The distance over which the wave's shape repeats. It is measured in meters.

A wave has a certain speed, frequency and wavelength. These are connected by the previous relation. Speed is measured in meters/second

Bit (BInary Digi**T) (b)** is a basic unit of information in computing and digital communications. A bit can have only one of two values, and may therefore be physically implemented with a two-state device. These values are most commonly represented as either 0 or 1.

Byte (B) is a unit of digital information that most commonly consists of eight bits. Historically, the byte was the number of bits used to encode a single character of text in a computer and for this reason it is the smallest addressable unit of memory in many computer architectures.

- 1 Byte = 8 bit

The development of smart home technologies and services has been somewhat limited by different communication protocols and technologies. These differ in their sophistication and maturity with some protocols being specifically developed for a consumer market e.g. X10 and CEBus, and others emerging from office automation and the control industry e.g. LonWorks.

3.1 Types of smart home technology

Smart home network technology can be classified into two main types, which are wiring system and wireless system.

In wiring system, the equipment is connected into the main power supply directly, so the data will be sent to the devices to activate or deactivate them. There are many types of wires that people may want to install in-wall. Many home automations are connected through wiring system such as new wire (twisted pair, optical fiber), Powerline, Busline, etc.

In the wireless system, there must have two main elements that are sender and receiver. Many new appliances use wireless technology to communicate with other devices. The example of wireless communication system are microwaves, Infrared (IR), radio frequency (RF), Wi-Fi, Bluetooth, IEEE 802.11, and so on.

There is also a variety of technologies for linking smart home components together.

The 4 main types of smart home technology are described as:

- Mains borne, e.g. X10 and Powerline;
- Busline, e.g. Konnex Association or LonWorks;
- Radio Frequency, e.g. Bluetooth
- Infrared, of various types.

Each has potential advantages and disadvantages and no single solution is ideal for all application areas so that a hybrid of different technologies is likely to be found in a smart home.

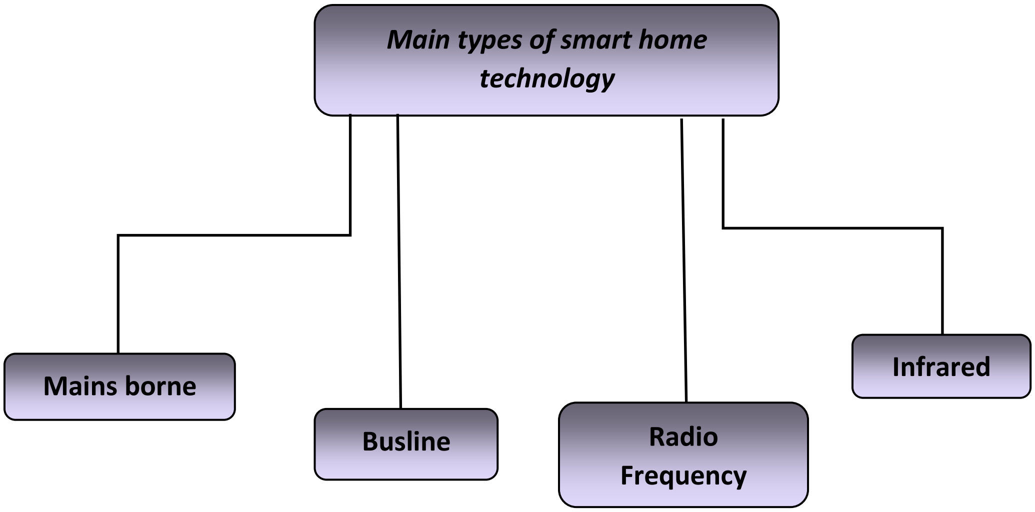


Figure 2: Main types of Smart Home Technology

Mains borne communication systems

They are easy to install, but can be prone to electrical interference from 'dirty' power lines. Where mains operated devices are needed, such as lights and actuators, installation tends to be easy, but where significant numbers of sensors are required it can be limiting.

Bus operated systems

They require additional wiring in the home which can make retrofit installation more difficult, but likely to be more reliable, which can be important for safety critical information such as alarm states.

Radio frequency transmission

Becoming increasingly popular as it can make retrofit installation of sensors particularly easy. Sensors can be located anywhere without extensive rewiring and modern battery technology means sensors can operate for years without battery replacement being needed. These technologies are increasingly being used in home security and social alarm systems.

Infrared

Well established as a communication medium for home systems, and ideally suited to control existing home devices such as televisions and video recorders Infrared can also be used to provide a user interface to a smart home system, allowing freedom of operation of any component. It also provides some flexibility for the connection of more specialist assistive devices for severely disabled people such as environmental control systems and communication devices. However, it is limited to line of sight operation and is also not particularly suitable for transmitting secure information.

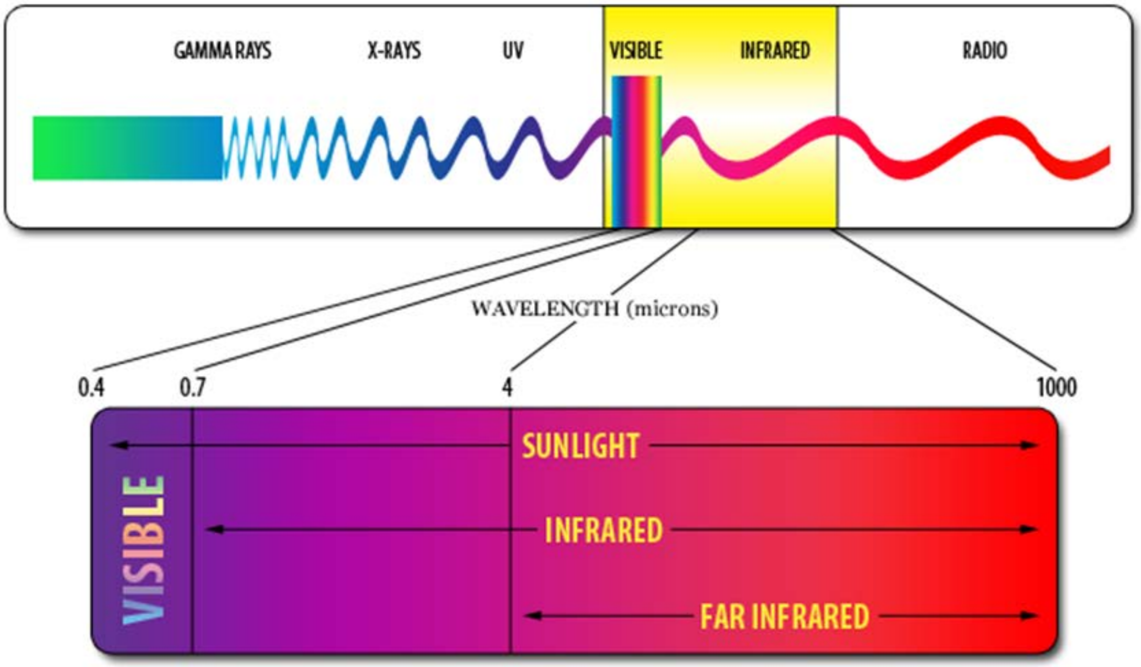


Figure 3: Wavelength

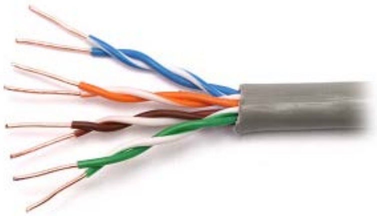
3.2 Wired

A wired network is the most common type of local area network (LAN) technology. A wired network is a collection of two or more devices linked by Ethernet cables. It is secure and dependable and should be used for the transmission of sensitive or personal data.

In smart home technology, the most widespread wired connections are taking place via following:

- **Twisted pair** cabling is a type of wiring in which two conductors of a single circuit are twisted together for the purposes of canceling out electromagnetic interference (EMI) from external sources.

- **UTP** (Unshielded Twisted Pair) cables are found in many Ethernet networks and telephone systems. Twisted pair cabling is



often used in data networks for short and medium length connections because of its relatively lower costs compared to optical fiber.

- **PLC** (Power Line Communication) is a communication protocol that uses electrical wiring to simultaneously carry both data and Alternating Current (AC) for electric power transmission or electric power distribution.

- **Ethernet** was developed at Xerox PARC between 1973 and 1974. It is a family of computer networking technologies commonly used in local area networks and metropolitan area networks. Ethernet evolved to include higher bandwidth, improved media access control methods and different physical media. The original Ethernet uses coaxial cable as a shared medium, while the newer Ethernet variants use twisted pair and fiber optic links in conjunction with hubs or switches. Ethernet stations communicate by sending each other data packets: blocks of data individually sent and delivered.

- **Optical fiber** refers to the medium and the technology associated with the transmission of information as light pulses along the glass or plastic strand of fiber. Optical fiber carries much more information than conventional copper wire and is in general not subject to electromagnetic interference and the need to retransmit signals. It is used as a means to transmit light between the two ends of the fiber and in communications, where is permits transmission over long distances and at high bandwidths.

3.3 Wireless

The wireless technology standards are everywhere. Bluetooth, 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. Wireless allows for devices to be shared without networking cable which increases mobility but decreases range. 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.

- **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. It can also 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 sometimes 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.

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 internet-working functions. To cover an extended area, basic cells may sometimes partially overlap.

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.

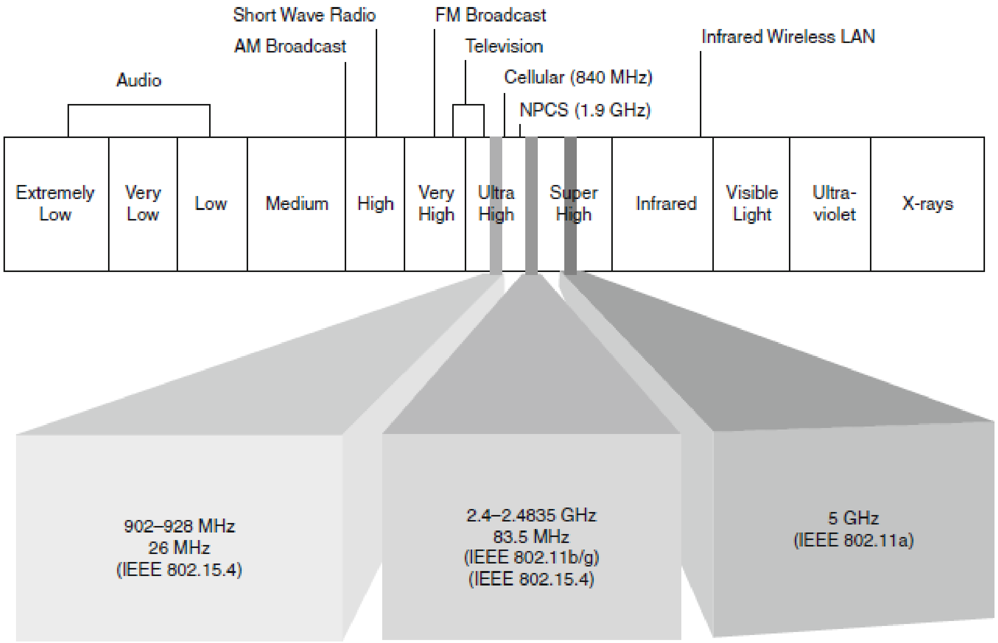


Figure 4: Radio Frequencies for WiFi

IEEE802.11 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.

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 electronic 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 electronic 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.

- **Radio Frequency Identification** (RFID) describes a system that transmits the identity of an object wirelessly using radio waves. 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. 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. 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. However, researchers are looking for new ways to improve the readability of RFID tags in these difficult environments.

- **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. 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.

  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.

  The challenges that the use of Bluetooth face 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.

- **NFC (Near Field Communication)** is a form of contactless communication between devices like smartphones or tablets. Contactless communication allows a user to wave the smartphone over a NFC compatible device to send information without needing to touch the devices together or go through multiple steps setting up a connection. Fast and convenient, NFC technology is popular in parts of Europe and Asia, and is quickly spreading throughout the United States.

  Near field communication maintains interoperability between different wireless communication methods like Bluetooth and other NFC standards through the NFC Forum. Founded in 2004 by Sony, Nokia, and Philips, the forum enforces strict standards that manufacturers must meet when designing NFC compatible devices. This ensures that NFC is secure and remains easy-to-use with different versions of the technology. Compatibility is the key to the growth of NFC as a popular payment and data communication method. It must be able to communicate with other wireless technologies and be able to interact with different types of NFC transmissions.

  The technology behind NFC allows a device, known as a reader, interrogator, or active device, to create a radio frequency current that communicates with another NFC compatible device or a small NFC tag holding the information the reader wants. Passive devices, such as the NFC tag in smart posters, store information and communicate with the reader but do not actively read other devices. Peer-to-peer communication through two active devices is also a possibility with NFC. This allows both devices to send and receive information.

  Both businesses and individuals benefit from near field communication technology.

  By integrating credit cards, subway tickets, and paper coupons all into one device, a customer can board a train, pay for groceries, redeem coupons or store loyalty points, and even exchange contact information all with the wave of a smartphone. Faster transaction times mean less waiting in line and happier customers. Fewer physical cards to carry around means the customer is less likely to lose one or have it stolen.

  Google has launched Google Wallet that supports MasterCard PayPass, PayPal offers money transfers between smartphones, and other companies are expected to follow suit. As the technology grows, more NFC compatible smartphones will be available and more stores will offer NFC card readers for customer convenience.

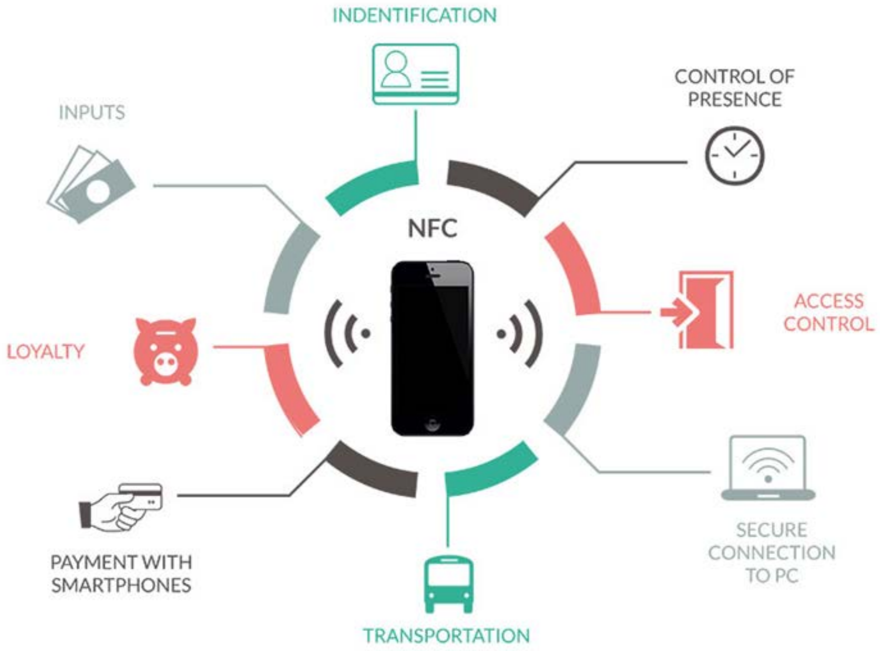


Figure 4: Uses of NFC technology

- **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. 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.

  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 home 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. 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.

3.4 Comparison between Wired and Wireless

SPECIFICATIONS	WIRED NETWORK	WIRELESS NETWORK
Speed of operation	Higher	Lower compared to wired networks but advanced wireless technologies that can make possible to achieve speed equivalent to wired network.
System Bandwidth	High	Low, as frequency spectrum is very scarse resource.
Cost	Less as cables are not expensive.	More as wireless subscriber stations, wireless routers, wireless access points and adapters are expensive.
Installation	Wired network installation is cumbersome and it requires more time	Wireless network installation is easy
Mobility	Limited, as it operates in the area covered by connected systems with the wired network	Not limited, as it operates in the entire wireless network coverage.
Transmission medium	Copper wires, Optical fiber cables, Ethernet	EM waves or radiowaves or infrared
Network coverage extension	Requires hubs and switches for network coverage limit extension	More area is covered by wireless base stations which are connected to one another
Applications	LAN(Ethernet), MAN	WLAN, WPAN (Zigbee,Bluetooth), Infrared
Channel interference and signal power loss	Interference is less as one wired network will not affect the other	Interference is higher due to obstacles between wireless transmitter and receiver (weather conditions, reflection from walls, etc.)
QoS (Quality of Service)	Better	Poor due to delay in connection setup
Reliability	High compared to wireless counterpart, as manufactured cables have higher performance due to existence of wired technology since years	Reasonably high. This is due to failure of router will affect the entire network

Wireless connectivity is just a substitute for cabled connectivity. Wireless does not and technically cannot provide the theoretical bandwidth of a physical cable connection. However, wireless can provide mobility and is an excellent option for connectivity in older buildings where pathways for cable may not be available. The wireless technologies, probably most useful for smart buildings technology systems include Wi-Fi and an emerging technology, Zigbee.

Both Wired and Wireless networks are very common in the workplace as well as in the home. Technology has been created to store, transmit and receive data through networks at very high rates of speed. Networks have become essential to completing daily business tasks and most business, those who rely heavily on information technologies, would be crippled without their networks.

Advances in networking storage have allowed for organizations to use their networks, not only for the sharing of resources but also for storing data to be used for data analysis. In the future, the speed of networks will increase as they have in past years. The cost of networks will continue to decline and using a network will be essential for every organization. As computing technology increases in power, and decreases in size, the price of creating a high-powered full featured network will rapidly decrease.

4. Smart home applications

A smart home can include several interfaces between the resident and the system. The units must be simple to understand and to use and they must endure the use they are designed for. Remote controls should, for instance, survive being dropped on the floor, impacts and vapor. In addition, they should be of a good design, well fitting into the flat.

Staff are receiving the alarms and messages from the system, they check on the situation and then sign out the alarm. There are several possible solutions for the transmitting of alarms. The transmittances must be reliable, be simple to read and easy to sign out the messages.

In this chapter the applications offered by the smart home system are illustrated.

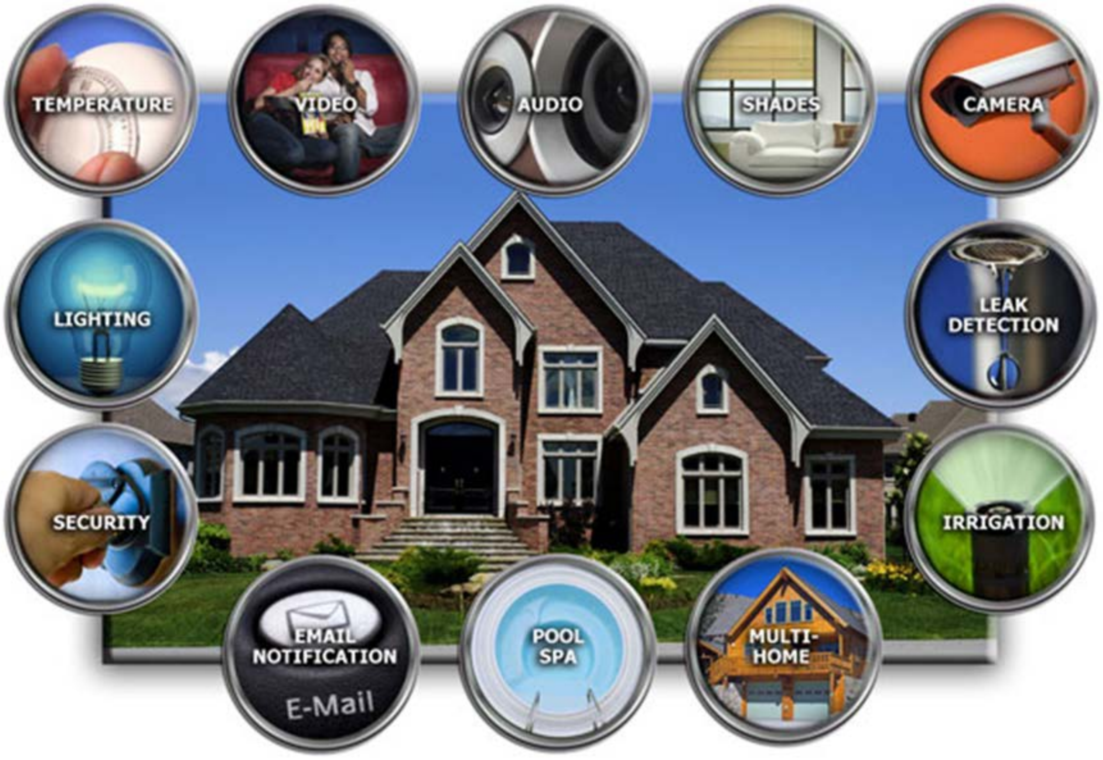


Figure 5: Smart Home Services

Light control

It intelligently controls the behavior of the lights according to the presence of the inhabitants. As example, when a person enters a room in the daytime, the system will open the drapes instead of turning on the lights, but at night it would make sure the lights came on and they turned off when no one is in the room hence waste of energy can be reserved. Additionally, if a kid’s movie is ordered in a Smart Home, the lighting could automatically be set at medium with shutters open, but for a horror movie, shutters would be lowered and all lights extinguished.

Figure 7: Control via the tablet

Daylight harvesting

Photoelectric controls are designed to strategically use daylight to reduce the need for artificial lighting, a process called “daylight harvesting.” They may be located in perimeter offices, atriums, hallways or in areas with skylights. Ambient light sensors measure natural and ambient light then based on the amount of natural light, adjust the lighting to maintain a constant light level. In some spaces manual or automatic blinds, or other means of reducing the direct solar exposure glare, excessive light levels, and heat gain, can be used to supplement photoelectric controls. These may include motorized window shades or blackout shutters. Proper daylight-harvesting design not only includes providing adequate daylight to an area but does so without undesirable side effects such as heat gain and glare. Successful daylight-harvesting designs will incorporate shading devices to reduce glare and excess contrast. Window size and spacing, glass type, and the reflectance of interior finishes must be taken into account as well. Despite all of these design considerations, daylight harvesting provides little benefit without an integrated electric lighting system due to the increased thermal loads from the sun. The electric lighting and thermal loads must be reduced while simultaneously increasing daylight to an area.

HVAC control

HVAC control includes A/C control, that automatically switches on the AC or increase the cooling intensity specified duration before the scheduled workers arrive to the unit, reduces the cooling level or switches off the AC when the unit is unattended and control the cooling level based on the temperature level inside the unit. Automated ventilation system, which will be switched on to replenish clean air based on temperature, moisture, smoke, heat, dust, or carbon dioxide level in the unit.

HVAC systems must control variable conditions of the system and its components.

These conditions include liquid and gas pressure, temperature, humidity, the flow rate of liquids and gases and the speed and on/off state of mechanical equipment.

A number of instruments and terminal devices available in the field are used to gather data on the system and assist in controlling it. System controllers use input and data from sensor devices to make decisions about the system, and then, based on the input information, control actuator devices.

Sensors and transmitters include thermostats, liquid differential-pressure transmitters for pumps and chillers, differential pressure sensors for fluids and airflow, static pressure sensors, air-pressure sensors, and humidity sensors.

An example of an actuator or operator is an actuator for a damper that is mounted to the damper shaft and triggers the start of the damper operation.

That operation could be a temperature sensor detecting a high temperature and sending a signal to the controller, which results in the controller sending a signal to an actuator to engage a motor that opens or closes a damper or vent.

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 way. They could be controlled easily from any place in the house by switching them ON or OFF from rooms in the house. The remote control and monitoring of these appliances can be performed remotely via the Internet or GSM mobile phones. Furthermore, some machines 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 are introducing appliances that communicate with objects using RFID. 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.

Safety and Security

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. In case of an alarm, both the home owner and the security company will be informed about the existence 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.

Connecting consumers' security systems to the network has many advantages. It is possible to remotely monitor their home settings and send notifications by SMS or email of any security breaches. Home events such as movement detection, doors opening or power outages can also be stored locally or in the cloud. An electronic portal allows consumers' doors to be locked or unlocked remotely. The same platform can also be used to detect gas or water leaks, using sensors that trigger an alarm in the event of abnormal gas or water consumption. This enables users to take actions remotely if they are on holiday or handle a contingent situation promptly. For example in case of fire, smoke detectors, using specific radio protocols, would enable the consumer to be notified remotely when smoke is detected and then connect to a webcam to check the home or alert the fire service.

Telemedicine

Services that provide health and social care directly to users in their own homes in an area of care defined as telecare, which uses interactive video and audio contact between a user and care provider. Peripheral devices can also be attached to computers to aid in an interactive examination, and video-conferencing can be used when face to face consultation is necessary. The "real-time" consultation, diagnosis, treatment and delivery of medical care is carried out with the user in the home, eliminating the need for frail or homebound individuals to travel to health care offices or facilities. "Store and forward" electronic information-processing technologies transmit medical and health information, x-rays and the data between health care providers and patients and among a patient's multiple health care providers, for more efficient and accurate record-keeping on diagnosis and treatments.

5. Communication Protocols

Just like other electronic systems, smart devices all run on a variety of different protocols. They are sets of rules and standards for communication between electronic devices. They are like languages, for example if one device speaks only ZigBee and another speaks only Z-Wave, they won't be able to communicate with each other. Ideally, in a smart home the devices must speak the same language or the user has to use products that are multilingual.

Furthermore, some of smart home network standard can work using both wiring system and wireless system. An example of wireless communication system for smart home is Z-wave, which is a reliable and affordable wireless home automation solution. Z-wave is a wireless RF-based method for instant remote control of appliances.

a. OpenHAB

OpenHAB is a mature, open source home automation platform that runs on a variety of hardware and is protocol agnostic, meaning it can connect to nearly any home automation hardware on the market today.

The openHAB runtime is a set of OSGi (Open Services Gateway initiative) deployed on an OSGi framework. It is therefore a pure JAVA solution and needs a JVM (Java Virtual Machine) to run. It provides a highly modular architecture, which even allows adding and removing functionality during runtime without stopping the service.

b. C-Bus

C-Bus is a proprietary protocol created by Clipsal for use with its brand of home automation and building lighting control system. C-Bus requires Ethernet-network likeCat 5 Unshielded Twisted Pair (UTP) cables, though a two-way wireless version also exists. This system is primarily used in Australia (e.g. Sydney Opera House) and in Asia, but it is becoming more known in Europe as well.

c. CEBus

CEBus, the Consumer Electronic Bus (CEBus) protocol, also known as EIA-600, is by some considered the US standard for home networking. It was first released in 1992 with the intent of expanding the capability of X10. It is an open architecture and is outlined by a set of specification documents which define details for communicating through power lines, twisted-pair cables, wireless, and other media.

d. INSTEON

INSTEON derives directly from X10, for which is backward compatible. It is a proprietary protocol developed by SmartLabs, Inc. It offers two-way communication where the controlled devices also function as repeaters for the messages to increase reliability. If the message isn't getting through on one platform, it will try the other. Instead of routing the message, an Insteon device will broadcast the message, and all devices pick up the message and broadcast it until the command is performed. The devices act like peers, as opposed to one serving as an instigator and another as a receptor. This means that the more Insteon devices are installed on a network, the stronger the message will be. Insteon operates in 904 MHz range, which allows 38.4 kbps data rate using FSK modulation.

e. KONNEX

Konnex (KNX) is a standard (EN 50090, ISO/IEC 14543), OSI-based network communications protocol for home automation. It is the result of a convergence of three existing European standards: the European Home Systems Protocol (EHS), BatiBUS, and the European Installation Bus (EIB). In contrast with other similar technologies, KNX defines several possible physical communication media and it is designed to be independent of any particular hardware platform. The KNX standard is administered by the Konnex Association.

f. BACNet

BACnet is an acronym for Building Automation and Control Networks. This international data communication protocol was first published in 1996, and was developed and is maintained by the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE).

BACnet provides a standard for representing the functions and operations of building automation and control devices. For example, the protocol covers how to request a value from a humidity sensor or send a pump status alarm.

For each type of building automation and control device, a standard software object is created that contains the identifier and properties of such a device reflecting the functions and operation of the device. Some of these properties may be inherent or required properties of the device, while other properties may be optional features of the device. The essence of BACnet is to move away from proprietary communications to similar devices by different manufacturers and treat communications and control of like-devices in a standard common way.

This approach and structure allow BACnet to be used in HVAC, lighting systems, fire alarm systems, and other building automation systems. In addition to standardization of the device objects, BACnet also defines the message types between a server and a client. These messages are called “service requests” and the BACnet standard defines 35 message types that are divided into five groups or classes. The latter involves messages for the following:

1. Accessing and manipulating the properties of the objects
2. Alarms and events
3. File uploading and downloading
4. Managing the operation of remote devices
5. Virtual terminal functions

BACnet can communicate over several types of networks, including Ethernet, ARCNET, MS/TP (master-slave/token-passing), and PTP (point-to-point) for use over phone lines or hardwired EIA-232 connections.

g. LonWorks

LonWorks (local operating network), is often referred to as a communications protocol for control networks, but as it bundles a communications protocol with a dedicated microprocessor and media transceivers, it more closely resembles a networking platform. LonWorks was created by the Echelon Corporation for networking devices over media such as twisted pair, powerlines, fiber optics, and RF.

In 1999, the communications protocol (then known as LonTalk) was submitted and accepted as a standard for control networking (ANSI/CEA-709.1-B). In 2009, LonWorks became an international standard, ISO/IEC 14908. Whereas LonTalk addresses the issue of how devices communicate, LonWorks defines the content and structure of the information that is communicated.

The protocol is primarily focused on building and home automation, but is also used in transportation and industrial automation. The standard calls for two primary physical-layer signaling technologies; twisted-pair cable and a power line carrier, although LonWorks can also use radio frequency (RF), infrared (IR), coaxial cable and fiber optic cable. The LonWorks platform uses an affiliated IP tunneling standard—ANSI/CEA-852—in use by a number of manufacturers to connect the devices on LonWorks-based networks to IP networks and applications. Many LonWorks networks are deployed with some IP network integration.

h. MODBUS

Modbus is a communications protocol published by Modicon in 1979. At that time Modbus primarily focused on communication to programmable logic controllers (PLCs) manufactured by Modicon and used in industrial automation.

Modicon is currently a company owned by Schneider Electric and in 2004 the Modbus standard was transferred to a nonprofit organization, Modbus-IDA, whose members are primarily users and suppliers in the automation industry.

Modbus is an application-layer messaging protocol for client–server communication between devices connected on different types of buses or networks. It can be implemented over an Ethernet network as an asynchronous serial transmission such as RS-232 or RS-485, or as a high-speed, token-passing network call Modbus Plus. For Ethernet and Modbus Plus the message created by the Modbus protocol is "tunneled" or imbedded into the frame or packet structure that is used on an Ethernet or token-passing network.

The most common implementation of Modbus uses the serial RS-485 physical layer with either Modbus RTU (a binary representation of the data) or Modbus ASCII (human readable). The Ethernet implementation option uses Modbus/TCP.

Modbus, like other communication protocols, defines a message structure and format for message fields; how a controller requests access to another device, how to respond to requests, how errors will be detected and reported, how to identify devices, how to recognize a message to a device, and so on.

Modbus versions have different functionality. For example, the basic Modbus protocol is a master–slave arrangement that does not provide for a "slave" device to report to the master unless it is polled by the master. In the Modbus implementation over Ethernet, Modbus/TP devices can report to a master. Typical Modbus implementations are limited to 247 devices, although in a Modbus/TP implementation, no such limit exists.

Modbus is a simple yet effective protocol. Typical problems that the designers have to overcome include high latency and timing problems.

i. UDP (User Datagram Protocol)

UDP is a connectionless transport layer protocol: each output operation by an application produces exactly one UDP datagram, which in turn causes one IP datagram to be sent. This is different from a stream oriented protocol such as TCP (see below), where the amount of data written by an application has little to do with what actually gets sent in a single IP(Internet Protocol) datagram. The UDP layer is responsible for communicating between two applications within two host computers; each application has a 16 bit port number assigned to it. There are reserved port number for various applications. On the other hand, the IP layer only provides communication between the two host computers, and there can be multiple applications running on each computer. UDP provides no reliability: it sends the datagrams that the application writes to the IP layer, but there is no guarantee that they ever reach their destination.

j. UPB (Universal Powerline Bus)

UPB is a protocol for communication between devices used for home automation. It uses power line wiring for signaling and control.

UPB was developed by PCS (Powerline Systems of Northridge, California) and released in 1999. Based on the concept of the ubiquitous X10 standard, UPB has an improved transmission rate and higher reliability. While X10 without sociality firewalls has a reported reliability of 70-80%, UPB reportedly has a reliability of more than 99%.

The UPB communication method consists of a series of precisely timed electrical pulses –called UPB Pulses- that are superimposed on the normal AC power sine wave. Receiving UPB devices can easily detect and analyze the UPB Pulses and extract the encoded digital information from them.

k. TCP/IP (Transmission Control Protocol/Internet Protocol)

TCP/IP is the suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TSP and IP. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks. Even network operating systems that have their own protocols, such as Netware, also support TCP/IP.

It is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network. When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

l. X10

X10 was the first general-purpose home network solution. PICO Electronic, a UK-based engineering firm, patented it in 1978. After a first unsuccessful attempt to market it in Europe, the company established itself in the US, where it was more successful. The RadioShack, the US-based chain of electronics retail store, was the first to offer consumer solutions based on this technology.

X10 is a Powerline system, so uses the existing electrical network in the house and can allow users to remotely control, at least in principle, any appliance connected to the house mains. A controlling device would just be plugged in between the mains and the electrical appliance to be controlled. Properly instructed, this controlling device will then turn the appliance on or off at specific times or as a response to specific events coming from the home network. The original implementation allows one-way communication and can address up to 256 devices subdivided into eight different “homes” (channels) to lessen the chances of interferences with other systems nearby. The X10 signal is sent when the voltage value crosses zero, which happens twice at every current cycle. Virtually all other Powerline home communication protocols use a variation of this method.

In spite of its limitations, and thanks to the low installation costs and its ease of use, X10 is still widely used today by DIY enthusiasts, especially in the US, where a multitude of off-the-shelf components are readily available. However, due to the differences between the US (120V/60HZ) and European (220V/50HZ) power lines, devices built for the US market will not work in Europe.

In more recent years, this technology made a comeback due to the fact that the patent for the protocol expired in late 1990s, and several forums on the Internet now can provide resources for anyone interested in investigating this technology.

A wireless version of this protocol which offers limited two-way communication seem to exist but, besides being called X10, it might have little to do with the original Powerline technology. After the original idea first implemented by X10, several other protocols have emerged using the same concepts, sometimes enhancing the original specifications, such as implementing two-way communication, providing support for more devices and different types of media. The communication protocols listed below are an example of the most known.

The genesis of many smart home products was in 1975, when a company in Scotland developed X10. X10 allows compatible products to talk to each other over the already existing electrical wires of a home. All the appliances and devices are receivers, and the means of controlling the system, such as remote controls or keypads, are transmitters. If you want to turn off a lamp in another room, the transmitter will issue a message in numerical code that includes the following:

- An alert to the system that it's issuing a command,
- An identifying unit number for the device that should receive the command and
- A code that contains the actual command, such as "turn off."

All of this is designed to happen in less than a second, but X10 does have some limitations. Communicating over electrical lines is not always reliable because the lines get "noisy" from powering other devices. An X10 device could interpret electronic interference as a command and react, or it might not receive the command at all.

While X10 devices are still around, other technologies have emerged to compete for your home networking dollar. Instead of going through the power lines, many new systems use radio waves to communicate.

Two of the most prominent radio networks in home automation are ZigBee and Z-Wave. Both of these technologies are mesh networks, meaning there's more than one way for the message to get to its destination.

m. 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 layers 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 addresses are stored and sent using 16 bit or 64 bit numbers, which limit the network size to 264 devices.

IEEE 802.15.4 standard defines Star, Cluster Tree and Mesh networks as possible topologies for the wireless network as shown in *Figure 8.*

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.

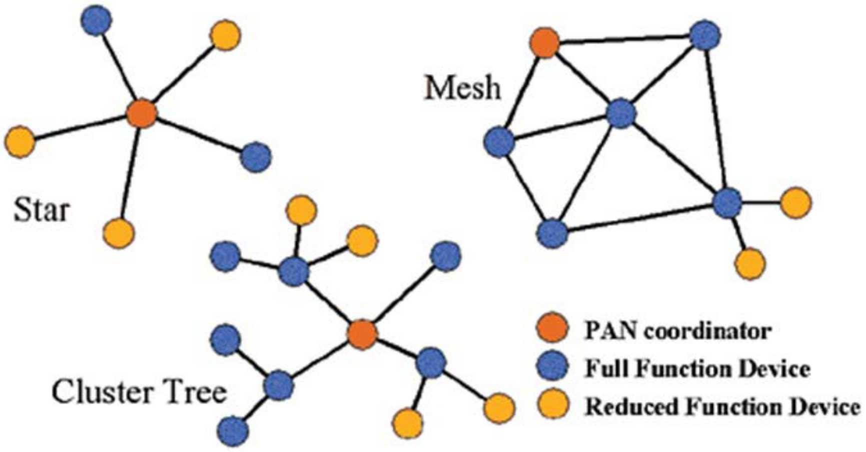


Figure 8: Networks of IEEE802.15.4 standard

ZigBee's name illustrates the mesh networking concept because messages from the transmitter zigzag like bees, looking for the best path to the receiver. While Z-Wave uses a proprietary technology for operating its system, ZigBee's platform is based on the standard set by the Institute for Electrical and Electronics Engineers (IEEE) for wireless personal networks. This means any company can build a ZigBee-compatible product without paying licensing fees for the technology behind it, which may eventually give ZigBee an advantage in the marketplace. Like Z-Wave, ZigBee has fully functional devices (or those that route the message) and reduced function devices (or those that don't).

Today, ZigBee is used by a variety of cable and telecommunication companies including Comcast, Time Warner Cable, EchoStar, DirecTV, Charter, Rogers, Deutsche Telekom, Videocon. These companies are using ZigBee in their set-top boxes, satellite transceivers and home gateways to deliver home monitoring and energy management solutions to their customers.

ZigBee is also available in products from retailers around the world enabling the do-it-yourself-er to easily install and create their own smart home to improve their comfort and efficiency.

n. Z-Wave

Similarly to ZigBee, Z-Wave is a communications standard based on wireless communication. The technology is developed and maintained by Zensys, a Denmark-based company. The Z-Wave Alliance is an international consortium of manufacturers that oversees interoperability between Z-Wave products and enabled devices. This protocol is a mesh networking technology where each node or device on the network capable of sending and receiving control commands. Devices can work as stand alone or in groups, and can be programmed into sequences (called “scenes” or “events”) that trigger multiple devices, either automatically or via remote control.

Z-Wave uses a Source Routing Algorithm to determine the fastest route for messages. Each Z-Wave device is embedded with a code, and when the device is plugged into the system, the network controller recognizes the code, determines its location and adds it to the network. When a command comes through, the controller uses the algorithm to determine how the message should be sent. Because this routing can take up a lot of memory on a network, Z-Wave has developed a hierarchy between devices: Some controllers initiate messages, and some are "slaves," which means they can only carry and respond to messages.

It mainly operates in 868 MHz (Europe), 908 MHz (United States), and 921.42MHz (Australia) bands and latest version of Z-Wave (400 series) supports the 2.4 GHz. These bands allow 9.6, 40 and 200 Kb/s data rates respectively using Frequency Shift Keying (FSK) modulation schemes.

o. OPC

OPC is somewhat of an acronym embedded in an acronym. OPC stands for “OLE for process control”; in turn, OLE stands for “object linking and embedding.” OPC is based on Microsoft’s OLE/COM technology which essentially allows Windows programs to communicate with hardware devices.

OPC operates in a client–server approach. The OPC server converts the communications protocol of a hardware device into the OPC protocol.

The OPC client software uses the OPC server to obtain data or send commands to the hardware device. The OPC client software, typically a human–machine interface (HMI), allows the client to communicate to the hardware device.

OPC is an open standard. Software vendors simply include OPC client capabilities in their products and they become compatible with hardware devices.

An OPC server has subsystems addressing functions such as data access, alarms and events, and historical data. The OPC server can interact with other applications such as Microsoft Excel, a web browser, or any ODBC database.

One analogy to an OPC configuration may be the use of printer drivers on PCs. Rather than have each application on a PC have a driver for a printer, one driver is used for all applications. This eliminates duplication, inconsistencies and conflicts.

6. Conclusion

The smart home market is still immature with arguments still continuing as to whether the business and domestic markets are one or separate and it has been subjected to 'technology push' so that there is transference between these two applications.

In the domestic market, consumers are still skeptical about potential benefits, technologies are difficult to integrate for interoperability, and it is difficult for the consumer to get good service and advice. Conflicting standards have contributed to this lack of progress and although smart home technology (or variants of it) could have a wide mass consumer market, those not interested in living in a smart home are most likely to be aged 55 and over, although these same people do want safety and security in their homes.

As well as the general consumer markets there is potential for using technology to support people with special needs by maintaining and supporting them in independent living. However, care professionals still do not know that the technology exists and we know that it is not sufficient to just provide information; infrastructure has to be in place to support its use. What is needed is a 'whole system approach' to ensure that the technology is integrated into a wider care package and that it is being appropriately and ethically used. Funding is also likely to be a problem as it involved multi-agencies and costs cover not only the equipment and its installation and maintenance but also the support infrastructures that underpin it.

As long as the future of the smart home market is concerned, this study helps us understand by graphical and predictive analyses how the smart home market will evolve in the next five years in North America and Europe.

North America recorded strong growth in the smart home market during the last several years. The installed base of smart home systems in the region increased by 75 percent to reach 10.2 million at the end of 2014. An estimated 1.8 million of these were point solutions designed for one specific function. As some homes have more than one smart system in use, the installed base totaled an estimated 7.9 million smart homes at the end of the year. This corresponds to 6% of all households placing North America as the most advanced smart home market in the world. Between 2014 and 2019, the number of households that have adopted smart home systems is forecasted to grow at a compound annual growth rate (CAGR) of 37%, resulting in 38.2 million smart homes. Market revenues reached US$ 42 billion (€3.2 billion) in 2014, an increase of 48 percent between 2014 and 2019, reaching US$ 18.2 billion (€13.7 billion) in yearly revenues at the end of the forecast period.

The European market for smart home systems is still in an early stage and 2-3 years behind North America in terms of penetration and market maturity. At the end of 2014 there were a total of 3.3 million smart home systems in use in the EU28+2 countries, up from 1.75 million in the previous year. Around 0.34 million of these systems were multifunction or whole-home systems whereas 2.93 million were point solutions. This corresponds to around 2.7 million smart homes when overlaps are taken into account, meaning that 1.2% of all households in the region were smart at the end of the year. The number of European households that have adopted smart home systems if forecasted to grow at a compound annual growth rate (CAGR) of 61% during the next five years, resulting in 29.7 million smart homes by 2019. Market revenues grew by 60% to €0.77 billion (US$ 1 billion) in 2014. The market is forecasted to grow at a CAGR of 58% between 2014 and 2019 to reach €7.6 billion (US$10.2 billion) at the end of the forecast period. The number of smart homes is depicted in *Figure 9.*

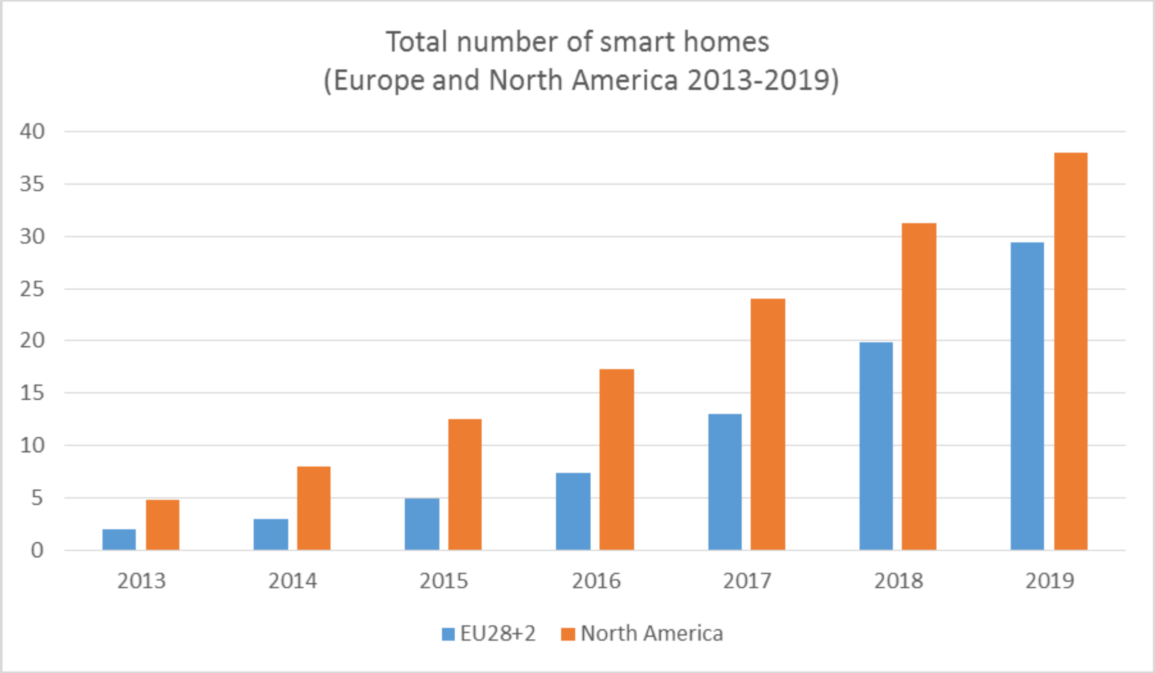


Figure 9: Smart homes in Europe and North America

7. Resources

1. Toril Laberg, Haakon Aspelund, Hilde Thygesen: "*Smart Home Technology Planning and management in municipal services", Oslo 2005*
2. M2M Research Series www.berginsight.com *Smart homes and home automation*
3. Paolo Carner, "*Project Domus: Designing Effective Smart Home Systems"*, 2009
4. M.R. Alam, M. Bin Ibne Reaz, Mohd Alauddin Mohd Ali, *"A Review of Smart Homes-Past, Present and Future", 2006*
5. Antonio Scotto DiCarlo, *Smart Homes*
6. Nazmiye Balta-Ozkan, Benjamin Boteler, Oscar Amerighi: "*Energy Research & Social Science"* 3 (2014) 65-77
7. A.J. Bernheim Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, C. Dixon: "*Home Automation in the Wild: Challenges and Opportunities"*, 2011
8. *Report Internet of Things Research Study, 2014*
9. Digital Trends *"What the heck are Zigbee, Z-Wave and INSTEON?Home automation standards explained"* by Drew Prindle, 2014
10. International Journal of Advanced Science and Technology Vol. 15, Rosslin John Robles, Tai-hoon Kim *"Applications, Systems and Methods in Smart Home Technology:A Review",* 2010
11. I. Colak, G.Fulli. S.Sagiroglu, M.Yesilbudak, C-F. Covrig "*Smart grid projects in Europe: Current status, maturity and future scenarios", 2015*
12. A.J. Dinusha Rathnayaka, Vidyasagar M. Potdar, Samitha J. Kuruppu *"Evaluation of Wireless Home Automation Technologies", 2011*
13. International Journal of Computer Engineering & Technology(IJCET) *"Smart Home Systems using Wireless sensor network- A comparative analysis" vol 3, 2012*
14. Lionel Gremeau *"Service Providers & Smart home", 2012*
15. M. Sripan, X.Lin, P.Petchlorlean, M.Ketcham *"Research and Thinking of Smart Home Technology", 2012*
16. Ebook: "*Build Your Own Smart Home"* by Robert C. Elsenpeter, Toby J. Velte, 2003
17. Ebook*: "Smart Building Systems for Architects, Owners and Builders"* by James Sinopoli, 2010
18. Ebook: *"Smart home Systems"* by P.Lalanda, J.Bourcier, J.Bardin, S.Chollet, 2010
19. www.nfc-forum.org
20. www.sengpielaudio.com /calculator-period

21. Frequency - diracdelta.co.uk
22. www.telcomhistory.org
23. Ebook: *“Integrated Wireless Technologies for Smart Home Applications”* Mahmoud A. Al Qutayri and Jeedella S. Jeedella Khalifa University of Science, Technology and Research U.A.E.
24. Roger L. Freeman *“Fundamentals of Telecommunications”*