Department of

Electrical and Computer Engineering

A Novel Three Stage NetworkJoining Protocol for Home Automation

A thesis submitted in fulfilment of the requirements for the degree of Master of Engineering

Salma Nasrin

College of Science, Engineering and Health

RMIT University

June 2017

Declaration

I certify that except where due acknowledgement has been made, the work is that of the author alone; the work has not been submitted previously, in whole or in part, to qualify for any other academic award; the content of the thesis is the result of work which has been carried out since the official commencement date of the approved research programme; and, any editorial work, paid or unpaid, carried out by a third party is acknowledged**.**

Name: Salma Nasrin

Date: 07/06/2017

Acknowledgements

Firstly, I would like to express my sincere gratitude to my advisor Dr. Peter John Radcliffe for the continuous support of my higher degree study and related research, for his patience, motivation, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my master's study.

Dr Jidong Wang, my co-supervisor, has helped me immensely at some critical moments of the research activity; my grateful thanks to him.Thanks also to all the staff in School of Electrical and Computer Engineering at RMIT for their professional jobs.

I would like to acknowledge the support I have received for my research through the provision of an Australian Government Research Training Program Scholarship.

Last but not the least, I would like to thank my family: my parents and to my husband, my son, brothers and sister for supporting me spiritually throughout writing this thesis and my life in general.

Abstract

Modern advances in electronics and communication technology have given rise to the development of several home automation technologies and systems. Current home automation systems have several drawbacks including high cost, not being of a Do It Yourself (DIY) nature, and there is currently no safe way for a simple Internet of Things (IoT) device to join a Local Area Network (LAN) without the addition of extra user interface hardware. The simplest IoT devices, for example a mains power switch, could contain just a cheap Wi-Fi interface and very limited computing capability. Such devices are already available for under US $4 but are not usable in the IoT context as they lack the ability to join a Wi-Fi network in a secure DIY manner. The ability to securely join IoT Devices to Wi-Fi networks is an on-going area of research. This thesis describes a novel three-stage network joining protocol, which that allows IoT devices to securely join a Wi-Fi network even if they completely lack a user interface. This protocol can eliminate a central controller for a home automation system and allow users to purchase off the shelf devices from a range of manufactures and control them by a PC or mobile device in a very simple manner. This new method will significantly reduce costs as the system and does not require expert configuration or a central controller. This in turn may help revitalize the home automation industry, which has not seen great penetration into suburban homes. The protocol is implemented using a WPA2 based LAN, an Android phone and a Raspberry Pi which represents an IoT device lacking any form of keyboard and display. The method allows cost reductions for simple IoT devices and is suitable for immediate adoption by manufacturers of IoT devices.

KEY WORDS: Home Automation, Network Joining Protocol, Internet of Things (IoT), Local area network (LAN), Raspberry Pi.

The ideas above have been the basis of two papers as listed below-

S. Nasrin and P. J. Radcliffe, "Novel Protocol Enables DIY Home Automation," in *Telecommunication Networks and Applications Conference (ATNAC)*, 2014.

S. Nasrin and P.J.Radcliffe, "A Novel Three Stage Network Joining Protocol for Internet of Things based Home Automation Systems", Computer Communication & Collaboration, 2016.

TABLE OFCONTENTS

List of Figures

Abbreviation

Abbreviation	Name of Abbreviation
IoT	Internet of things
LAN	Local area network
PC	Personal computer
SSID	Service Set Identifier
Wi-Fi	Wireless fidelity
LED	Light Emitting diode
DIY	Do-It-Yourself
LCD	Liquid Crystal Display
HD	High Definition Video
XML	Extensible Mark-up language
WPA2	Wi-Fi Protected Access2
NFC	Near field Communication
RFID	Radio Frequency Identification
AP	Access Point
MAC	Media access control Address
GUI	Graphical User Interface
DDC	Device Discovery Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
DHCP	Dynamic Host Configuration Protocol

Chapter1: Introduction

1.1 Research Background

The Internet of Things (IoT) is rapidly gaining interest in the world of Wireless telecommunications and also promises to be one of the major factors influencing the development of home and workplace technologies [1-2]. The aim of the IoT is to link the Internet with sensors and devices and so make possible a huge number of new and improved products and applications. IoT and home automation introduce new concepts and many development opportunities for the smart home [3-20]. The application of information communication technology has brought a huge change in modern life. The earlier 'Internet of computers' has been transformed into the 'Internet of people' by the introduction of social websites. The next move was mobile computing. The different generations of Internet connection have made it possible for faster accessibility accompanied by better quality. The further advancement of this technology is the 'Internet of Things' through which interoperability and intelligence can be achieved. The applications of IoT can be observed in number of areas such as the kitchen, agriculture, and health care. Home automation with the Internet of things (IoT) provides better flexibility in managing and controlling household objects and will support the interconnectivity of a large number of devices within a smart home and achieve better resource utilization. Though the concept of smart homes is an old research area, considerable new work has been carried out based on Internet of Things.The main theme of this research work is discovering how IoT devices may securely join a Wi-Fi network, but the economics of the network architecture are also very important.

Three categories of home automation architecture have been found in the literature. The first is the server based home automation architecture using an Internet based server or Java based server [21-23]. These architectures are user-friendly [21], allow joining of networks for an IoT device [22], and support a wide range of home devices [21-23].

A second category, the bridge-based architecture, uses another protocol to solve the "joining the network" problem and provide data communication, and finally bridges to Wi-Fi. ZigBee based systems [24-31] have been used to implement home automation network and consist of a coordinator, routers and several end devices.

The third category of architecture requires extra or enhanced hardware to achieve joining the Wi-Fi network. The only purpose of this extra /enhanced hardware is to join the network. The Nest based smart thermostat bought by Google [32-34] is one example of this type of home automation architecture. This device has a display unit and a rotary selector for data entry and selecting a Wi-Fi network to join.

1.2 Problem Statement

In the present day, home automation is becoming essential for improving our life. Home automation offers a futuristic way of life in which an individual gets to control their entire house using a smart phone, from turning on a TV to locking/unlocking doors. It also offers a more efficient use of energy.

Home automation has very poor penetration into the domestic market for several reasons. The first is that installation of a home automation system requires expensive experts. The second problem identified is that existing systems has no plug-n play capability, and very few systems allow a homeowner to install or add to the system in a DIY (Do It Yourself) manner. The third disadvantage was that nearly all of the system needs a central controller, which increases the cost of the system. Together these shortcomings make current home automation systems too expensive for most consumers. A significant amount of research has been conducted into modern home automation system. Currently Three main approaches have been seen in the design of home automation devices; they are Dedicated IO, Bridge and Central Controller.In Central controller requires a permanently powered central server or PCbeing connected and powered on constantly, which is an extra cost. Additionally users cannot configure the system by themselves thus also increasing cost [21-23]. This means that as a solution it is very expensive: Devices and central controllers are expensive, running costs are high and adjustments are difficult and costly.

Bridge-based system using additional hardware, translates between Wi-Fi and some other protocol, thus creating a bridge. ZigBee Alliance based Home automation system made up of many vendors who made products to work with IEEE 802.15. However, some users have noted that Zigbee devices may not be a useful for low cost IoT devices into the future.

Many researchers have been used additional IO devices and protocols on the automation device for securely joining the local network and controlling devices. Such an approach requires extra hardware and so increases costs. The IO protocols are different to Wi-Fi protocols, for example NFC and Bluetooth. Ina Dedicated IO based approach, an additional unique IO hardware is used for the purpose of securely joining the local network. For example implemented NFC Tags in devices that users could tap their NFC-enabled smart phones against to send control information, but the actual data transmission was still be accepted over traditional network structures.

All the available systems described above are expensive and may require experts to install or modify the system, which is another large expense. Many of the existing systems require a personal computer to be permanently active and there is no suitable way to easily connect to an IoT device, which lacks input devices such as a keyboard and display. Few of the existing systems allow a homeowner to safely install or add to the system in a DIY (Do It Yourself) manner. Moreover, all the Internet of Things and home automation in general has one significant problem- it has very poor penetration into the average domestic home. It is not possible to buy IoT devices at the typical local hardware store. If IoT devices made cheaper and be setup by the average homeowner in a secure manner then the home automation market could be very much bigger. If such a system were possible then costs to the consumer would drop and home automation may become much more affordable and popular.

1.3Research Objectives

- To develop a new secure network joining protocol for home automation architecture
- To implement and test the secure network joining protocol to prove DIY style IoT devices may safely join a home LAN.

1.4Thesis Outline

The rest of this thesis is organized as follows.

- Chapter 2 gives an overview of existing home automation systems and commercial products available. Current home automation technologies are also reviewed and compared.
- Chapter 3 provides research questions that drive the work in this thesis.
- Chapter 4 proposes a new home automation architecture that uses no central controller, bridging hardware, or extra hardware for the purposes of joining a home Wi-Fi network.
- Chapter 5proposes a novel three-stage network joining protocol by which an IoT device can securely join local Wi-Fi network of proposed home automation system in chapter 3.
- Chapter 6 describes the implementation and testing of the proposed new protocol by laboratory experimentation.
- Chapter 7discusses the details results of the implementation protocol and limitations and /or problems encountered during the period of the project
- Chapter 8proposesfuture research required to enable the full DIY paradigm to be successful
- Finally, chapter 9 provides conclusions to this thesis.

Chapter2: Literature Review

2.1 Internet of Things

The concept of the Internet of Things [35] was introduced in proposal by Kevin Ashton in 1999. He saw the original Internet as the Internet of computers. Each computer was connected and allowed to transfer data back and forth. When the Internet users started to grow and social media sites gained popularity, it became an era of the Internet of People. Countless websites and apps (Face book, Instagram, and Twitter just being the biggest examples) were developed and used by a large percentage of the population to stay connected. So now that every device and every person is connected via the Internet. The next logical step is to start connecting things.

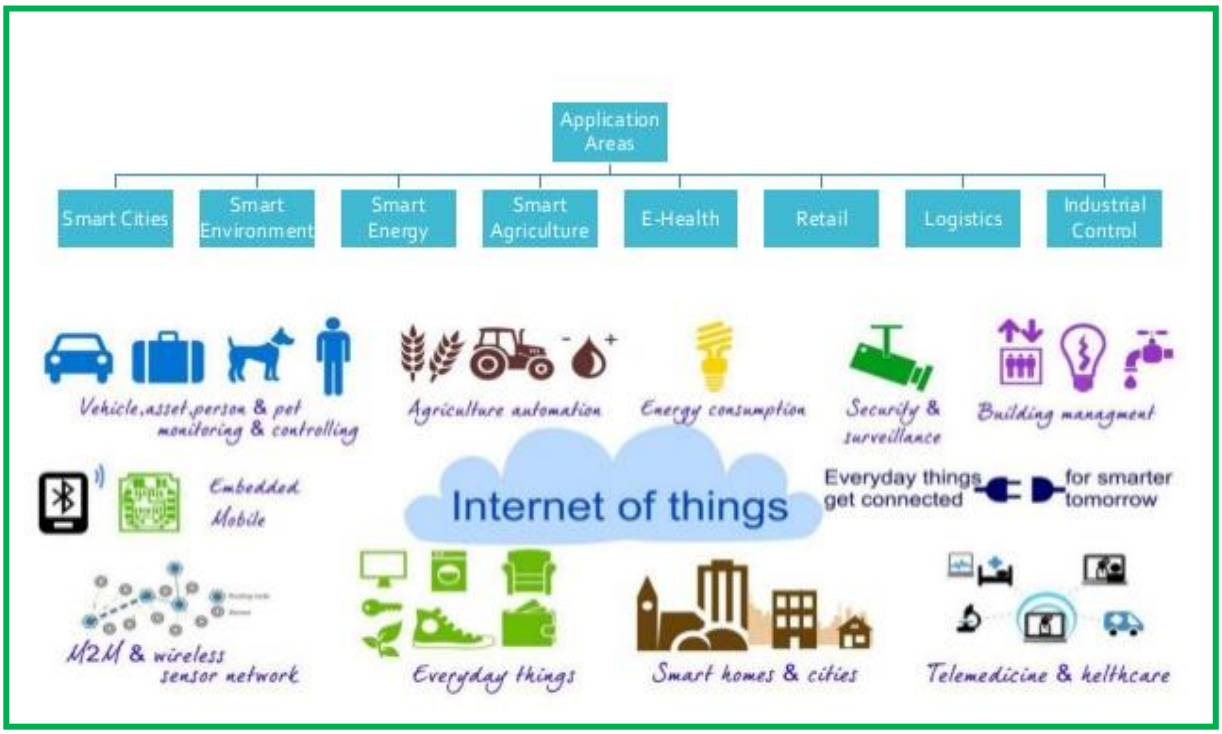

Figure 2.1: Branches of possibilities stemming from the Internet of Things [36]

With quickly advancing technology, the Internet of Things has the "ability to provide smarter services to the environment as more data becomes available" [6]. There are boundless possibilities to what can be done with the Internet of Things as can be seen in Figure 1.

2.2 Home Automation and Internet of Things

IoT technology can also be applied to create new concepts and a wide development space for smart homes to provide intelligence, comfort and to improve the quality of life. It is instructive to compare the state of the Internet and Ethernet compared to home automation. We all expect to be able to buy an Ethernet card or Ethernet printer for a desktop from any manufacturer computer and it will just work. This has resulted in a very competitive market and low cost devices, which reduces the costs to the consumer and increases the size of the market. Home automation has no such heterogeneity or interoperability; one cannot choose devices from different manufacturers and expect them to work. The market place is fragmented with low manufacture volumes and high costs which ensures the home automatic market stays small.

To solve this problem there needs to be a home automation system which describes an architecture and protocols that will allow the home owner to purchase home automation devices just as they would an Ethernet printer, choose from any manufacturer, plug it in and it works. If this methodology is accepted as a standard then the home automation market may "take off" as manufacturing volumes will rise and costs will drop thus dramatically increasing the size of the home automation market

There are several applications of the Internet of Things which will impact our daily life. The applications can be classified based on the type of network availability, coverage, scale, heterogeneity, repeatability, user involvement and impact [6-20].

The applications can be categorized into four domains: (1) Personal and Home automation; (2) Enterprise; (3) Utilities; and (4) Mobile. The smart home has been of interest to

researchers over the last 30 years. Several studied this topic which has branched out into a wide variety of applications. According to the literature, the smart home will enable the management and control of different areas of a residence. Personal and Home IoT at the scale of an individual or home, Enterprise IoT at the scale of a community, Utility IoT at a national or regional scale and Mobile IoT which is usually spread across other domains mainly due to the nature of connectivity and scale. There is a huge crossover in applications and the use of data between domains. For instance, the Personal and Home IoT produces electricity usage data in the house and makes it available to the electricity (utility) company, which can in turn optimize the supply and demand in the Utility IoT. The Internet enables sharing of data between different service providers in a seamless manner creating multiple business opportunities.

2.3 Existing Product for Home automation

The Internet of Things is changing simple homes into smart homes, where everything from our lights to our door locks can be controlled from our smart phone. The following are some products that monitor and control everything from the thermostat on wall to the crock-pot on the kitchen counter -- right from smart phone. In this section, existing products are briefly introduced and the technologies, which they are based upon, and their security features are briefly discussed. The section conclusion summarizes problems with technologies.

2.3.1Belkin'sWeMo:

Belkin'sWeMo[36] home automation system can monitor and control WeMo-branded smart wall switches and plugs, LED light bulbs, motion sensors and lighting devices as shown in Fig. 2.2. It can be managed from desktop or Smartphone application through Belkin's free cloud service which requires Internet connectivity and there's no extra hub

required. The WeMo switch cost is US$39.99. Each WeMo device uses its own channel to link it to online services such as Gmail to trigger specific actions.

Figure 2.2: Belkin'sWeMo Home Automation [37]

2.3.2 Canary

The Canary home security system [37] contains an HD video camera with sensors for air quality, motion, sound, temperature and vibration in one unit as shown in Fig. 2.3. The system uses machine learning to determine normal activity in the home and sends alerts to the canary mobile app. if anything changes. The price of this product is US$199.

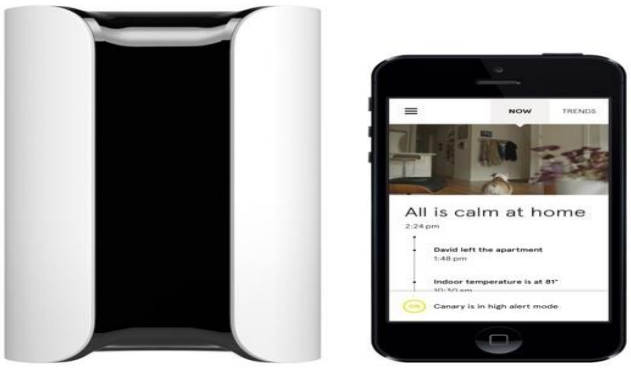

Figure 2.3: Canary Home security System [38]

2.3.3 Energy aware Technology Neurio:

Neurio puts a Wi-Fi-enabled sensor [38] shown in Fig.2.4 is placed inside a home's electrical panel and use power signatures to identify individual devices and appliances. It also uses machine learning to interpret that activities such as monitors power use, breaks down activity by device. The system is able to inform the users when something important happen, such as leaving the oven turned on. The Price of Neurio isUS$179.

Figure 2.4: Energy aware Technology Neurio[39]

2.3.4 Securifi Almond+

Almond [39] also serves, as a smart home monitoring is a wireless router/range extender. It controls the smart devices and appliances using the Zigbee, Z-Wave and Wi-Fi communications protocols.

Figure 2.5: Securifi Almond+ wireless router [40]

It offers a Smartphone app and browser-based control interface, with a touch screen colour LCD that functions as a master monitoring and control console, and is designed to be wall mountable. The price of that product is US$244.

2.3.5 Lowe's Iris

Lowe's [40] is another smart home monitoring and control system that supports a wide range of smart devices and appliances. Three different models of Lowes Iris is available in the market as below-

a) Safe and Secure start-up kit (US$149) that includes a hub, motion and contact sensors and a keypad;
b) Comfort and Control kit (US$249) that includes a smart thermostat and smart plug; and
c) Smart Kit (US$299) that includes all of the above plus a Wi-Fi range extender.

Figure 2.6: Lowe's smart home monitoring and control System [41]

2.3.6 Nest Product:

The Nest Thermostat[41] is a smart home automation system that is specially designed for controlling the home temperature from a smart phone, tablet or laptop.The Nest is simple to install and easy to adjust: turn the outer stainless-steel ring to the right to increase the temperature and left to turn it down. The ring also allows the user to tediously enter network SSIDs and passwords. The display is more complex than required to show the temperature in order to help the user join the Nest to the local area network. The Price of that product is US$230.00

Figure 2.7: Nest Thermostat System [41]

2.3.7 Smart phone Controlled Switch - Lazy Bone (Wi-Fi):

LazyBone [42] is a smart switch that can be controlled by mobile phone via Bluetooth or Wi-Fi. It is supporting both Android and iOS. It is mainly used to control a home's electrical equipment, such as light bulbs. However, by using the momentary mode, it can be used control a garage door. This Wi-Fi Lazy bone can also be set to Access Point (AP) mode. It can control other devices point to point even without a router. The cost of this product is $US29.50 to US$48.50.

Figure 2.8: Smart phone Controlled Switch - Lazy Bone (Wi-Fi)System[43]

2.3.8 Analysis of Existing Products:

Home automation products [36-42] make us aware of what is going on within our house and have the potential to put money back in our wallet that we would otherwise be spent on unnecessary and rising energy costs. All of the above IoT products available in the market are expensive, cost several hundred dollars for a full system, and few are really of a Do It Yourself (DIY) nature for the average householder. Installation can be difficult and may require experts to install the system, which adds the extra cost. Among the products available in market, Lazy bone at around US $30 is very cheap. It is a convenient and easy-to-use

product that can be used to control home's electrical equipment, such as light bulbs. However, it lacks strong security protocol thus a hacker can break the Wi-Fi security and get the LAN SSID and password.

2.4 Existing Protocols for Home automation

There is a wide variety of protocols, on which a smart home can be built [43-48]. Following is an overview of some of the most popular home technology protocols on the market.

2.4.1 X10

X10 [43] is not known for high speed or robust communication between units on the home automation network. The main advantages of this protocol include low cost, no new wiring is required, it is simple to install, and controls up to 256 lights and appliances, and time proven.

It has been around for over 30 years because X10 products talk over home's electrical wires they may have difficulties in two situations. The first is when there is an appliance running that generates noise onto the power line. Appliances that may cause problems are motors, light dimmers, and advanced electronics. The second issue with X10 is when the X10 transmitter is on one phase of our home's electrical wiring and the receiver is on another phase. A special bridge needs to be installed to allow communications between phases.

2.4.2 UPB

Similar to X10, Universal Power line Bus (UPB) is another wired protocol [44-45]. It has advantages over X10 in being less susceptible to power line noise and having increased range, (it can transmit over one mile). UPB uses a home's existing power lines, which reduces costs. The limitation of UPB is that it is difficult to combine it with the newer

wireless technologies such as Wi-Fi and smart phone. Another disadvantage of this protocol is a relatively low bandwidth causes slow performance. It is not as secure as wireless as no encryption is provided. The technical complexity makes the system difficult for user to setup.

2.4.3Enocean

EnOcean [45-46] is one of the latest technologies in home automation, aimed at zero energy consumption through energy harvesting. The advantages of the EnOcean devices are their ability to work without battery and having wireless communication ability. This system is powered by micro energy converters and uses ultra-low power electronics [47]. Early designs of EnOcean devices used piezo electric generators but were later replaced by electromagnetic energy sources [46]. Maintenance is minimal because the devices are self-powered. Radio interference is also minimal as it operates in the less crowded 315 MHz band.

2.4.4 Insteon

Insteon which was first introduced in 2005 can communicate by both by power lines and wirelessly [47]. Insteon users can add wireless capability to an existing X10 network as it is X10 compatible. Non-technical individuals can set up and add devices to the network through Insteon technology. There are almost 200 different Insteon-enabled home automation devices available on the market including the "hub" controllers. Insteon devices are relatively expensive compared to other systems. The InsteonStarter Kit is cheaper than the Insteon Hub, and the Insteon app is limited and frustrating to the normal user [48]. The Insteon system may not be suitable for an IoT device as the network joining method is not published and so security is unclear [49].

2.4.5 Z-wave&Zigbee

Z-Wave [48] is a low power RF communications system that runs on the 908.42MHz frequency band and so is less affected by traffic on the 2.4 GHz band. A significant advantage of Z-Wave is its interoperability. All Z-Wave devices can communicate with all other Z-Wave devices, regardless of type, version or brand. Further, the interoperability is backwards and forward-compatible in the Z-Wave ecosystem; that is, Z-Wave products introduced today will work with Z-Wave products from a decade ago and with products in the future (although possibly with some limits on functionality).There are approximately 1,200 different Z-Wave compatible devices on the market. Z-Wave's mesh network is achieved be enabling all devices to double as repeaters. All Z-Wave modules are produced by a single manufacturer, Sigma Designs. A single manufacturer always represents a risk as the supplier may disappear or suddenly raise prices.

There are many similarities between Z-Wave and ZigBee [48-49]. Like Z-Wave, ZigBee is exclusively a wireless home automation protocol. While it claims many home automation enthusiasts, its full acceptance is limited by the lack of interoperability between ZigBee devices, which often have difficulty communicating with those from different manufacturers. As a result, ZigBee is not necessarily an ideal choice for anyone just starting down the home automation road unless they use devices from just one manufacturer. There are different versions of ZigBee, which do not necessarily talk seamlessly with each other. The significant advantages are as follows-

- ZigBee has always had a focus on ultra-low power consumption which made it ideal for battery-operated devices or locations where wiring would be difficult.
- This multi-hop mesh networking approach can use redundant pathways to make sure the message gets through even if one of the devices is out of order [48-49].
- ZigBee devices can be strung together in networks of up to 65,000 nodes [48-49].

Disadvantages include-

- ZigBee is integrated only at the radio level.
- Device makers develop propriety software that sits on top of ZigBee thus destroying interoperability between manufacturers.
- There is less quantity and availability of devices in comparison with other systems.

The Philips Hue lighting system [50] offers LED light bulbs that can be switched on and off, dimmed and produces colours throughout the RGB spectrum, which is controlled via a website or smart phone application. The system uses ZigBee and bridges the bulbs to the Internet using an additional ZigBee to Wi-Fi router, which is an extra cost to the system. The Hue bulbs are not protected by security as strong as WPA2 and can be hacked to obtain the LAN password [50].

2.4.6 Wi-Fi

This is the networking protocol that is able to share an Internet connection among laptops, game consoles, and so much more. It's very fast, ubiquitous and most homes have a Wi-Fi system [51-53], usually an 802.11 a/g/n system. The other protocols use less power and bandwidth but Wi-Fi's reach cannot be understated, even if it is overkill to use it to turn a lamp on and off. Wi-Fi systems based on home routers tend to be power consuming and so unsuited to battery power. Wi-Fi does not provide a home automation system merely a communications system on top of which a home automation system may be built.

Recently Wi-Fi modules costing only US $5 dollars each have become available, for example the ESP8266. These units have open source software and have ample room for user code. These can be the basis of remarkably cheap IoT devices based on Wi-Fi.

2.4.7 Bluetooth

Bluetooth [54-55] is at the core of many products; from light bulbs to speaker docks to locks. Kwikset claims to have introduced the first Bluetooth lock, Kevo, in 2013.The advantages of Bluetooth technology include very low power usage, low cost, and that it is built into most mobile phones. Problems include security issues and that it can only connected two devices at once. It is not a true networking system, and can easily lose connection in certain conditions. Bluetooth is simply an end-to-end communications protocol that can be used for home automation.

2.4.8 Thread

Thread [56] is a new wireless protocol for smart household devices. Seven founding members, including Google's Nest Labs and Samsung Electronics [32-34], formed the Thread Group in July 2014. More than 250 devices can be connected on a single Thread network. Using the same frequency and radio chips as ZigBee, Thread claims to provide a reliable low power, self-healing, and secure network that it simple to use. Thread can also be connected to the cloud for ubiquitous access. Thread is used by the Nest Learning Thermostat and Nest Protect, and more products are supposed to enter the market supported by thread..

2.4.9 Apple home kit

AppleHomeKit [57] is a software framework that can be connected directly to the iPhone and a dedicated app is available to control the smart home devices. HomeKit uses Wi-Fi and Bluetooth as the primary communications protocol and according to Apple, a Z-Wave/Zig-Bee bridge is being developed. Apple has approved an Insteon-HomeKit bridge as well, and Lutron offers a Homekit-compatible hub for its Caseta Wireless system.

2.4.10 Analysis of Existing Products

Although home automation systems [36-42] have been available for decades the market is small, typically limited to technology freaks, early adopters and wealthy customers who can afford to pay a technician to install the system. Few customers are willing to pay many hundreds of dollars just to control lights or provide a thermostat function. All existing commercial systems have problems in terms of high cost or not providing a simple DIY experience where consumers can buy from any manufacturer and expect interoperability.

2.4.11 Security Issues

Automating everyday tasks and increasing home efficiency are major advantages of home automation, but security concerns must be addressed in order to protect home users. Most commercial systems do not state what methods they use so security is uncertain.Open standards such as Bluetooth, WiFi and Zigbee do state their security methods and these have been well researched and validated. Where faults are found fixes are quickly implemented, for example the WPS security issue [58].

2.4.11.1 DoSAttack (Network Attack)

A Denial of Service (DoS) attack [58] is where the attacker denies access to resources such as IoT devices by injecting large volumes of traffic or interfering with legitimate traffic. For communications systems with an external interface a well set up firewall will protect against most external attack traffic. Attack traffic generated by internal connected devices is difficult to detect and eliminate but this can be achieved using devices such as IDPS (Intrusion Detection and Prevention Systems). Direct interference with local wireless links and deliberate jamming is impossible to eliminate. For Wi-Fi, the well-known de-auth attack [59] continues to be a problem. Wired systems can be protected against DoS attacks but wireless

systems will always be vulnerable to a determined attack. This weakness must be keep in mind for wireless IoT systems.

2.4.11.2 Man in the middle Attack (Cryptanalysis Attack)

The man-in-the-middle attack [58] is where an attacker or hacker intercepts a announcement between two systems and the attacker poses as the legitimate sender. As the attacker has the new communication, they can scam the recipient into thinking they are still getting a genuine message. The best possible way to avoid man-in-the-middle attacks is to use a strong encryption method between the client and the server. In the case of Wi-Fi with WPA2 there is strong encryption [60] with the main weakness being the user's handling of the network password. Another successful approach is the use of digital certificates where parties use a trusted third party to confirm identities [61]. For domestic IoT devices, the security afforded by encryption such as WPA2 is probably adequate.

2.4.11.3 Eavesdropping:

Eavesdropping is where an attacker listens to network transactions with the aim to decode or interfere with those transactions [58]. Again strong encryption is the key to preventing this type of attack with the well-known protocols having a well-defined and known capability. Protocol is such as WPA2 are well beyond the ability of casual hackers to crack thus making home IoT devices relatively secure.

2.4.11.4 Replay attack

A replay attack (also known as playback attack) [62] is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and re-transmits it,

possibly as part of a masquerade attack by IP packet substitution. The key to eliminating this type of attack is that the data packets need encryption and sequence numbers so that a previous message is no longer valid.

2.4.11.5 Routing Attack

Routing attacks [58] are committed by a network adversary with keen knowledge about the router being used in the network. Usually the external border gateway routers are targeted by as these routers share information between multiple protocols from different partnered companies.

2.4.11.6 Security Summary

It is very important to choose an IoT protocol that provides good security to protect the homeowner. From the work reviewed, this suggests an open protocol with strong proven security. This limits the choise to Wi-Fi, ZigBee or Bluetooth. After an extensive study, WiFi protocol with WPA2 security layer was choosen in this research. The other advantages of the Wi-Fi over ZigBee and Bluetooth are diccussed in the following section.

2.4.12 Analysis of Existing Protocols in the Wireless Home Automation

There are three key open protocols that are useful for IoT devices: Wi-Fi, Bluetooth, and ZigBee. Wi-Fi and Bluetooth are built into most mobile phones and laptops, and thus have a convenience and cost advantage over ZigBee.

Feature(s)	IEEE 802.11b	Bluetooth	ZigBee
Power Profile	Hours	Days	Years
Complexity	Very Complex	Complex	Simple
Nodes/Master	32	7	64000
Latency	Enumeration up to 3 Seconds	Enumeration up to 10 seconds	Enumeration 30ms
Range	100 m	10m	10m-300m
Extendibility	Roaming Possible	No	YES
Data Rate	11Mb/s	1Mb/s	250kb/s
Stack size	100+ kbyte	100+ kbyte	8-60 kbyte
Topology	Star	Star	Star, cluster, mesh
Security	Authentication Service Set ID (SSID), WEP	64 bit, 128 bit	128 bit AES and Application Layer user defined

Figure 2.4.12: A comparison of the different wireless [63].

Figure 2.4.12 from [63] shows the relative advantages of these three protocols. Note that Wi-Fi also has WPA2 which provides strong encryption. Bluetooth Operates with 2.4 GHz frequency band and only works well within one room not across an entire house [63-65]. Due to this small range, Bluetooth [64] is not suitable for automation of the whole house. Bluetooth has another significant limit [65] in that only a small number of devices can be simultaneously active in an area due to interference. Finally, speed of transfer is also very slow and decreases very rapidly with increasing distance. Concerning the security issue, Bluetooth is a WPAN standard with moderately secure and still has weakness in it security architecture. For example, Its E0 cheaper algorithm is weak, unique key sharing can lead to eavesdropping, security services are limited, and devices addresses are not validated [64].

A ZigBee network is scalable and it is easy to add or remove a ZigBee end device to the network. It has some disadvantages as regards security [66] compared to Wi-Fi based WPA2 systems. ZigBee has weakness in key distribution as the security key is transmitted either

over the air or preinstalled in the device in an unsecured way [67]. Eavesdropping and manipulating data is another weakness that found in the ZigBee protocol.

Wi-Fi [67] has only one weakness compared to Bluetooth and ZigBee, it consumes more power which means battery operation for extended periods is not possible. The newer low power Wi-Fi may change this situation [68-70]. The majority of IoT devices have mains power available and those that do not might use Bluetooth or ZigBee with a bridge to Wi-Fi. This approach has been used by the Philips Hue light bulbs[50].Wi-Fi data rates are higher than Bluetooth or ZigBee [69] though this is not an issue for the majority of home IoT devices. Most homes, mobile phones, and laptop computers already have Wi-Fi and an IoT based system can use this for zero cost thus making a Wi-Fi based IoT system much cheaper. Finally, the security of Wi-Fi, when using WPA2, is very good and quite adequate for the home environment.

2. 5 Existing Home Automation System Architectures for IoT

The main theme of this research work is discovering how IoT devices may securely join a Wi-Fi network but the economics of the network architecture are also very important. Three main approaches as shown in Fig. 2.9 (a), (b) and (c) have been found in the literature for the design of home automation devices. They are: a) dedicated IO, b) Bridge, c) Central controller

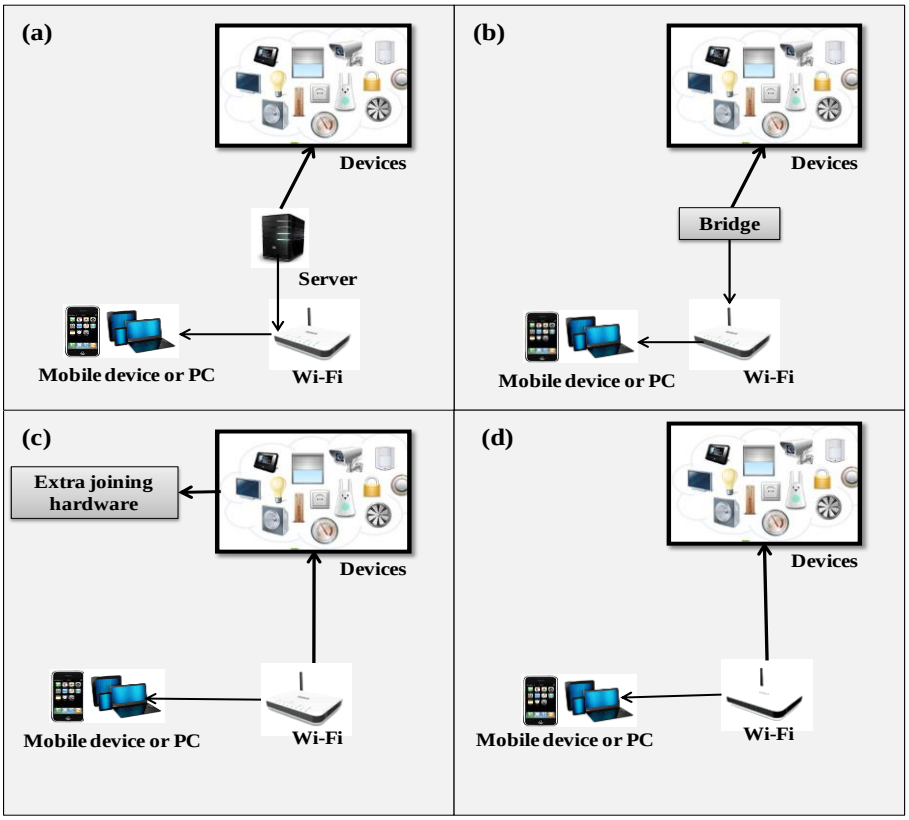

Figure 2.9 Home Automation Communication Architectures: (a) Server based communication architecture (b) Bridge based communication architecture (c) Joining extra hardware based communication architecture (d) Proposed Minimalist IoT Network Architecture.

2.5.1 Dedicated I/O based architecture

Many researchers have been used additional IO devices and protocols on the automation device for securely joining the local network and controlling devices. Such an approach requires extra hardware and so increases costs.

The IO protocols are different to Wi-Fi protocols, for example NFC [71], and Bluetooth [54]. Chen et. al. [54] implemented NFC Tags in devices so that users could tap their NFC-enabled smart phone against the device to send control information, but the actual data transmission was still carried over traditional network infrastructures.Near Field Communication (NFC) is a relatively recent short-range, high frequency, two-way communication technology based on the Radio Frequency Identification (RFID) principle. When two NFC-enabled devices (named Initiator and Target) are located near to each other, a peer-to-peer connection is established between them, and they both may send and receive information. Two operational modes, that is, active and passive, are possible for an NFC device. In the active mode, which is not possible in traditional RFID solutions, NFC peers may exchange messages; in the passive mode, one of the two nodes acts only as a passive tag. An NFC tag may store a given amount of information: a Universal Resource Locator (URL) addressing a specific resource on the web, the value of a specific measure, or figure [71]. NFC applications are gaining an increasing popularity [71], as many of the smart phones available in the market are now equipped with an NFC transceiver, which is used, as an example, in contactless transactions such as mobile payments and transit ticketing. Among the most widespread applications are smart posters and object tracking, based on the passive operational mode. NFC may be also fruitfully employed to make pervasive computing environments more personalized, dynamic, and smart. NFC, as other contact less systems, is intended to be easy to use for everyday transactions, as the interaction is carried out with a simple touch, swipe, or tap.

Piyare and Tazil [72] utilized Bluetooth as a communications protocol in a home automation system. However, it was only used to allow a phone to communicate to a central controller. The advantage of this was that the end devices did not need to have Bluetooth hardware and so no extra cost was incurred, though, as has been seen so often, use of a central control only increases cost and complexity and reduces flexibility.

Kumar and Lee [73] proposed an Android based smart home system using Bluetooth and Arduino. This system is based on the Arduino micro web server as the main controller. The paper suggests usage of a mobile application based on the Android OS. The approach used Bluetooth and the RESTful based web services as an interoperable layer. The main advantage of this system is that it is flexible and scalable solution. The most important disadvantage of this system is that it is limited to Bluetooth communication, which has a limited range and requires extra hardware, such as the siren nRF24L01+ radio module, which is used in order to communicate and coordinate actions with the other sensor nodes within the environment.

This approach works well for larger appliances that are more complicated where the addition of an interface or additional IO hardware is trivial or already included. It provides some opportunity for the joining event to be streamlined and the user's experience may be marginally improved. However this approach does not scale well and when implemented on simpler devices such as a mains switch it greatly increases size, complexity and cost. There have been notable compromises made using this approach, with devices of an intermediate complexity, which have sort to minimize the impact of adding an interface by implementing a simplified interface. Such approaches include the Nest, acquired by Google [32]. The Nest is a smart thermostat, which learns about its environment and controls the temperature accordingly. Its interface is a round screen, 1.75” in diameter, and a rotating ring [33]. Rotation of the ring is used to scroll through options and depressing the ring will make a selection. This is an extremely compact approach sufficient for most day-to-day operations

but is exceedingly inconvenient for the user when this ring is to be used to input their local Wi-Fi password to join the device to their network [34]. The NEST approach makes an expensive thermostat and if this approach were used for simple devices such as power switches the cost would be prohibitive.

Overall, it can be concluded that adding extra IO hardware can enable network joining but this comes at a financial cost and may result in an inferior user experience.

2.5.2 Bridge based Architecture

The second approach, again using additional hardware, translates between Wi-Fi and some other protocol, thus creating a bridge. The network-joining problem is solved by the non-Wi-Fi protocol. ZigBee is one of the popular protocols in this approach [24-31], which has secure joining inherent in the protocol [24]. Control of a device is thus maintained by a bridging device running a protocol like ZigBee connected to a local router. Insteon and Z wave are another example of bridging protocols, however like ZigBee they ultimately rely on extra infrastructures to be in place. These secondary protocols are simply bridging the IoT device over to another, primary, protocol to avoid building capabilities into the device to handle the primary Wi-Fi protocol. Such an approach will increase cost and complexity of IoT devices and the networks they inhabit [26].

2.5.3 Central Controller based Home automation

A third approach implements a central controller to which devices are physically wired. The central controller is then connected to the LAN to either by cable or Wi-Fi. The physical connection to devices offers an inherent security advantage but sacrifices the flexibility offered by a wireless connection. The individual devices do not need an Internet connection and may thus be made more cheaply though the cost of wiring a home can be high. These

systems are not easily altered and users are quickly locked into a single product line thus increasing costs. The central units themselves are expensive while set-up and installation usually requires trained professionals. While the individual devices are simpler and seem to offer advantages for the user experience, the overall system's complexity is increased and its flexibility reduced thus compromising any gains to the user experience.

Several studies have been carried out for the server based home automation architecture using an Internet based server or Java based server, networked hardware equipment, cellular networks, Wi-Fi, GPRS networks, database, GSM network, IPv6 approach or Android mobile phone [71-84]. The architectures are described as user-friendly [71-81], low-cost and flexible to use [71], easily joining networks as an IoT device [69], and support wide range of home devices [72-76]. These all approaches require a permanently powered central server or high end PC which is an extra cost. Additionally, users cannot configure the system by themselves thus also increasing cost [71-77]. The other drawbacks include high cost due to the use of SMS messages for control and reporting of status [69-79], high cost due to wired installation, extra cost for development and hosting of web pages [73-75], inflexibility, poor manageability, and difficulty in achieving security[73-75].

KNX is one of the more mature and successful protocols used in this approach but it is expensive. It is built of several well-established protocols and is tailored to situations such as home automation [84].

Considerable research been carried out to develop the remote control systems for home automation. Earlier systems are mainly based on the use of telephone line, such as a phone-based system for home automation using a hardware-based remote controller [72-78], and a personal computer [72]. Telephone is used as a remote control input device in these systems and has no friendly user interface. With the advancement of Internet, various Internet-based remote-control architectures for home automation have been proposed [72-76]. These

systems rely on the Internet and generally feature friendly graphical user interfaces. In this approach, an Internet connected personal computer need to run all the time as a home server.

2.5.4 Analysis of Current System Architectures:

All the systems described above, and many others, are expensive and may require experts to install or modify the system, which is another large expense. Many systems require a personal computer to be permanently active and there is no suitable way to easily connect an IoT device, which lacks a keyboard and display. None of the systems allow a home owner to install or add to the system in a simple DIY (Do It Yourself) manner where the user can chose to buy from a range of manufacturers, as we are used to doing with open Wi-Fi based equipment. If such a system were possible then costs would drop and home automation may become much more affordable and popular.

Chapter3: Research Questions

The literature search has shown that existing home automation systems are not suitable for IoT implementation if costs are to be reduced and a simple DIY experience is to be possible. The ideal IoT device has only Wi-Fi for a communications mechanism, can be controlled without a central controller, and should be purchasable from a shop and installed by the homeowner. The removal of the central controller and using Wi-Fi presents a considerable challenge to the designer of such a system. The functionality previously provided by the central controller must be delegated to the IoT device and devices such as a Smart Phone.

These ideas result in some very interesting research questions.

- **Question 1**: What architecture will allow the elimination of a home automation system's central controller?
- **Question 2**: What architecture would allow DIY installation and additions using devices from different manufacturers?
- **Question3**: Can existing network protocols handle the key tasks of secure joining IoT devices or are new protocols required?

3.1 Scope of the Study

This research proposes a Minimalist IoT Network Architecture (MINA) for home automation system with simple network joining protocol. Particularly we examine problem of how can IoT devices without additional hardware such as a keyboard and display join a Wi-Fi network in a safe and secure manner. If this problem is solved it would reduce the cost of IoT devices and home automation system. Accordingly, we introduced a three stage novel

network joining protocol to securely join the IoT device to a local Wi-Fi network. The protocol is implemented using a WPA2 based LAN, an Android phone and a Raspberry Pi which represents an IoT device lacking any form of keyboard and display. There is no central controller in our proposed system and the IoT devices do not have extra hardware purely for joining the Wi-Fi network. The proposed network joining protocol would allow users to purchase off the shelf devices from a range of manufactures and control them by a PC or mobile device in a very simple manner.

There are many other issues to be resolved for a complete DIY architecture, for example IoT to IoT communications and how a single application on a Smart Phone can discover, display and control any IoT device. Another issue is that of low power nodes though this may be solved by then 802.11 ah Wi-Fi protocol. The growth of the IoT has just started. We are rapidly evolving, but there is a lot of unknown. Unknown applications, unknown devices, and unknown use cases. The best way to proceed is using one common worldwide standard for technology and application programming interfaces that can get these devices to talk to each other and to the cloud without networking infrastructure upgrades. Standardization and implied interoperability is one of the main reasons Wi-Fi is very popular, and that's another big reason that it is suitable for the IoT. Needs of security and protecting privacy in the borderless world created by IoT are real and can be delivered using Wi-Fi.

3.2 Significance of the study

Consider a simple Wi-Fi enabled mains power switch, which is currently available for US $20. Currently these devices do not have a secure way of joining a home Wi-Fi network. Such secure joining could be achieved using a central controller, NFC, Bluetooth, or extra IO hardware such as a screen and keyboard. The addition of this extra hardware will increase the cost of a very simple IoT device and make it uncompetitive.

The development of a user-friendly secure joining protocol, which requires no extra hardware and no central controller, will enable homeowners to buy a cheap IoT device and install it themselves into their home network. This has the potential to significantly decrease costs from hundreds of dollars to tens of dollars and so increase the smart home market to the benefit of consumers and manufacturers alike.Based on the research questions identified in this study a system architecture will be proposed in which a simple Wi-Fi IoT device can join a LAN by a new three-stage network joining protocol. A novel Device Discovery (DD) protocol will also be proposed. It is intended that these protocols will be an open standard that will ensure that devices from a range of manufacturers will be compatible with each other.

Chapter4: Proposed System Architecture

This section describes the design of the Minimalist IoT Network Architecture (MINA) and the required network protocols that satisfies the architecture shown in Fig 2.9(d). Figure 4.1 shows the overall architecture of the proposed home automation system.

The first step is to eliminate the central controller as shown in Fig. 4.1, which will save considerable costs. Each device has a WPA2 protected Wi-Fi link and some computing power so it can handle any timing for its own activities. User may use their smart phone or PC to directly control the IoT devices.

The elimination of the central controller requires that its functionality be dispersed between the IoT devices and the mobile device. These functions include safe joining of the IoT to the home LAN, device discovery, and device display and device control. This thesis focuses on the safe joining issue, which is the subject of the next chapter.

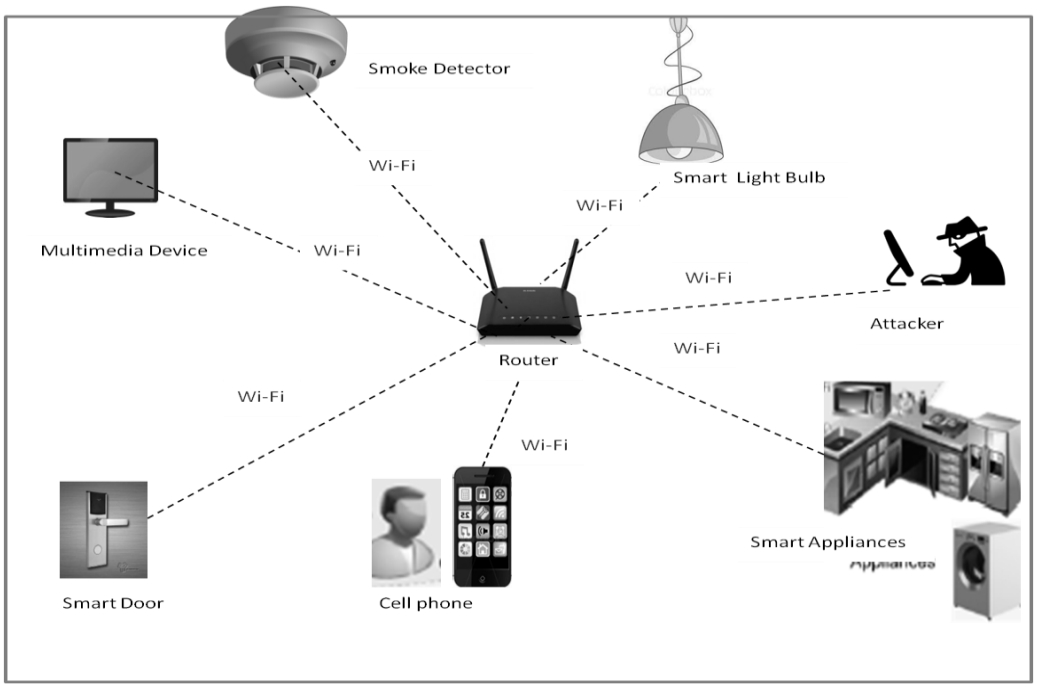

Figure 4.1 Proposed Home Automation System Architecture

The system uses the hotspot capabilities of a smart phone to establish an initial temporary but secure connection to pass credentials for the local home network. It requires little adjustment to existing controllable devices and is extremely appropriate to simpler devices such as mains switches while maintaining a high level of security. It is intended to reduce costs by only using the hardware already necessary for a wireless IoT device. The main idea behind this architecture is that wireless devices would be sold with a pre-programmed unique SSID and Password. These smart IoT devices would then automatically try to join a Wi-Fi network with this pre-programmed configuration. The device can only then be contacted on a network meeting the pre-configured credentials; this is achieved by a smart phone generating that network using its AP mode (hotspot). This temporary link would be secured by the encryption offered by secure wireless protocols (e.g. WPA2), allowing the SSID and password for the local, permanent, and Wi-Fi network to be passed to the IoT device. Once it receives the local Wi-Fi credentials, the IoT device would be able to disconnect from the phones hotspot and join the local network. The important feature of our proposed architecture is that it eliminates the central controller, which will save considerable cost. The second feature is that the system uses the hotspot capabilities of a smart phone to establish an initial temporary but secure connection to pass credentials for the local home network. The overall idea behind this architecture is that wireless devices would be sold with a pre-programmed unique SSID and Password. These smart IoT devices would then automatically try to join a Wi-Fi network with this pre-programmed configuration. The next chapter will describe a protocol which will implement this system.

Chapter5: Three Stage Network Joining Protocol

5.1 Protocol Description

Figure 5.1 shows a new three-stage network joining protocol that enables a simple Wi-Fi IoT device to join a LAN in a secure manner. Figure5.1 (a) shows the initial link being setup between the mobile phone acting as a hotspot (a wireless access point or AP) and the IoT acting as a normal Wi-Fi device. The mobile phone is set up to a unique SSID and password that comes with the IoT device from the manufacturer. This setup is all done using WPA2, which provides a secure link from mobile phone to the IoT device. Attackers would need to break WPA2 to seal the useful information. Figure 5.1(b) shows that the mobile device passing the Local Area Network (LAN) SSID and password to the IoT devices via the WPA2 protected hotspot link. Attackers would like to obtain the LAN SSID and password but again cannot get any of this information without the ability to break WPA2 or knowledge of the unique IoT password. Figure 5.1(c) shows that both IoT and mobile device have changed their Wi-Fi to the LAN and both can communicate with each other, and any other LAN device.

The basic three-stage network joining protocol has not addressed the important issue of setting up the IoT SSID and password. Here we offer 3 solutions, the first offered while simple and economic has flaws which may be acceptable in low security situations. The last solution offered is robust and its security is only limited by the limits of the Wi-Fi encryption protocol. All solutions rely on a mobile phone that can act as a Wi-Fi hotspot. Mobile phones should not be regarded as an extra cost as they are already owned by most home owners and are only required for the short process of joining the network. A mobile phone hotspot is normally intended to link a PC directly to a mobile phone using Wi-Fi, and then via the phone's 3G/4G link to the Internet. There is a necessary hotspot side effect, which is of

great use: applications running on the mobile phone acting as hotspot can also communicate with applications running on the PC or other Wi-Fi connected device.

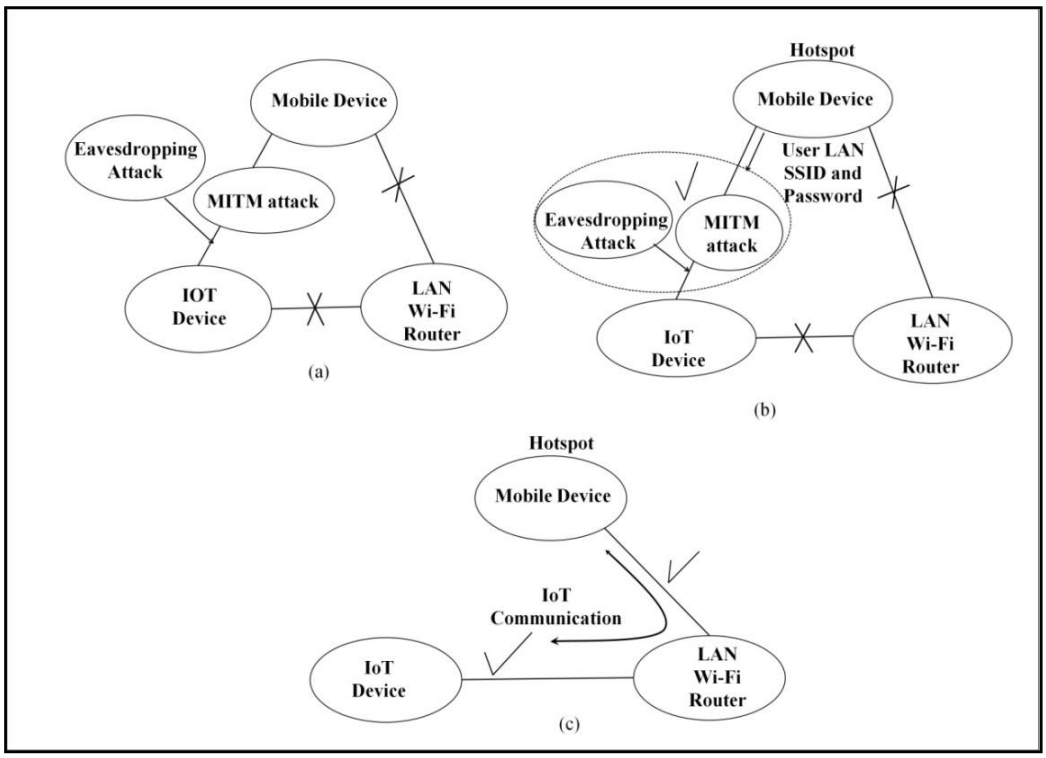

Figure 5.1 Three stages in IoT joining Protocol: (a) secure mobile to IoT connection established. (b) Transfer of LAN SSID and (c) Final state with IoT device joined to the LAN.

Solution 1: An IoT device is configured with a default pre-defined SSID and password set by the manufacturer at the factory. One problem with using the default SSID is that some confusion might result if a company or homeowner next door sets up an IoT device at the same time. Hackers would soon know the default information, post it on the web, and so hackers world-wide would be listening for just such a connection. They would then be able to capture the LAN SSID and password as it passed from mobile phone to IoT.

Solution 2: Consider that the simple IoT device can use otherwise unused combinations of existing device buttons to initiate joining a LAN resulting in some variation on the default

connection information. Wired routers use this approach to joining a secure network; usually a paper clip can be used to push a hidden reset switch and the router then is set to a known IP address and password [85]. This only works for wired routers because the method of joining the network requires a physical cable link to a PC, which is assumed to have no listeners. The IoT device must use the Wi-Fi link and this may well have listeners. When the hotspot tries to send the LAN SSID and password to the IoT device an attacker can listen in and try variations on the default connection information. It does not seem possible to devise a scheme using just a few keys on the Wi-Fi IoT device that could not be followed by an intelligent attacker who understands the basic variation algorithm. The cracking need not even be real time. The packet transfers could be recorded and cracked after the event to get the LAN SSID and password.

Solution 3: The manufacturer provides a unique SSID and password for each IoT device. In the final outgoing test, the IoT device gets a random SSID and PW, which is printed and packed, with the device. This approach provides a user-friendly way to provide a secure link between mobile phone and IoT where the attacker cannot break the Wi-Fi security and get the LAN SSID and password. It comes at minimal cost to the supplier and the resulting security is only limited by the nature of the Wi-Fi security (most likely WPA2).

5.2 Protocol Design

Figure 5.2 shows the bounce diagram of successfully connecting an IoT device to the local network. Three major steps are required to join the local network as described in Fig.5.2

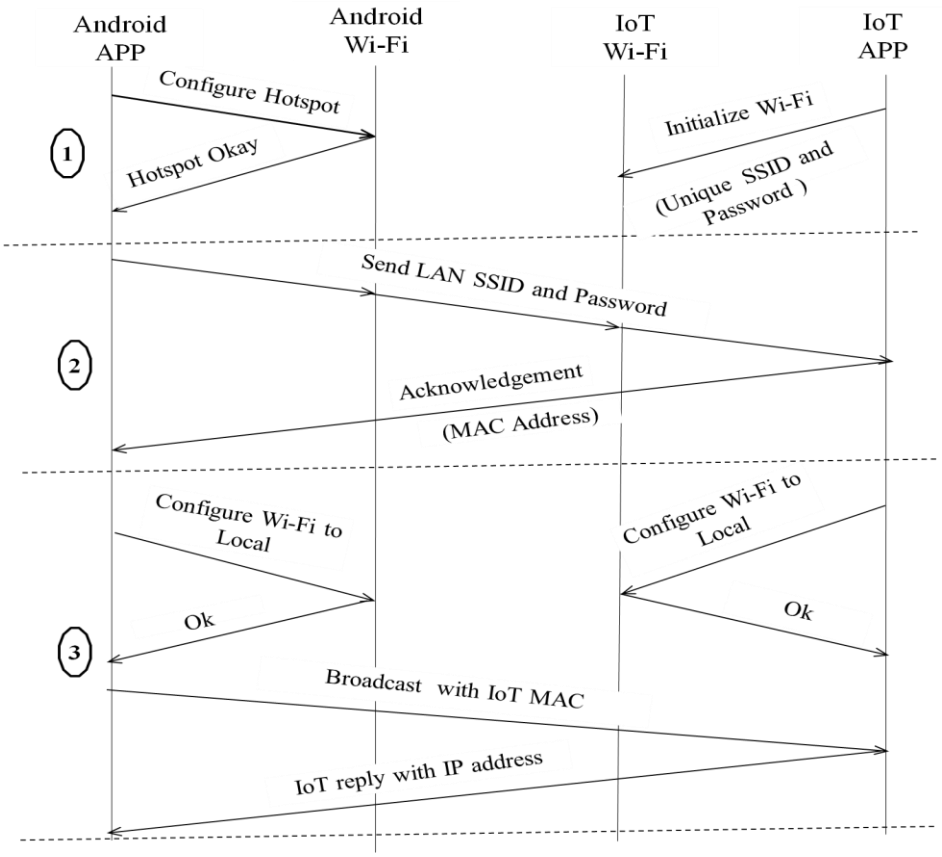

Figure 5.2: A bounce diagrams for Successful Connection of three stage novel Network Joining protocol

Stage 1: In the first stage, the Smartphone is put into the hot spot mode, where it's become a Wi-Fi wireless access point (AP). The IoT device will try to connect to the wireless network using the unique SSID and password preprogrammed provided by manufacturer

Stage 2: The Smartphone in hotspot mode sends the home LAN SSID and password to the IoT device. This is protected as the Wi-Fi link to the IoT device uses WPA or WPA2. The IoT device replies that it has successfully received the home Wi-Fi SSID and password. This reply also carries the MAC address of the IoT device, which is used in the next step.

Stage 3: Finally, in the third stage, the Smartphone and the IoT device both join the home Wi-Fi network. The IoT device has now safely joined the home network and can be contacted with any device on the home network. The mobile phone can directly contact the IoT device to ensure it has joined using the MAC address captured in the previous step. The entire joining operation is secured by WPA/WPA2.

This chapter has proposed a novel three stage joining protocol so that IoT devices can join an existing Wi-Fi LAN with the full security of WPA and at minimum cost. Other products and protocols such as those examines in the literature search are more costly as they require extra hardware and in some cases are less secure.

Chapter6: Design and Implementation

After designing the system architecture and the new three-stage protocol, the system was implemented and tested in a laboratory environment. In assessing the capacity of current hardware to support protocol, four key functions needed to be achievable. First, it needed to be possible to force the smart phone in and out of AP mode. Secondly, the Wi-Fi configuration of a smart phone needed to be configured by programming into both hot spot and AP mode. Thirdly, communications between, IoT device, and smart phone needed to be achievable. Finally, the Wi-Fi Credentials of an IoT device needed to be configured from program. These key functions were mapped successfully to the Android operating system.

6.1 Development Equipment& Development Environment

The equipment used to develop the novel network joining protocol included an Android phone, a Raspberry Pi to represent an IoT device, and a home router as shown in figure 6.1.

The Android phone used was a Samsung Galaxy Note3 with Android version 4.4.2 but any Android phone capable of being a hotspot would be suitable.

The IoT device would ideally be a low-end microprocessor and Wi-Fi interface that matches what would be used inside a very inexpensive IoT mains power switch. In order to speed development a Raspberry Pi was used instead though for the purposes of the protocol only the Wi-Fi and a little computing power was used. The Raspberry Pi used was a model B unit running Raspbian Wheezy, a Debian based Linux distribution.

A NETGEAR WNR614 router was used to represent a home Wi-Fi router. This is a typical home router.

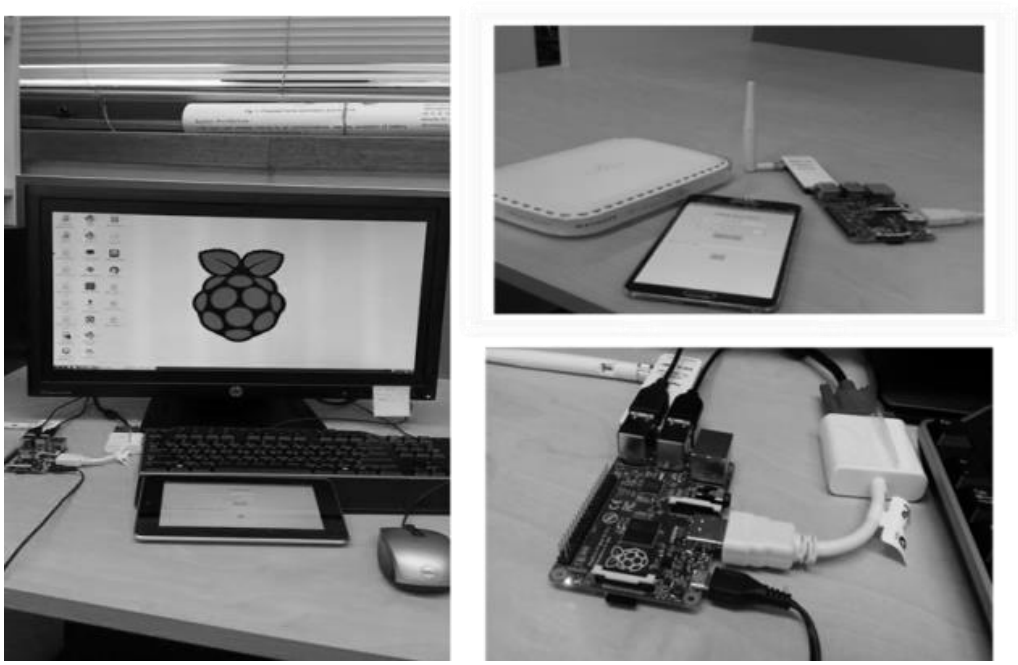

Figure 6.1 Testing application with IoT device (Raspberry Pi, Wi- Fi router and Android device)

The development environment used for Android was Eclipse Juno running on a Mint 13 Linux with the Google ADT plug-in. This allowed for quick Android code development and the downloading of code into the Android phone.

The code for the Raspberry Pi was written on the Pi using the C language and the Geany IDE.

6.2 Software Design

This section shows the key software functionality required to achieve the 3 stages of network joining. This section does not show the GUI interface required for user input. The operational GUI is shown in the next section on testing along with the extra GUIs necessary to cope with error conditions identified and handled.

6.2.1Stage 1: Smart phone into AP Mode:

Turning on the phone's hotspot is the first stage of the new protocol. Rather than requiring, the user to go through the complex steps to achieve a hotspot mode (make the phone an access point) this is achieved using code. Network functionality must not be in the

same activity as the GUI activity and so a new thread must be created and given the SSID and password for the IoT device. This is shown in Fig. 6.2

```
Discoverer(String SSID, String PW, Context activityContext, Activity A) {
//--- Capture all parameters.
LAN_SSID = SSID ;
LAN_PW = PW ;
context = activityContext ;
broadcastData = LAN_SSID + "," + LAN_PW + "\0";
deviceData = "Did not even receive own broadcast, wifi down?" ;
callingActivity = (MainActivity)A ; // This is a pointer to the main activity.
`
```

Figure 6.2 Setting Android Wi-Fi Mode

Once this has been done, the Wi-Fi can be set up and a socket selected.

```
//--- get access to wi-fi and grab socket.
Log.d(TAG, "Started thread.");
mWifi = (WifiManager) context.getSystemService(Context.WIFI_SERVICE);
DatagramSocket socket = newDatagramSocket(DISCOVERY_PORT);
socket.setBroadcast(true);
socket.setSoTimeout(TIMEOUT_MS);
```

Figure 6.3 Setting Android Wi-Fi Mode

Note that Android uses a particular IP address for hotspot mode, 192.168.43.*, thus, the broadcast address must be 192.168.43.255.

6.2.2 Stage 2: The Discovery Request

The previous stage has put the Android phone into hotspot mode with the SSID and password to suit the IoT device. The IoT device is continually trying to join this network and will succeed as soon as the Android hotspot is set up. The IP address allocated to the IoT by

```
privatevoidsendDiscoveryRequest(DatagramSocket socket) throwsIOException {
Log.d(TAG, "Sending data " + broadcastData);
DatagramPacket packet = newDatagramPacket(broadcastData.getBytes(),
broadcastData.length(),
        getBroadcastAddress(), DISCOVERY_PORT);
socket.send(packet) ;
          }
        privatevoidlistenForResponses(DatagramSocket socket) throwsIOException {
        byte[] buf = newbyte[1024];
        try {
        while (true) {
        DatagramPacket packet = newDatagramPacket(buf, buf.length);
        socket.receive(packet);
              String s = newString(packet.getData(), 0, packet.getLength());
        //--- assume reply packet is different to sent packet.
        if ( s.equals(broadcastData) ) {
```

Figure 6.4 Sending Broadcast Discovery & Receiving Reply

the Android hotspot mode is unknown and so a UDP broadcast request must be sent out with the LAN SSID and password, and the IoT will reply. This reply contains the IoT MAC address, which can serve as its identity. The sending and receiving is shown in Fig. 6.4.

Figure 6.5 shows key elements of the C code used on the Raspberry Pi that waits for the Broadcast containing the LAN SSID and password and then replies to the Android device.

```
while(1) // forever loop.
{
//--- setup class with ip and port.
Tudp_handler rx_udp( broadcast, BROADCAST_PORT) ;

//--- start listener
 cout << endl << "   Waiting for UDP packet on IP " << broadcast <<", port " << BROADCAST_PORT
     << endl ;
if (rx_udp.wait_receive_udp () )
 {//--- got an error
           cout << "   Send error: " << rx_udp.error_message << endl << endl ;
           return(-1) ;
       }
  cout << "   Received packet: " << rx_udp.rcv_str << endl ;


//--- Extract SSID and password of wifi.
  istringstream ss(rx_udp.rcv_str);
  getline(ss, SSID, ',');
  getline(ss, password, ',');
 cout << "   Got SSID: " << SSID <<", PW: " << password << endl ;

 //--- now reply back.
  Tudp_handler tx_udp( broadcast, BROADCAST_PORT) ;
  tx_udp.send_str = MESSAGE ;
 if ( tx_udp.send_broadcast_udp() )
   {//--- got an error
    cout << "   Send error: " << tx_udp.error_message << endl ;
     return(-1) ;
   }
  cout << "   Sent reply to address: " << broadcast << endl ;
}//while

}
```

Figure 6.5 Raspberry Pi Code to capture LAN SSID and password.

6.2.3 Stage 3: Communicating via the LAN

The previous stage sent the LAN SSID and password to the IoT device. In stage 3 the IoT and Android device both set, their Wi-Fi links to the LAN and can communicate via the home router. The code to achieve this is very similar to as shown above except the Android device is not running as hotspot (wireless access point or AP) just a Wi-Fi device and the connection is now through the home router.

6.2.4 Conclusion

This chapter shows key code fragments that allow the Android phone and the IoT device to move through the 3 stages of secure joining to a home LAN. Given this success, the user interface can be designed to capture user input and error modes can be discovered and handled.

Chapter7: Problem Analysis, GUI Development& Testing

This chapter examines the possible network issues and programmatic problems that could affect operation. These errors are detected and handled in code. The user interface can then be designed to cope with both normal operation and the error conditions. This approach will enhance the code and make the user GUI more robust and user friendly.

7.1 Stage 1:Setting up hotspot communications.

Fig. 7.1(a) shows the Android connection application getting ready to enter hotspot mode. When the user is ready to proceed, they press the button. Fig.7.1 (b) shows the user being asked for the SSID and Password that came with the IoT product, perhaps from a sticker on the case or a separate piece of paper. When this is entered and the "Next" button is pressed then the Android Hotspot mode is enabled with these parameters and the Android device can securely communicate with the IoT device. This proved that the code for stage 1 fully worked as intended.

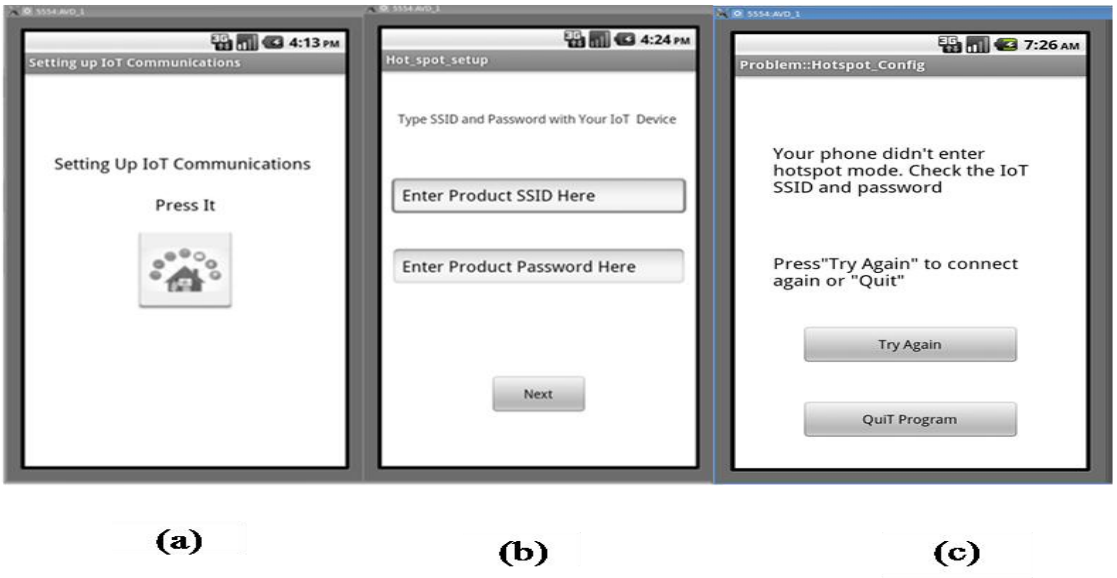

Figure 7.1 Screenshots of the connection joining mobile application :(a) Entry for setting up IoT Communications (b) Entry for hotspot setup

7.1.1.Stage 1: Programmatic error

Stage 1 set up the Android hotspot mode and it is possible for this to fail. The failure can be detected by the errors reported during the set up routines that set the Wi-Fi link to hotspot. As shown in the figure Code 1 in section 6.3 this results in an exception that can be caught by a try-catch block. Fig. 7.1(c) shows the GUI telling the use of this problem.

7.2 Stage 2: Secure transfer of LAN SSID & password:

Once the hotspot mode is enabled, communication with the IoT device is possible. Fig 7.2(a) shows the Android application asking the user for the LAN SSID and password for joining the home local network (this is the same screen as seen in 7.1(b)). When the user presses "Next" the LAN information is sent to the IoT device.

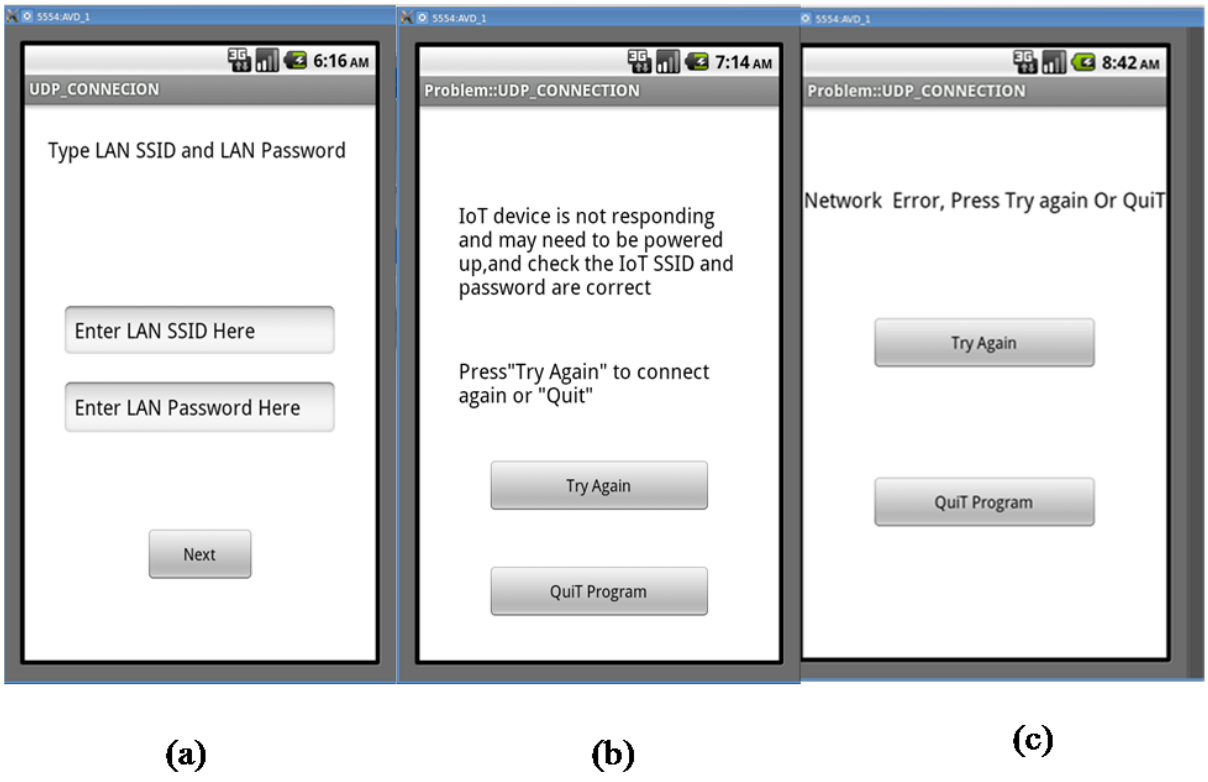

Figure 7.2 Screenshots of the Hotspot connection joining mobile application: (a) Entry for hotspot setup and (b) Entry for Unsuccessful connecting due to incorrect SSID and/or password and (c) Entry unsuccessful due to hotspots node fail and/or packet loss and/or IoT failure

The Android device knows that the IoT device is on the hotspot Wi-Fi network but not the IP address of the device. To find the IoT device the Android device sends out a UDP broadcast packet with the LAN SSID and password. The IoT device replies with an acknowledgement also by UDP.

While a TCP connection would have been preferred to ensure proper delivery of the packets this would have required knowledge of the IoT IP address

7.2.1 Errors in Stage 2

In stage, 2 there could be a number of errors-

a) The user may type in the wrong product SSID or password and so there will be no reply to the UDP packet sent to the IoT device. This problem may be detected with a simple timeout; a 1 second timeout will give the IoT device enough time to respond if it is indeed connected.

b) The UDP packet may be lost in transit. This problem may also be detected with a simple one-second timeout.

c) The phone transmit or receive routines may fail, though this is very unlikely.

Again, code can be added to cope with these problems and the appropriate GUI screen shown to the user.

Problems a) and b) are both discovered using a timeout and so the user will see screen 7.2b which informs the user that the IoT device is not responding and may need to be powered up, and to check the IoT SSID and password are correct, and then either try again or quit.

Error c) above can be detected from try-catch blocks and results in screen 7.2c which tells the user there was a network error and asks them to try again or quit.

7.3Stage 3: IoT devices connected to LAN

Both the mobile phone and the IoT device now leave the hotspot and try to join the LAN. Again the IP address of the IoT device (and mobile phone) is uncertain as IP addresses on most LANs are allocated the router using DHCP. The mobile application must find the IoT IP address and again it resorts to a broadcast message, which contains the identity of the IoT, the MAC address collected during hotspot mode. The IoT device will recognize its own unique ID and reply with its IP address and now the mobile application and IoT can communicate freely. Fig. 7.4(a) shows the screen to report the IoT and mobile phone successfully communicating via the LAN. This completes the network joining protocol activity and the mobile phone application can now enter control mode as shown in Fig. 7.4(b).

7.3.1 Errors in Stage 3

Stage 3 requires that the Android device change from hotspot mode where it is acting as a Wi-Fi access point (AP) to being a normal Wi-Fi device. It must then send a UDP packet and receive a reply from the IoT device. The errors are similar to stage 2-

a) The user may type in the wrong LAN SSID or password and so there will be no reply to the UDP packet sent. This problem may be detected with a simple timeout; a 1 second timeout will give the IoT device enough time to respond if it is indeed connected.
b) The UDP packet may be lost in transit. This problem may also be detected with a simple one second timeout.
c) The phone transmit or receive routines may fail, though this is very unlikely.

The GUI screens to report this to the user are very similar to those used in Fig 7.2b and 7.3c except that they are reported for the Home LAN not the IoT hotspot.

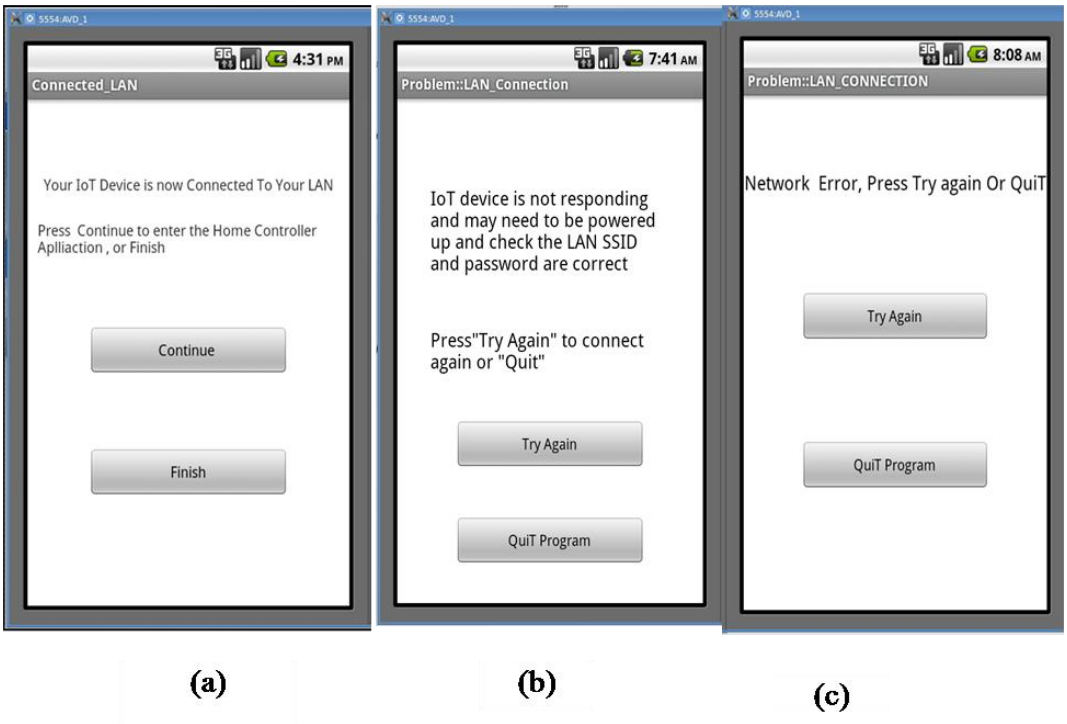

Figure 7.3 IoT devices connected to LAN :(a) Successful Connection to LAN and (b) Entry for Unsuccessful connecting due to incorrect SSID and/or password and (c) Entry unsuccessful due to packet loss and/or IoT failure

7.3.2 Limitations and Problems Encountered

In order to test the full system, the Raspberry Pi was configured to automatically run the developed code on start up. This was done with a Shell script to launch the C++ program that runs the IoT joining and communications code. Initial tests showed several problems with the IoT code. While the phone's hotspot was being configured, the IoT device would make several, failed attempts to join the phone's hotspot and would still not be able to connect once the hotspot was up and stabilised. This intermittent fault caused great confusion as troubleshooting failed to replicate earlier results of properly joining any Wi-Fi network. After much testing and analysis, it was shown that the problem was due to the power supply of the Raspberry Pinot being able to deliver the peak current requirements of the unit. Baseline

testing was repeated with a new power supply of higher capacity and the Raspberry Pi behaved in a more consistent manner.

7.4 Conclusion

This chapter has shown the implementation of the three stage networking joining protocol for IoT devices on real hardware. The initial design was tested and then enhanced to overcome programmatic problems and network problems. The final result shows that the system works well and when there are errors the user is sufficiently informed to be able to choose what to do next. The user interface is viable for typical smart phone users.

Chapter 8: Proposed Device Discovery Protocols

This thesis is focused on solving the secure network joining problem. This is only one of many problems that must be solved in order to allow IoT devices without a central controller to provide cheap home automation with a DIY experience. This chapter discusses some of these other problems to be solved in the context of being future work. While none of the proposals are complete they do point the way to very interesting new research that may be of great use to the home automation industry.

8.1 Proposed Device Discover and Control Protocol

There are no standard device discovery protocols and controlling techniques available to enable compatibility between devices from different vendors. Furthermore, existing systems have a lack of extendibility and adaptability by the end users. For example, end users should be able to add new devices on demand and end users should not depend on expert installation. This requires a new smart home access control concept. We propose [86] a novel plug and play Device Discovery and Control Protocol (DDC), which will allow and IoT device to be added to a network and be discovered by a mobile phone or personal computer acting as a temporary controller. This is done without the aid of any extra or central controller. Furthermore each IoT device will carry and XML definition of how to display its functionality and how to control the device's behaviour. This new XML standard would define the device properties, GUI display elements such as on and off buttons, and control signals to and from the IoT device.

Consider that a homeowner wants to add a mains power switch to control a floor lamp. With a traditional home automation system, the homeowner faces considerable costs starting an expert to modify the controller and associated software interfaces. The homeowner will then have to buy a power switch from the same manufacturer as the controller. In case of the

DDC protocol, anyone can purchase a device from a range of manufacturers that support the DDC protocol. An app on your phone or computer will automatically find the new device, and display the appropriate control buttons and information. Such IoT devices could be sold at a hardware store, and be installed by a homeowner in a DIY manner.

8.2 Basics of the New Device Discovery and Control protocol:

Fig.8.1.1 summarizes the process of discovering and controlling IoT devices on a home local network using the proposed DDC protocol.

Stage 1: A mobile phone or personal computer will act as a temporary controller and send a broadcast to all IoT devices requesting them to reply.

Stage 2: In this step, every IoT device will response to the controller with their identity and XML information discussed previously.

Stage 3: The controller may then ask an individual IoT for its status. For example, IoT_1in Fig. 8.1.1may be a garage door and the controller may request the status of the door. The controller may also request an action such as door close. The possible status and actions are all contained in the XML, which is uploaded from the IoT device to the controller in stage 2.

Stage 4: Devices may also be configured to send out broadcast addresses, and to respond to broadcast signals. This enables actions to occur when the temporary controller is no longer available.

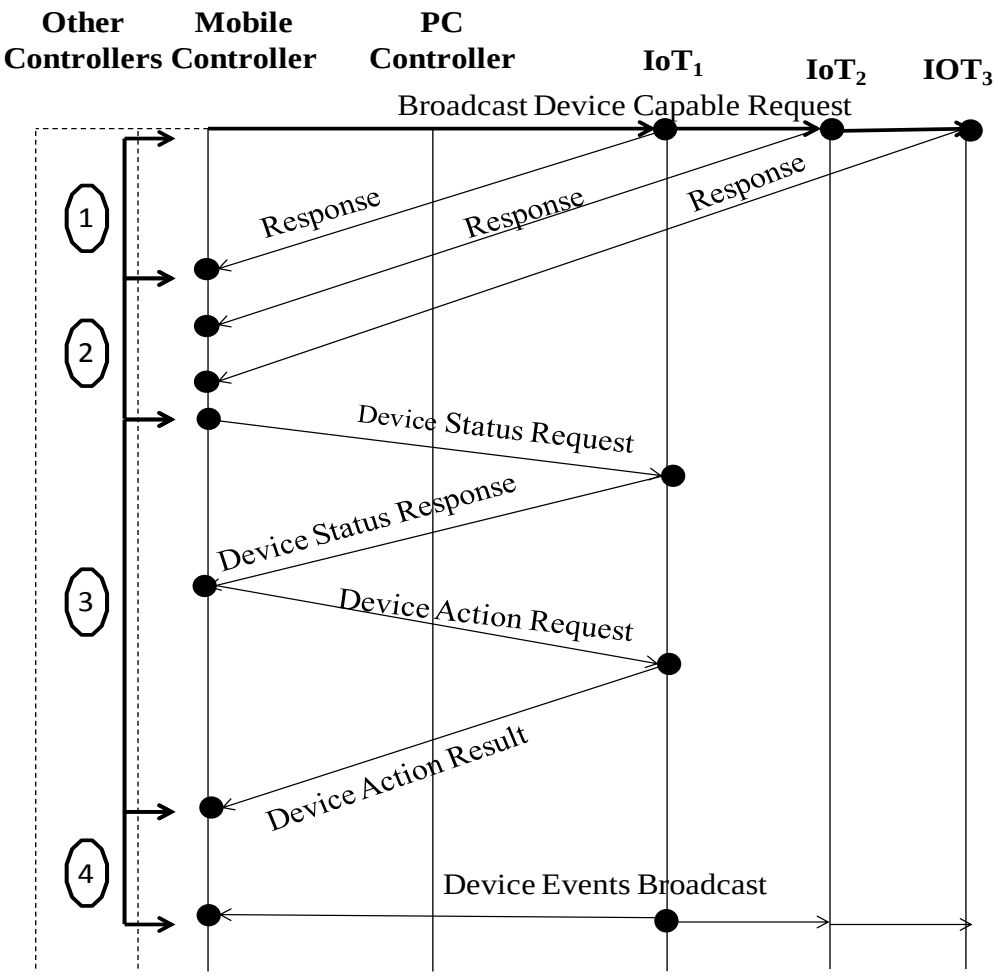

Figure 8.1.Basics of the proposed DDC protocol

Chapter 9: Conclusions and Future Works

This thesis has been driven by the research questions outlined in chapter 3.

- **Question 1**: What architecture will allow the elimination of a home automation system's central controller?

  Answer: The theoretical and practical work done has shown that a normal household LAN and a normal consumer mobile phone is an adequate architecture providing that each IoT device can support Wi-Fi and has a little intelligence. With programmable Wi-Fi, nodes now costing US$3 this has become a practical reality. There is no need for a central controller.

- **Question 2**: What architecture would allow DIY installation and additions using devices from different manufacturers?

  Answer: the same architecture as above allows DIY installation providing user-friendly protocols can be developed as below.

- **Question3**: Can existing network protocols handle the key tasks of Secure joining IoT devices or are new protocols required?

  Answer: new protocols are required if the user experience is to be made very simple and so achieve a DIY experience. This thesis has developed a new secure joining protocol, which is discussed below.

The main contribution of this thesis is that is has examined the existing literature and found no published solution to the problem of how a modest and inexpensive device can securely join a Wi-Fi network without considerable cost. Consider a mains power switch, given the existing home automation paradigm such as shown with the Google Nest thermostat application. The costs of the simple mains switch will blow out with the addition of-

a) The cost of extra hardware used just to join the home network such as a display and input device or NFC link.
b) A central controller.
c) Installation by experts.

The goal set in the research questions were to develop a novel architecture and network protocol that would enable an IoT device without these costs to securely join a home Wi-Fi network. The novel three-stage network joining protocol achieves these goals, is simple and builds on existing standard protocols. The solution has been implemented and the cost saving is considerable. An IoT device does not need a display or keyboard, and no central controller is required providing the IoT has a little intelligence and Wi-Fi capability. The process is so simple that the average householder can join an IoT device to their home Wi-Fi network without expert help thus further reducing costs. Such significant cost savings are just what is required to help IoT devices penetrate the cost sensitive home automation market.

This method is of immediate use to IoT manufacturers. The approach developed has been implemented on Android and it would be interesting to develop the same idea on iOS 7 and other operating systems.

The new network joining protocol is only one of several innovative protocols required in order to make a complete IoT based home automation system without a central controller and the Future Work chapter offers some recommendations for these new protocols.

The first is an XML definition of the IoT device capabilities, how to display the control elements on a GUI, the IoT control signals, and how to request IoT status information. This XML would be embedded within the IoT device and sent to any controller on request. The second proposal is a novel Device Discovery and Control protocol which will allow devices to be discovered, and controlled as defined by their XML.

There is still much work to be done defining the full protocols and encryption methods to suit embedded systems but this is clearly achievable. Work is continuing in this area and it is planned that the full protocol definition will be made public domain in future so as to allow multiple manufactures to produce IoT devices to this new open standard. This should result in a significant drop in the cost of home automation and so an increase in the market for home automation products.

References

[1] Agrawal, S., & Das, M. L. (2011, December). Internet of Things—A paradigm shift of future Internet applications. In *2011 Nirma University International Conference on Engineering* (pp. 1-7). IEEE.

[2] Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers*, *17*(2), 261-274.

[3] Ahuja, S., Johari, R., & Khokhar, C. (2016). IoTA: Internet of Things Application. In *Proceedings of the Second International Conference on Computer and Communication Technologies* (pp. 235-247). Springer India.

[4] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645-1660.

[5] Benson, V. (2015). Personal Information Security and the IoT: The Changing Landscape of Data privacy.

[6] Hu, S., Tang, C., Yu, R., Liu, F., & Wang, X. (2013, April). Connected intelligent home based on the internet of things. In *Information and Communications Technologies (IETICT 2013), IET International Conference on* (pp. 41-45). IET.

[7] Monnier, O. (2013). A smarter grid with the Internet of Things.*Texas Instruments White Paper*.

[8] Vermesan, O., & Friess, P. (2011). Internet of things-global technological and societal trends from smart environments and spaces to green ICT. River Publishers.

[9] Muhammad, A. P., Akram, M. U., & Khan, M. A. (2015, December). Survey Based Analysis of Internet of Things Based Architectural Framework for Hospital Management

System. In *2015 13th International Conference on Frontiers of Information Technology (FIT)* (pp. 271-276). IEEE.

[10]Gluhak, A., Krco, S., Nati, M., Pfisterer, D., Mitton, N., & Razafindralambo, T. (2011). A survey on facilities for experimental internet of things research.*IEEE Communications Magazine*, *49*(11), 58-67.

[11] Ning, H., & Wang, Z. (2011). Future internet of things architecture: like mankind neural system or social organization framework?. *IEEE Communications Letters*, *15*(4), 461-463.

[12] Darianian, M., & Michael, M. P. (2008, December). Smart home mobile RFID-based Internet-of-Things systems and services. In *2008 International conference on advanced computer theory and engineering* (pp. 116-120). IEEE.

[13] Li, X., Lu, R., Liang, X., Shen, X., Chen, J., & Lin, X. (2011). Smart community: an internet of things application. *IEEE Communications Magazine*, *49*(11), 68-75.

[14] Atzori, L., Iera, A., & Morabito, G. (2011). Siot: Giving a social structure to the internet of things. *IEEE communications letters*, *15*(11), 1193-1195.

[15] Yashiro, T., Kobayashi, S., Koshizuka, N., & Sakamura, K. (2013, August). An Internet of Things (IoT) architecture for embedded appliances. In*Humanitarian Technology Conference (R10-HTC), 2013 IEEE Region 10* (pp. 314-319). IEEE.

[16] Piyare, R. (2013). Internet of things: Ubiquitous home control and monitoring system using Android based smart phone. *International Journal of Internet of Things*, *2*(1), 5-11.

[17] Zheng, Y., Wang, H., & Li, Y. (2012). Establishment of IOT-Based Identity Recognition System. *IERI Computers Letters*, *1*(3), 57.

[18] Mandula, K., Parupalli, R., Murty, C. A., Magesh, E., & Lunagariya, R. (2015, December). Mobile based home automation using Internet of Things (IoT). In *2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)* (pp. 340-343). IEEE.

[19] Kang, B., Park, S., Lee, T., & Park, S. (2015, January). IoT-based monitoring system using tri-level context making model for smart home services. In *2015 IEEE International Conference on Consumer Electronics (ICCE)* (pp. 198-199). IEEE.

[20] JeyaPadmini, J., & Kashwan, K. R. (2015, April). Effective power utilization and conservation in smart homes using IoT. In *Computation of Power, Energy Information and Commuincation (ICCPEIC), 2015 International Conference on* (pp. 0195-0199). IEEE.

[21] Atukorala, K., Wijekoon, D., Tharugasini, M., Perera, I., & Silva, C. (2009, September). SmartEye integrated solution to home automation, security and monitoring through mobile phones. In *2009 Third International Conference on Next Generation Mobile Applications, Services and Technologies* (pp. 64-69). IEEE.

[22] Milton, M. A. A., & Khan, A. A. S. (2012, May). Web based remote exploration and control system using android mobile phone. In *Informatics, Electronics & Vision (ICIEV), 2012 International Conference on* (pp. 985-990). IEEE.

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

[24] Dou, N., Mei, Y., Yanjuan, Z., & Yan, Z. (2009, December). The networking technology within smart home system-ZigBee technology. In *Computer Science-Technology and Applications, 2009. IFCSTA'09. International Forum on* (Vol. 2, pp. 29-33). IEEE.

[25]. Baviskar, J., Mulla, A., Upadhye, M., Desai, J., and Bhovat, A. (2015), "Performance Analysis of Zigbee Based Real Time Home Automation System", Proc. Int. Conf. Communication, Information & Computing Technology (ICCICT), Mumbai, India, pp. 1-6.

[26] Al-Ali, A.R., Qasaimeh, M., Al-Mardini, M., Radder, S., and Zualkernan, I.A. (2015), "ZigBee-Based Irrigation System for Home Gardens", Proc. Int. Conf. Communications, Signal Processing, and Their Applications (ICCSPA), Sharjah, pp.1-5.

[27] Malhotra, J. (2015), "ZigBee technology: Current status and future scope", Proc. Int. conf. Comuter and Computational Sciences (ICCCS), Noida, pp. 163-169.

[28] Obaid, T., Rashed, H., Abou-Elnour, A., Rehan, M., Salah, M.M., and Tarique, M. (2014), "ZigBee technology and its application in wireless home automation systems", Intrnational Journal of Computer Networks & Communications (IJCNC), 6(4): 115-131.

[29] Shewale, A.N., and Bari, J.P. (2015), "Renewable energy based home automation system using ZigBee", International Journal of Computer Technology and Electronics Engineering (IJCTEE), 5(3): 6-9.

[30]Yan, D., & Dan, Z. (2010, August). ZigBee-based Smart Home system design. In *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*.

[31] Baviskar, J., Mulla, A., Upadhye, M., Desai, J., & Bhovad, A. (2015, January). Performance analysis of ZigBee based real time Home Automation system. In *Communication, Information & Computing Technology (ICCICT), 2015 International Conference on* (pp. 1-6). IEEE.

[32] "Nest, Google and you." January 2014 https://nest.com/blog/ -2014/01/13/nest-Google-and-you/

[33] "Nest Learning Thermostat 2nd Generation Teardown" April 2015 https://www.ifixit.com/Teardown/Nest+Learning+Thermostat+2nd+Generation+Teardown/13818.

[34] "A step-by-step guide to setup on the Nest Learning Thermostat, "April 2014; https://nest.com/support/article/A-step-by-step-guide-tosetup-on-the-Nest-Learning-Thermostat

[35] Aggarwal, C. C., Ashish, N., & Sheth, A. (2013). The internet of things: A survey from the data-centric perspective. In *Managing and mining sensor data* (pp. 383-428). Springer US.

[36] http://www.technoven.com/internet-of-things-applications-area-iot-applications/

[36] http://www.belkin.com/au/Products/home-automation/c/wemo-home-automation/

[37]http://coolpile.com/gear-magazine/belkin-wemo-home-automation-iphone-ipad-ipod-switch

[38]http://www.techhive.com/article/2900947/security/canary-the-diy-home-security-system-goes-from-crowd-funding-sensation-to-mainstream-retail-product.html

[39]http://www.technologytell.com/hometech/101408/neurio-energy-management/

[40]https://www.securifi.com/rg/almondplus

[41]https://www.engadget.com/2012/11/14/verizon-brings-wireless-monitoring-service-to-lowes-iris-smart/

[42]https://nest.com/thermostat/meet-nest-thermostat/

[43]ttp://www.tinyosshop.com/index.php?route=product/product&product_id=657

[37] https://www.cnet.com/au/products/canary-smart-home-security-device/review/

[38]http://www.computerworld.com/article/2474727/consumerization-of-it/consumerization-150407-the-internet-of-things.html

[39]http://darwinsden.com/securifi-almond-review-home-automation-hub-and-wireless-router/

[40]http://www.techhive.com/article/3017143/home-control/iris-by-lowes-second-generation-review-good-features-diverse-ecosystem.html

[41]https://nest.com/

[42] http://www.tinyosshop.com/index.php?route=product/product&product_id=657

[43] “X10 devices and standards,”http://www.x10.com.

[44] Panigrahy, S. and Wahile, S. Home Automation–Analysis of Current.

[45] Ur, B., Jung, J. and Schechter, S. *The current state of access control for smart devices in homes*. City, 2013.

[46] "EnOcean devices and standards, http://www.enoceanalliance.org/en/home/

[47] "Insteon devices and standards,"http://www.insteon.com/.

[48] "Z-Wave devices and standards,"http://www.z-wavealliance.org/.

[49] http://www.zwave.com.au/

[50] 'Philips. Hue', https://www.meethue.com, Accessed on 23 December 2015.

[51] http://www.live-smart.co/smart-home/wifi-vs-zigbee-vs-z-wave-vs-bluetooth-smart-home-standards-fully-explained-6202

[52] http://embedded-computing.com/articles/connecting-devices-to-the-internet-of-things-with-wi-fi/#

[53] http://www.networkworld.com/article/3046132/internet-of-things/wi-fi-access-for-the-internet-of-things-can-be-complicated.html

[54] https://www.bluetooth.com/marketing-branding/markets/home-automation

[55] https://www.cnet.com/au/products/kwikset-kevo-bluetooth-door-lock/user-reviews/

[56] https://www.threadgroup.org/

[57] http://www.smarthome.com.au/smarthome-blog/apple-homekit-insteon-hub-pro/

[58] Zunnurhain, Kazi."Vulnerabilities with Internet of Things." *Proceedings of the International Conference on Security and Management (SAM)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2016.

[59] https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack

[60]http://smallbusiness.chron.com/strongest-wifi-encryption-66876.html

[61] http://www.tomsitpro.com/articles/deploying-wpa2-enterprise-encryption,2-836.html

[62] http://www.comptechdoc.org/independent/security/terms/replay-attack.html

[63]https://www.wirelessdesignmag.com/blog/2012/09/software-development-tools-optimize-zigbee-performance.

[64]https://blog.ecoventsystems.com/2015/03/wirelessprotocols/

[65]http://www.electronicsweekly.com/news/design/communications/pros-cons-bluetooth-low-energy-2014-10

[66] Lee, J-S, Su, Y-W and Shen C-C A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi The 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON) Nov. 5-8, 2007, Taipei, Taiwan pp 46-51

[67]Karygannis, T , Owens L, Wireless network Security: 802.11, Bluetooth and Handheld Devices, 2002 (http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf)

[68]http://www.rfwireless-world.com/Terminology/Advantages-and-Disadvantages-of-zigbee.html

[69] Razouka,b, w., Crosbyb, G.V. Sekkakia, A., New security approach for ZigBee Weaknesses , Procedia Computer Science 37 (2014) 376 – 381

[70]https://www.alienvault.com/blogs/security-essentials/security-issues-of-wifi-how-it-works.

[71] Longbiao, C., Gang, P., and Shijian, L. (2012), "Touch driven interaction via an NFC-enabled Smartphone", Proc. Int. Conf. Pervasive Computing and Communications Workshops (PERCOM Workshops), Lugano, Switzerland, pp. 504-506.

[72] Piyare, R., & Tazil, M. (2011, June). Bluetooth based home automation system using cell phone. In *Consumer Electronics (ISCE), 2011 IEEE 15th International Symposium on* (pp. 192-195). IEEE.

[73] Kumar, S., & Lee, S. R. (2014, June). Android based smart home system with control

via Bluetooth and internet connectivity. In *The 18th IEEE International Symposium on Consumer Electronics (ISCE 2014)* (pp. 1-2).IEEE.

[74] Gurek, A., Gur, C., Gurakin, C., Akdeniz, M., Metin, S.K., and Korkmaz, I. (2013), "An Android based home automation system", Proc. Int. Conf. *High Capacity Optical Networksand Emerging/Enabling Technologies,* Magosa, pp. 121-125.

[75] Teymourzadeh, R., Ahmed, S.A., Chan, K.W., and Hoong, M.V. (2013), "Smart GSM Based Home Automation System", Proc. Int. Conf. Systems, Process & Control (ICSPC2013), Kuala Lumpur, Malaysia. pp. 306-309.

[76] ElKamchouchi, H., and ElShafee, A. (2012), "Design and Prototype Implementation of SMS Based Home Automation System", Proc. Int. conf. Electronics Design, Systems and Applications (ICEDSA), Kuala Lumpur, Malaysia, pp. 162-167.

[77] Efendi, A.M., Kyo, O.S., Negara, A.F.P., Hoang, T., and Choi, D. (2013), "Routing Approach in Ipv6 Ubiquitous Internet-Based Home Automation Network", *Future InformationCommunication Technology and Applications,* 235: 189-197.

[78] ElShafee, A., and Hamed, K.A. (2012), "Design and implementation of a Wi-Fi based home automation system", *World Academy of Sci. Eng. Technol*. 68:2177-2180.

[79] Caytiles, R.D., and Park, B. (2012), "Mobile IP-Based Architecture for Smart Homes", *International Journal of Smart Home*, 6:29-36.

[80] Sultan, M.R.G.M., Abdullah, A.M.K., Mohammad, N.H., and Abu, F.M. (2013) "Design and Implementation of a GSM Based remote home security and appliance control system", Proc. 2nd Int. Conf. Advances in Electrical Engineering, Dhaka, Bangladesh, pp. 291-295.

[81] Sharma, U., and Reddy, S.R.N. (2012), "Design of Home/Office Automation Using Wireless Sensor Network", *International Journal of Computer Applications,* 43:53-60.

[82] Atukorala, K., Wijekoon, D., Tharugasini, M., Perera, I. and Silva, C. *SmartEye integrated solution to home automation, security and monitoring through mobile phones*. IEEE, City, 2009.

[83] Felix, C., &Raglend, I. J. (2011, July).Home automation using GSM.In*Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 International Conference on* (pp. 15-19).IEEE.

[84] W. S. Lee; S. H. Hong, "Implementation of a KNX-ZigBee gateway for home automation," Consumer Electronics, 2009. ISCE '09. IEEE 13th International Symposium on, pp.545,549, May 2009 .

[85] http://www.wikihow.com/Reset-a-Netgear-Router, accessed on 23 December

References of our Published paper:

[86] S. Nasrin and P. J. Radcliffe, "Novel Protocol Enables DIY Home Automation," in *Telecommunication Networks and Applications Conference (ATNAC)*, 2014.

[87] S. Nasrin and P.J.Radcliffe, "A Novel Three Stage Network Joining Protocol for Internet of Things based Home Automation Systems", Computer Communication & Collaboration, 2016.

Appendix A: Publications

S. Nasrin and P. J. Radcliffe, "Novel Protocol Enables DIY Home Automation," in *Telecommunication Networks and Applications Conference (ATNAC)*, 2014.

S. Nasrin and P.J.Radcliffe, "A Novel Three Stage Network Joining Protocol for Internet of Things based Home Automation Systems", Computer Communication & Collaboration, 2016.

Novel Protocol Enables DIY Home Automation

Salma Nasrin
School of Electrical & Computer engineering
Royal Melbourne Institute of technology (RMIT)
Melbourne, Australia
s3471132@student.rmit.edu.au

Dr. P J Radcliffe
School of Electrical & Computer engineering
Royal Melbourne Institute of technology (RMIT)
Melbourne, Australia
pjr@rmit.edu.au

***Abstract*-Modern advances in electronics and communication technology have given rise to the development of several home automation technologies and systems. However, current home automation systems have several drawbacks including high cost and not being of a DIY nature. These issues have held back home automation and it is important to solve them. In this paper, we describe a new architecture for a home automation system, which is built on novel network protocols. Firstly, we discuss related works about existing home automation systems and their merits and demerits. Next, we introduce the proposed home automation architecture, embodying the new protocols. The new system allows a user or homeowner to purchase off the shelf devices and control them by a PC or mobile device in a very simple manner. The system does not require expert configuration or a central controller therefore the cost will be significantly reduced. An additional network device will be required for remote access but local users will not require anything apart from the controlled device and a PC or mobile device. The key enabling technology that makes this possible is an XML definition of the device capabilities, display requirements, and control signals.**

Keywords— Home automation; distributed discovery protocol, Wi-Fi, smart home, home appliances, Bluetooth

I. INTRODUCTION

The term "home automation" refers to technology in a domestic environment where technology improves the quality of the resident's life by facilitating a flexible, comfortable, healthy and safe environment. The future that people have always envisioned is available through smart appliances. Modern advances in electronics and communication technology have given rise to the development of several home automation technologies and systems [1-3] and also the miniaturization and improvement of computers systems, sensors and networking. Home automation systems can be categorized by control source; locally controlled systems and remotely controlled systems. According to [1], home automation can be useful to those who need to access home appliances while away from their home and can improve the lives of the disabled.

Mobile phone systems provide a unique opportunity to satisfy the most important required factors in home automation systems including flexibility, security, easy to use and the ability to feedback information to a remote [4, 5]. Although the previous studies tried to address the issues associated with current home automation systems there is still scope for further improvement.

Home automation systems have not met with wide acceptance or sales because there are inherent problems with all current systems including:

- Installation requires expensive experts and is not of a DIY nature thus increasing costs and delays.
- Extensions or additions also require experts to both install the hardware and adjust the user interfaces and software. There is no plug-n-play mode, which would reduce cost.
- A central controller is needed for most systems, which is an extra cost.
- Sensors and systems are proprietary thus making it impossible to pick and choose devices from a range of manufacturers. The competition of non-proprietary open standards has been shown to decrease costs and increase volumes.

These problems raise several important research questions-

1. Can any existing architecture be extended to overcome these problems?
2. Would a new architecture and protocol better solve these problems?
3. Can an open standard be developed that will enable plug-n-play using devices from different manufacturers?

This paper is structured as follows; section II examines existing work in this area with particular attention to plug-n-play style installation. Section III describes the new system with details of system architecture and the new distributed discovery

protocol. Section IV contrasts the new and existing home automation protocols and section V discusses the security model. Finally section VI provides a conclusion.

II. LITERATURE REVIEW

Considerable research has been carried out on eliminating the need for home structural changes during home automation system deployment, and to provide end users with a simple, secure and easily configurable home automation system.

Atukorala et al., [2] designed and built a real-time home automation and monitoring system named Smart Eye, which uses cellular networks, an Internet based server, networked hardware equipment and GPRS networks. Even though the systems is user-friendly and easily expandable nevertheless a central server acts as the controlling unit which is an extra cost and is not of a DIY nature; users cannot configure the system by themselves thus increasing cost.

Piyare and Tazil [6] present the design and implementation of a low cost secure cell phone based home automation system. Appliances at home are connected to an Arduino BT board. Although the system provides a flexible and wireless solution to home automation, the cost of Arduino BT board and installation issues means this is not a good solution [7] for the average householder. The architecture does not completely alleviate the intrusiveness of the installation due to the incorporation of some wired communications. There is no plug-n-play mode, which would reduce cost and provide better flexibility.

Milton and Khan [8] developed a remote exploration and control system using a web application, web server, database, GSM network, and Android mobile phone. The system gives users an easy way to monitor remote locations and control electrical devices using a website and an android phone however, the system requires expert installation and configuration of the hardware thus increasing cost.

A traditional remote mode in [9] uses a PC as a local server, which has a high cost. Moreover, this method requires the PC to be permanently power on and may limit the other programs that can be run on the PC.

A cell phone based home appliance control system is presented in [10]. The system mainly consists of two cell phones; one is remote cell phone, which calls a master cell phone, which controls the operation of the remote home appliances. The master cell uses a server, which requires some level of administration, someone who knows how to set it up, create/modify users and groups, apply security and so is not of a DIY nature. Users can not configure the system by themselves thus increasing cost.

Another home automation system based on voice recognition targeted at elderly and disabled people was built and implemented by Humaidet el. [11]. Although the system is constructed in a way that is easy to install, configure, run and maintain, it works only on a local network and has lack of distinction between local access and remote access. There is also a lack of flexibility because there is no plug-n-play mode, which would reduce cost and offer better flexibility.

Alper et al. [12] proposed an intelligent automation system using Google Cloud Messaging server and the Android operating system as useful emerging technologies for home automation. The system has three types of hardware components; local devices to be controlled, a web server and support service. Data distribution through the free public Google platform makes the system cost-effective but these systems are difficult to install. They require professionals to go to the users houses one or multiple times to install appliances and configure control systems.

Al-ali and Al-rousan [13] developed a Java based home automation system which is integrated into a personal computer based web server, physically connected to all home devices. Java technology used in the system provides a built in security. However the use of a computer and wired installation per home increase the expense of the system. Again there is no DIY capability.

Rosendahl et.al. [14] highlighted the need for home automation systems and discussed some suitable network options for home automation system. They also proposed a mobile service prototype named REMOTILE. A J2ME implementation was used in REMOTILE to describe the whole structure of mobile application. The system could control all of the device functionality remotely from a conventional mobile phone while the user was at work or one the road. The system has considerable expenses and is difficult to install, especially in legacy homes.

In summary, the home automation systems examined all fail to meet the criteria for success that were laid out in the introduction. These include installation that does not require experts and is of a DIY nature thus decreasing costs and delays. Extensions or additions should also not require experts to install the hardware or adjust the user interfaces and software. Notably none addressed the plug-n-play requirement, and at the protocol level none provided separation between local and networked access. This leads us to suggest that a new architecture is needed to overcome these problems.

III NEW SYSTEM ARCHITECTURE

This section presents the architecture of the proposed home automation system. We propose a novel home automation architecture that realizes the goal of DIY home automation. The proposed architecture provides services dynamically to appliances in a home with wireless technologies using decentralized services modules.

System Architecture

Fig 1.Shows a top down view of the proposed home automation system. Given the low cost of wireless Internet, we have used that technology for all communications, with the exception of battery-powered devices which may use Bluetooth. Each controlled device, for example a mains power switch, contains a cheap Wi-Fi interface and very limited computing capability. Such devices are already available for under US23 but they lack the new proposed protocol [15]. Note there is no central controller; as we will show no central controller is needed. Existing systems have a central controller to provide computing power and control the timing of events and coordination of several devices. In the new proposed system, each device has a Wi-Fi link and some computing power so it can handle any timing for its own activities. Coordination between devices is seldom required but if needed it is possible for a device to directly send signals to another device. This signalling must be set up via the user's mobile device or PC but once set up the user's device is no longer required.

In this system we proposed four new protocols; a network joining protocol, a distributed discovery protocol, a local control protocol and a remote access protocol. The networking joining protocol allows the controlled device to be securely added to the home network. The distributed discovery protocol allows each controller (a mobile device or PC) to find each controllable device and tells a controller how to display the device and how to control that device. The local control protocol uses the information from device discovery to control that device. The remote access protocol extends the local area network to a remote device. This new set of protocols can eliminate a central controller for a home automation system and allow users to purchase off the shelf items from a range of manufactures. All protocols provide encryption suitable for embedded devices but that will not be dealt with in this paper. The full protocol details will be explained in future papers. In this paper we focus on the novel approach whereby a device can tell a controller what to display, and how to send commands to the device. We have called this protocol the Distributed Discovery Protocol (DD Protocol).

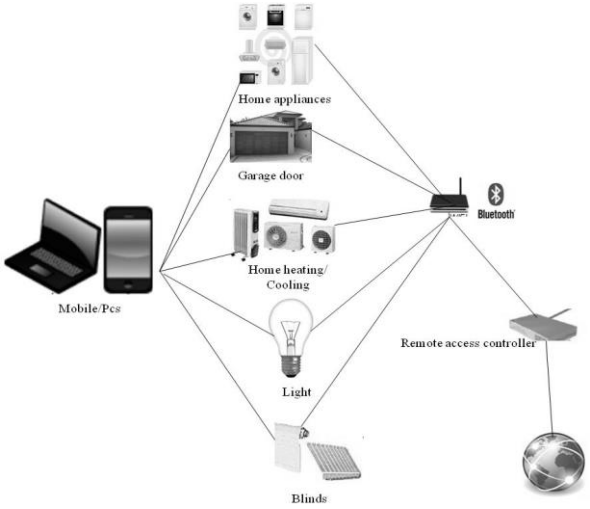

Fig. 1. Proposed home automation architecture

Distributed Discovery Protocol (DD protocol) Units

A controller may inform itself of the devices available in the house by sending out a device discovery request. Each device will then reply with a description of how to it may be displayed and controlled. For the format of this protocol we borrow from a simple yet very powerful concept used in HTML; a server sends information to the client about what should be displayed but not how to display it. Consider the following HTML fragment-

Hello, I <i>hope<\i> you are well!

The client is given text to display, and told that "hope" must be in italics. The client chooses the font, the font size, the colors, and sets the position. In a similar way, the DD protocol allows a device to tell any controller its capabilities using XML format. Consider two simple examples of a garage door opener and power switch. The device capability portion of the discovery reply might be as follows-

<device>
<manufacture_ID>Garagarama #673456<\manufacturer_ID>
<device_name writeable=yes>Garage Door<\device_name)<action control=up_button command=0x01>Door Up<\action>
<action control=down button command=0x01>Door Down<\action>
<action control=stop_button command=0x02>Door Stop<\action>
</device>

<device>
<manufacture_ID>Powercore#201401012345<\manufacturer_ID>
<device_name writeable=yes>Power Switch<\device_name)
<action

control=off_buttoncommand=0x03>Switch on<\action>
<action control=on button command=0x04>Switch Off<\action>
<status_report> On | Off<\status_report>
</device>

The controller can now choose how to display these devices, and if an option is selected by the user the command embedded in this information can be sent to the device. On a mobile phone, the DD application may choose to present a scrollable list of devices, and when one is selected the controls for that device are shown as in Fig 2. A PC with a larger screen may choose to tile the controls so all the house devices are available on one screen, which may scroll if there are many devices as shown in Fig 3.

Fig. 2. DD Protocol based application on a mobile screen

The consequences of this new DD protocol are that neither the controller nor the device need be installed by an expert. It becomes possible to buy a device off the shelf, allow it to enter the home network using the simple network joining protocol (not described in this paper), and then the device is enabled and ready for use. This process requires no expert configuration and no central controller.

Fig. 3. DD protocol based application on a PC screen

IVCONTRAST NEW AND EXISTING HOME DEVICES

Given the outline provided of the novel DD protocol it is now possible to contrast new and traditional home automation.

Case 1: Addition of a mains power switch. Consider that a home owner wants to add a mains power switch to control a floor lamp. With a traditional home automation system the home owner would have to get an expert to modify the controller and associated software interfaces. The home owner will have to buy a power switch from the same manufacturer as the controller. This is a costly process.

Now consider a DD based system. The home owner can look at a range of DD switches from a range of manufacturers and purchase the one that suits their needs. The power switch is placed between the power point and the lamp and the very simple network joining process followed. The home owner can now use their PC or mobile phone which runs a standard DD app to discover the new hardware and then control the new lamp. The whole activity is much quicker and much cheaper.

Case 2: Addition of a garage door opener. With a traditionally home automation system the home owner would have to search for a garage door opening system which was also compatible with their existing home automation system. If that was not available then first a normal garage door system would need to be installed, then an expert would be needed to add the necessary interface electronics to the controller, and adjust the controller software to cope with the new garage door.

With the DD based system the user would need to buy a simple garage door system and get it installed. They would also need to buy a DD to 433 MHz converter which can learn the commands from the key ring controller for the garage door. The converter would need to be added to the home network as per the power switch example and is then available on a PC or mobile phone app with no extra work from the home owner. Again the process is quicker and cheaper than traditional approaches.

SECURITY OF THE SYSTEM

Security is an important issue in the smart home to protect devices and sensitive information. There will be two level of security for the proposed home automation system. The first level is password access to the WLAN which will give access to devices that are not of a critical nature such as a light switch. The second level requires an additional password per device for critical devices such as a door lock. All protocols will take advantages of standard Wi-Fi security such as WPA/2.

VI CONCLUSION

This paper has described the overall architecture of a novel home automation system which allows a home owner to purchase off the shelf devices and in a very simple manner have they controlled by a PC or mobile device. There is no need for expert configuration and no need for a central controller. Remote access will require an additional network device to provide VPN access but local access does not require anything apart from the controlled devices and a PC or mobile device. The key enabling technology that makes this possible is an XML definition of the device capabilities, display requirements, and control signals. There is still work to be done refining the other protocols and encryption methods to suit embedded systems but this is clearly achievable. It is planned that the full protocol definition will be made public domain by the end of 2014 so as to allow multiple manufactures to produce devices that will work with a variety of open source applications for mobile devices and PCs. This should result in a significant drop in the cost of home automation and so an increase in the market for home automation products.

REFERENCES

[1] N. Dickey, D. Banks, and S. Sukittanon, "Home automation using Cloud Network and mobile devices," presented at the Southeastcon, 2012 Proceedings of IEEE, 2012.

[2] K. Atukorala, D. Wijekoon, M. Tharugasini, I. Perera, and C. Silva, "SmartEye Integrated Solution to Home Automation, Security and Monitoring through Mobile Phones," presented at the Next Generation Mobile Applications, Services and Technologies, 2009. NGMAST '09.Third International Conference on, 2009.

[3] S. R. Das, S. Chita, N. Peterson, B. Shirazi, and M. Bhadkamkar, "Home automation and security for mobile devices," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on*, 2011, pp. 141-146.

[4] C. Hui-Hsiung and W. Quincy, "Managing heterogeneous wireless sensor networks with the Session Initiation Protocol (SIP)," in *Advanced Communication Technology (ICACT), 2012 14th International Conference on*, 2012, pp. 1042-1045.

[5] F. Viani, F. Robol, A. Polo, P. Rocca, G. Oliveri, and A. Massa, "Wireless Architectures for Heterogeneous Sensing in Smart Home Applications: Concepts and Real Implementation," *Proceedings of the IEEE*, vol. 101, pp. 2381-2396, 2013.

[6] R. Piyare and M. Tazil, "Bluetooth based home automation system using cell phone," presented at the Consumer Electronics (ISCE), 2011 IEEE 15th International Symposium on, 2011.

[7] R. A. Ramlee, M. A. Othman, M. H. Leong, M. M. Ismail, and S. S. S. Ranjit, "Smart home system using android application," in *Information and Communication Technology (ICoICT), 2013 International Conference of*, 2013, pp. 277-280.

[8] M. A. A. Milton and A. A. S. Khan, "Web based remote exploration and control system using android mobile phone," in *Informatics, Electronics & Vision (ICIEV), 2012 International Conference on*, 2012, pp. 985-990.

[9] G. Xiang and Z. Li, "Research and Design of Smart Home System Based on Zigbee Technology," in *Artificial Intelligence and Computational Intelligence (AICI), 2010 International Conference on*, 2010, pp. 290-293.

[10] M. s. Nasr and F. Azwai, "Friendly home automation system using cell phone and J2ME with feedback instant voice messages," in *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on*, 2009, pp. 531-538.

[11] H. AlShu'eili, G. Sen Gupta, and S. Mukhopadhyay, "Voice recognition based wireless home automation system," presented at the Mechatronics (ICOM), 2011 4th International Conference On, 2011.

[12] A. Gurek, C. Gur, C. Gurakin, M. Akdeniz, S. K. Metin, and I. Korkmaz, "An Android based home automation system," in *High Capacity Optical Networks and Enabling Technologies (HONET-CNS), 2013 10th International Conference on*, 2013, pp. 121-125.

[13] A. R. Al-Ali and M. Al-Rousan, "Java-based home automation system," *Consumer Electronics, IEEE Transactions on*, vol. 50, pp. 498-504, 2004.

[14] A. Rosendahl and G. Botterweck, "Mobile Home Automation - Merging Mobile Value Added Services and Home Automation Technologies," in *Management of Mobile Business, 2007. ICMB 2007. International Conference on the*, 2007, pp. 31-31.

[15] SmartPhone Controlled Switch - LazyBone (Bluetooth) [online]. Available:http://www.tinyosshop.com/index.php?route=product/product&product_id=482 (Last Access on April 30, 2014).

Computer Communication & Collaboration (Vol. 4, Issue 3, 2016)
ISSN 2292-1028(Print) 2292-1036(Online)
Submitted on May 25, 2016
DOIC: 2292-1036-2016-03-001-68

A Novel Three Stage Network Joining Protocol for Internet of Things based Home Automation Systems

Salma Nasrin(Correspondence author)

School of Engineering

RMIT University

Swanston Street, Australia

E-mail: s3471132@student.rmit.edu.au

Peterjohn Radcliffe

School of Engineering

RMIT University

Swanston Street, Australia

E-mail: pjr@rmit.edu.au

Abstract: with the rapid progress of the Internet of Things (IoT) home automation has acquired more people's attention. The IoT push has reduced the costs and power requirements of devices which means that Wi-Fi based home automation will become more attractive. However, current home automation systems have several drawbacks including high cost, not being of a Do It Yourself (DIY) nature, and there is currently no safe way for a simple IoT device to join a LAN without the addition of extra user interface hardware. The simplest IoT devices, for example a mains power switch, could contain just a cheap Wi-Fi interface and very limited computing capability. Such devices are already available for under US23 but are not usable in the IoT context as they lack the ability to join a Wi-Fi network in a secure DIY manner. This paper describes a novel three stage network joining protocol which allows such IoT devices to securely join a Wi-Fi network even if they completely lack a user interface. The protocol is implemented using a WPA2 based LAN, an Android phone and a Raspberry Pi which represents an IoT device lacking any form of keyboard and display. The method allows cost reductions for simple IoT devices and is suitable for immediate adoption by manufacturers of IoT devices.

Keywords: Home Automation, Network Joining Protocol, Internet of Things (IoT), Raspberry Pi.

1 Introduction

The Internet of Things (IoT) is rapidly gaining interest in the world of wireless telecommunications and also promises to be one of the major factors influencing the development of home and workplace technologies [1-2]. The aim of IoT is to link the Internet with sensors and devices and so make possible a huge number of new and improved products and applications. IoT and home automation introduce new concepts and many development opportunities for the smart home [3-5]. Home automation systems consist of networked components that cooperate and that need to be coordinated.

This paper examines one particular problem that if solved will reduce the cost of IoT devices; how can IoT devices without additional hardware such as a keyboard and display join a Wi-Fi network in a safe and secure manner? The IoT device must learn of the target network SSID and password in a secure manner such that eavesdroppers cannot penetrate the network. If the device has a display and keyboard then this is a trivial operation but without such hardware the operation becomes problematic. An example of such a product is a Wi-Fi controlled mains power switch which is cost sensitive and will not be competitively priced if extra hardware is added purely for the purpose of joining the Wi-Fi network.

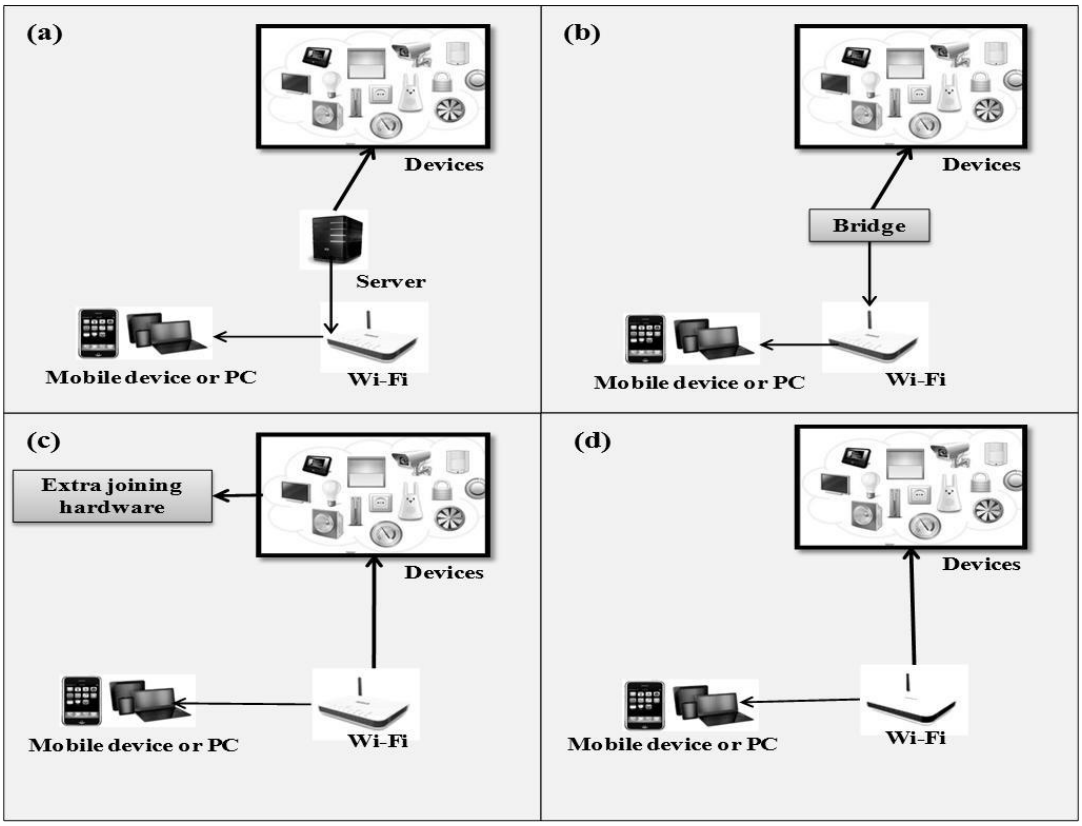

Figure 1 Home Automation Communication Architectures: (a) Server based communication architecture (b) Bridge based communication architecture (c) Extra hardware based communication architecture (d) Proposed minimalist communications architecture.

Fig. 1 (a) to (c) shows the existing solutions to this problem. Fig.1. (a) shows the server based home automation system in which a server or central controller is required. This may control an inexpensive device without display or keyboard but the cost of the server unit is a concern. A bridge based home automation system is shown in Fig. 1(b) which translates from Wi-Fi to some other protocol which does solve the network joining problem but the bridge adds an extra cost to the system. Fig.1 (c) shows a hardware joining based device where extra or enhanced hardware is added purely for the purposes of joining a Wi-Fi network, for example a display and keyboard or an NFC link. The added extra hardware is an unwanted cost that is not tenable in a competitive market.

This paper proposes an alternate scenario in Fig. 1(d) where there is no central controller and the IoT device does not have extra hardware for the purposes of joining a Wi-Fi network. Such a

System would clearly reduce costs but how can an off-the-shelf purchased device be safely connected to the Wi-Fi network, preferably without expert help? This paper examines existing work and finds that there is no published solution to this problem. This is a critical problem to solve so that devices such as mains power switches can be produced at minimal cost.

This paper proposes a number of solutions each with better security. The last solution offered is novel and allows an off the shelf device to be safely added to a network using a stock mobile phone running a simple application. While the method is simple it is novel and of immediate use to manufacturers of IoT devices.

The remainder of the paper is organized as follows. In section 2, a brief discussion of related work is provided. The overall system architecture is explained in section 3. Section 4 details a practical implementation and finally section 5 provides a conclusion and suggests some future research.

2 Related Literatures

The main theme of this paper is how devices may securely join a network but the economics of the network architecture are also of interest. The literature review is based on the four categories of home automation communications architecture discussed in the introduction and shown in Fig. 1.

2.1 Server based communication architecture

Several studies have been carried out for the server based home automation architecture using an Internet based server or Java based server, networked hardware equipment, cellular networks, Wi-Fi, GPRS networks, database, GSM network, IPv6 or Android mobile phone [6-14]. The architectures are described as user-friendly [6-7], easily joining networks as an IoT device [9], and supporting wide range of home devices [10-13]. These approaches all require a permanently powered central server or PC which is an extra cost. Additionally users cannot configure the system by themselves thus also increasing cost [6-13]. The other drawbacks include high cost due to the use of SMS messages for control and reporting of status[9], high cost due to wired installation, extra cost for development and hosting of web pages [12-13], inflexibility, poor manageability, and difficulty in achieving security [9-11].

2.2 Bridge based communication architecture

The bridge based architecture uses another protocol to solve the “joining the network” problem and provide data communication, and finally bridges to Wi-Fi. The ZigBee [15-20] home automation network consists of a coordinator, routers and several end devices. The ZigBee Alliance is made up of many vendors who made products to work with IEEE 802.15, however some users [18-19] have noted that ZigBee devices frequently have difficulty communicating with those made by different manufacturers. The combination of uncertain interoperability and the cost of a coordinator suggest that Zigbee devices may not be a useful basis for low cost IoT devices into the future [18-19].

Insteon [21] is a solution developed for home automation by Smart Labs and promoted by the Insteon Alliance. It is notable that the Insteon Starter Kit is cheaper than just the regular Insteon Hub . The Insteon app is limited and frustrating to the normal user [21]. The Insteon system may not be suitable for an IoT device as the network joining method is not published and so security is unclear.

The Philips Hue lighting system [22] offers LED light bulbs that can be switched on and off, dimmed and produces colors throughout the RGB spectrum which is controlled via a website or smart phone application The system uses ZigBee and bridges the bulbs to the Internet using an

additional ZigBee to Wi-Fi router which is an extra cost to the system. The Hue bulbs are not protected by security as strong as WPA2 and have been hacked to obtain the LAN password [23].

Like the lighting system, the door lock (Kwikset 910 TRLZW deadbolt) also communicates with a central controller that interfaces with the home network. The device and controller communicate over the Z-Wave wireless protocol [23-24]. Z-Wave devices are accessed via Z-Wave controllers, which may act as hubs to control any number of devices within a home. One serious problem is that if someone is allowed into the home temporarily they could conceivably take ownership of the device by pressing the control button and easily re-pairing the lock with a different Z-Wave controller. All Z-Wave modules are produced by a single manufacturer, Sigma Designs, which brings into question long term supply. Another problem is that Z-wave use protocols and devices adhering the Z-Wave standard, thus requiring additional devices to be installed both at the home and to the devices that are to be automated [18].

2.3 Extra joining hardware (Bluetooth, NFC, and Wi-Fi) based communication architecture

This category uses extra or enhanced hardware to achieve joining the Wi-Fi network. The only purpose of this extra/enhanced hardware is to join the network.

Chen et al. [25] published a paper on NFC-enabled smart phones, which have been utilized in home automation where three smart home applications, namely Touch&Connect, Touch&Listen and Touch&Watch, were introduced to improve the digital lifestyle of home users. However, operation of these touch-driven NFC smart home applications was neither quick nor convenient because users have to physically walk to NFC tagged devices and tap with the NFC enabled Smartphone before using the device.

Kumar and Lee [26] proposed an Android based smart home system using Bluetooth and Arduino. This system is based on the Arduino micro web server as the main controller. The paper suggests usage of a mobile application based on the Android OS. The approach used Bluetooth and the RESTful based web services as an interoperable layer. The main advantage of this system is that it is flexible and scalable solution. The most important disadvantage of this system is that it is limited to Bluetooth communication which has a limited range and requires extra hardware, such as the siren nRF24L01+ radio module, which is used in order to communicate and coordinate actions with the other sensor nodes within the environment.

Google [27] bought the Nest based smart thermostat that learns how best to control the heating system for the smart home. This device has a display unit and also has a rotary selector for any data entry, and uses this to join a Wi-Fi network. In order to join a network the thermostat lists the available networks in its display and the rotary selector is used to select a network and enter a password. While the Nest thermostat is clever, there is a non-trivial cost for the display and rotary selector which would not be appropriate for low end devices such as a mains power switch.

2.4 Analysis of the existing systems

All the systems described above, and many others, are expensive and may require experts to install or modify the system which is another large expense. Many systems require a personal computer to be permanently active and there is no suitable way to easily connect an IoT device which lacks input devices such as a keyboard and display. None of the systems allow a home owner to install or add to the system in a DIY (Do It Yourself) manner. If such a system were possible then costs to the consumer would drop and home automation may become much more affordable and popular.

2.5 Features of the proposed minimalist communications architecture

This paper proposes a minimalist architecture for home automation system with simple network joining protocol. There is no central controller in our proposed system and the IoT devices do not have extra hardware purely for the purpose of joining the Wi-Fi network. Existing work is examined and found that no published solution matches this flexible and low cost architecture.

3 System Architecture

This section describes the design of the minimalist network architecture and the required network protocol that satisfies the architecture shown in Fig 1(d). Figure 2 shows the overall architecture of the proposed home automation system. Each device has a Wi-Fi link and some computing power so it can handle any timing for its own activities. This approach eliminates the need for a central controller and so significantly reduces cost.

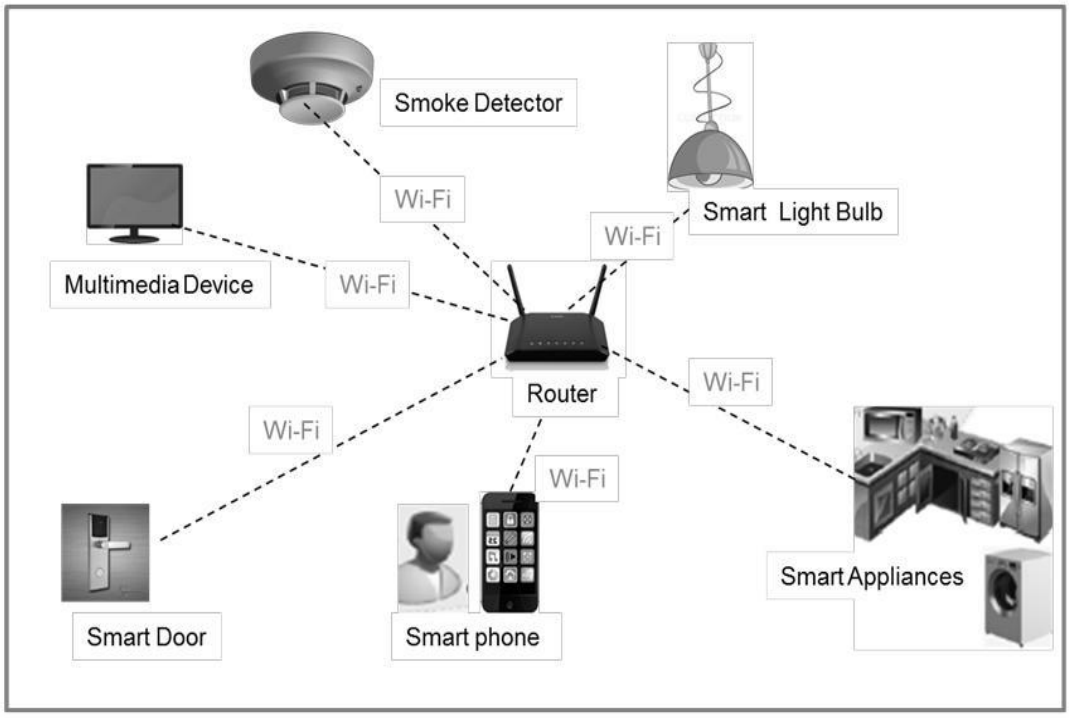

Figure 2 Proposed Home Automation System Architecture

Figure 3 shows a new three stage network joining protocol that enables a simple Wi-Fi IoT device to join a LAN in a secure manner. Fig. 3(a) shows the initial link being setup between the mobile phone and the IoT as a hotspot. This is all done using WPA2 which is secure and then provides a secure WPA2 encoded link from mobile phone to the IoT. Attackers would need to break WPA2 to get anything useful. Fig.3 (b) shows that the mobile device passing the Local Area Network (LAN) SSID and password to the IoT devices via the WPA2 protected hotspot link. Attackers would like to obtain the SSID and password but again cannot get any of this information without the ability to break WPA2 or knowledge of the IoT password. Fig.3(c) shows that both IoT and mobile device have changed their Wi-Fi to the LAN and both can communicate with each other, and any other LAN device.

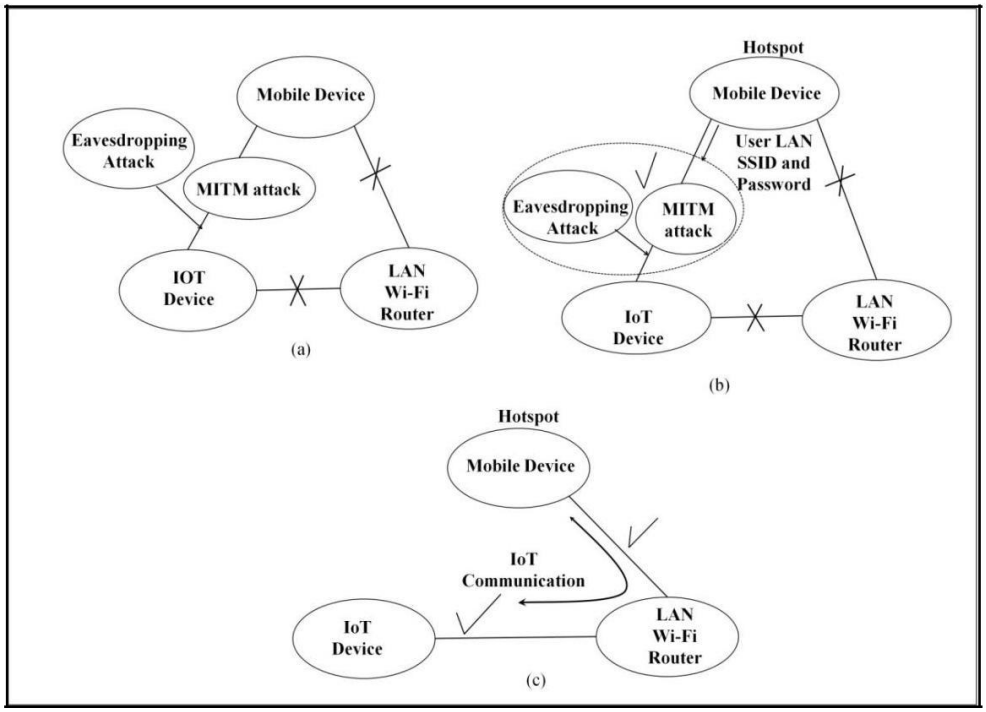

Figure 3 Three stages in IoT joining Protocol: (a) secure mobile to IoT connection established. (b) Transfer of LAN SSID and (c) Final state with IoT device joined to the LAN.

The basic three stage network protocol has not addressed the important issue of how the IoT SSID and password are set up. Here we offer 3 solutions, the first offered while simple and economic has flaws which may be acceptable in low security situations. The last solution offered is robust and its security is only limited by the limits of the Wi-Fi encryption protocol. All solutions rely on a mobile phone that can act as a Wi-Fi hotspot. Mobile phones should not be regarded as an extra cost as they are already owned by most home owners and are only required for the short process of joining the network. A mobile phone hotspot is intended to link a PC directly to a mobile phone using Wi-Fi, and then via the phone's 3G/4G link to the internet. There is a necessary hotspot side effect which is of great use; applications running on the mobile phone can also communicate with applications running on the PC or other Wi-Fi connected device.

Solution 1: An IoT device is configured with a default pre-defined SSID and password set by the manufacturer at the factory. One problem with using the default SSID is that some confusion might result if a company or home owner next door sets up an IoT device at the same time. Hackers would soon know the default information, post it on the web, and so hackers world-wide would be listening for just such a connection. They would then be able to capture the LAN SSID and password as it passed from mobile phone to IoT.

Solution 2: Consider that the simple IoT device can use otherwise unused combinations of existing device buttons to initiate joining a LAN resulting in some variation on the default connection information. Wired routers use this approach to joining a secure network; usually a paper clip can be used to push a hidden reset switch and the router then is set to a known IP address and password [28]. This only works for wired routers because the method of joining the network requires a physical cable link to a PC, which is assumed to have no listeners. The IoT device must use the Wi-Fi link and this may well have listeners. When the hotspot tries to send the LAN SSID and password to the IoT device an attacker can listen in and try variations on the default connection information. It does not seem possible to devise a scheme using just a few keys on the Wi-Fi IoT

device that could not be followed by an intelligent attacker who understands the basic variation algorithm. The cracking need not even be real time. The packet transfers could be recorded and cracked after the event to get the LAN SSID and password.

Solution 3: The manufacturer provides a unique SSID and password for each IoT device. In the final outgoing test, the IoT device gets a random SSID and PW which is printed and packed with the device. This approach provides a user friendly way to provide a secure link between mobile phone and IoT where the attacker cannot break the Wi-Fi security and get the LAN SSID and password. It comes at minimal cost to the supplier and the resulting security is only limited by the nature of the Wi-Fi security (most likely WPA2).

4 System Implementation & Testing

This section shows a successful implementation of the new 3 stage protocol using an Android phone and a Raspberry Pi to represent an IoT device. The user interface requirements can be seen to be minimal and within the capability of most mobile phone users.

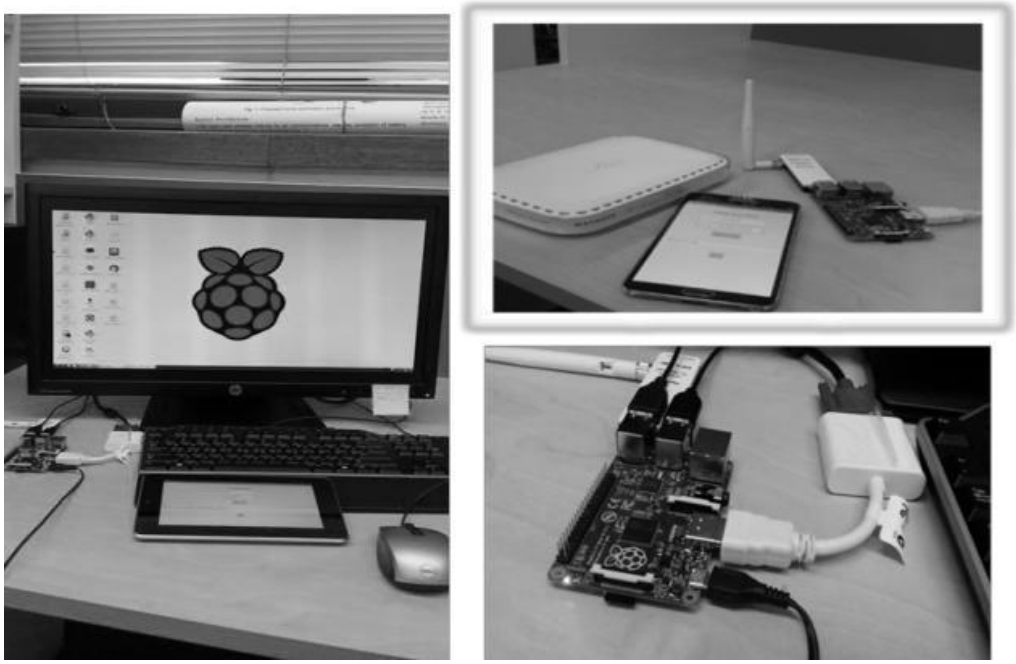

Figure 4 : Testing application with IoT device (Raspberry Pi, Wi-Fi router and Android device)

Fig. 4 shows the devices selected to implement the test bed; a current Android phone, a domestic wireless router, and a Raspberry Pi to represent an IoT device. The Raspberry Pi has IO capabilities well in excess of a dumb IoT device but only the Wi-Fi link was used for the purposes of demonstrating the feasibility of the protocol. The Android device was programmed using Eclipse and ADT. The Raspberry Pi was running Linux and had a small C program to respond to the Wi-Fi communications. This research used a Samsung Galaxy Note3 with Android version 4.4.2 but any phone capable of being a hotspot would be suitable.

There are two methods by which the Android phone can be configured as a hotspot; manual configuration [29] and configuration performed by an application program. The long sequence of manual steps may prove difficult for the average consumer and the process may be simplified by using an application to drive the entry to hotspot mode. Once the hotspot is enabled; communication with the IoT device (Raspberry Pi) can be initiated. As a starting point the IoT device should be turned on and the IoT Communications application should be started on the mobile phone

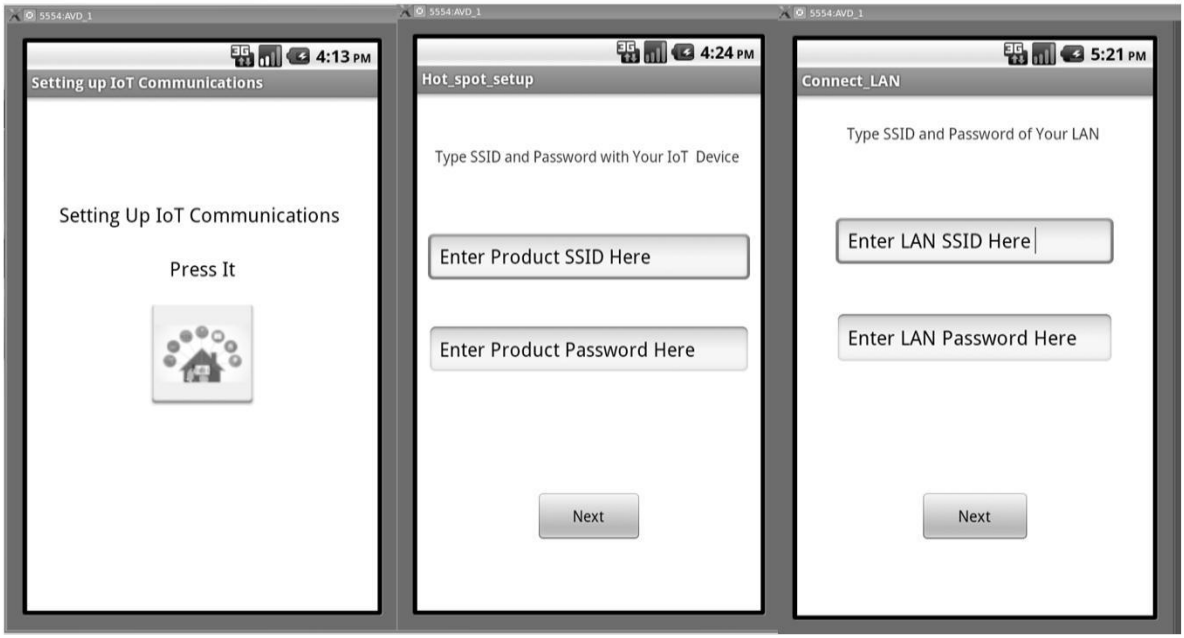

Figure 5 Screenshots of the connection joining mobile application:

(a) Entry for setting up IoT Communications (b) Entry for hotspot setup

(c) Entry for connecting to LAN.

Stage 1: Hotspot Connection: Fig. 5(a) shows the Android connection application getting ready to enter hotspot mode. If this is successful then image 5(b) appears. Fig.5 (b) shows the user being asked for the SSID and Password that came with the IoT product, perhaps from a sticker on the case or a separate piece of paper. When this is entered and the "Next" button is pressed then the Android Hotspot mode is enabled with these parameters and the Android device can securely communicate with the IoT device. At this point the IoT device and the mobile application can communicate with a fixed port address but the IoT IP address may vary. To solve this problem the Android device sends a broadcast message asking for the IoT device to identify itself. The IoT device answers this request with a unique identity and from the IP packet header the Android application will know the IP address of the IoT device.

Stage 2: Secure transfer of LAN SSID & password: Once the hotspot mode is enabled and the IoT device has replied, further communication with the IoT device is possible. Fig 5(c) shows the Android application asking the user for the LAN SSID and password for joining the local network.
When the user presses "Next" the LAN information is sent to the IoT device.

Stage 3, IoT devices connected to LAN: Both the mobile phone and the IoT device now leave the hotspot and try to join the LAN. Again, the IP address of the IoT device (and mobile phone) is uncertain as IP addresses on most LANs are allocated using DHCP. The mobile application must find the IoT IP address and again it resorts to a broadcast message, which contains the identity of the IoT. The IoT device will recognize its own unique ID and reply with its IP address and now the mobile application and IoT can communicate freely. Fig. 6 (a) shows the screen to report the IoT and mobile phone successfully communicating via the LAN. This completes the network joining protocol activity and the mobile phone application can now enter control mode as shown in Fig. (6b). The display and control activity is beyond the scope of this paper.

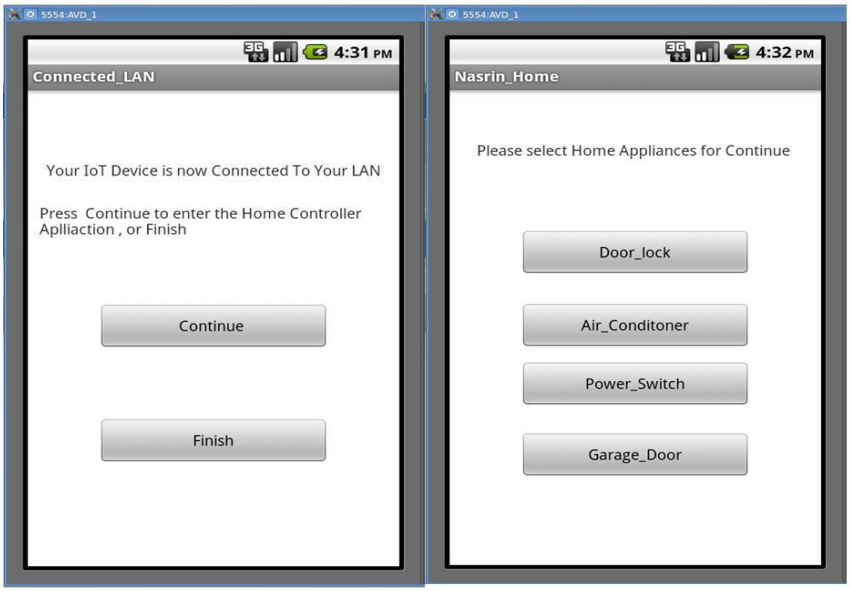

Figure 6 Successfully LAN Connection:

(a) Successful Connection to LAN (b) Further IoT Control

This implementation demonstrates that the proposed network joining protocol can be implemented on real hardware and that the user interface requirements can be streamlined to meet the expectations and capabilities of the average every day user who can operate a mobile phone. Even though a Raspberry Pi was used for the IoT device the limited resources used show that an IoT device with just a Wi-Fi interface and no other hardware can be securely connected to a LAN. The proposed network joining protocol is thus a very cost effective solution that will reduce costs for cost sensitive IoT devices such as mains powered switches.

5 Conclusions and Future Work

This paper has examined the existing literature and found no published solution to the problem of how a very simple and inexpensive device can securely join a Wi-Fi network without the added cost of a central controller or additional hardware. Consider a mains power switch, the addition of a display and input device or NFC link capable of helping join a LAN would significantly affect the price. The goal set in Fig.1 was that an IoT device without such extra hardware should be able to securely join a Wi-Fi network. The novel 3 stage network joining protocol offered in this paper achieves these goals, is simple and builds on existing standard protocols.

The solution has been implemented and the cost saving is considerable. In reference to Fig. 1, the IoT device does not need a display or keyboard, and no central controller is required providing the IoT has a little intelligence. Such significant cost savings are just what is required to help IoT devices penetrate the cost sensitive home automation market. This method is of immediate use to IoT manufacturers.

While the method proposed is very simple and within the capability of most home owners it may be possible to build on this method to simplify the connection process even further. In the real world of home owners it is of great importance to minimize the complexity of any task in order to ensure the home owner can get the product to work and reduce the cost of support that a manufacturer must provide.

The approach developed has been implemented on Android and it would be interesting to develop the same idea on iOS 7 and other operating systems.

References

[1]. Asghar, M. H., Mohammad zadeh, N., and Negi, A. (2015), "Principle application and vision in Internet of Things (IoT)", Proc. Int. Conf. *Computing, Communication & Automation(ICCCA),* Noida, pp. 427-431.

[2]. Singh, V.K., Kushwaha, D.S., Singh, S., and Sharma, S. (2015), "The Next evolution of the Internet—Internet of Things", *Int. J. Eng. Res. Computer Sci. Eng. (IJERCSE*), 2(1): 31-35.

[3]. Gubbi, J., Buyya, R., Marusic, S., and Palanaswami M. (2013), "Internet of Things (IoT): A vision, architectural elements, and future directions", *Future Generation Comp. Sys*. 29(7): 1645-1660.

[4]. Benson, V. (2015), "Personal Information Security and the IoT: The Changing Landscape of Data privacy", *Computer Communication & Collaboration.* 3(4):15-19.

[5]. Hu. S., Tang, C., Yu, R., Liu, F., and Wang, X. (2013), "Connected intelligent home based on the Internet of Things", Proc. IET Int. Conf. Information and Communications Technologies (IETICT), Beijing, pp.41-45.

[6]. Gurek, A., Gur, C., Gurakin, C., Akdeniz, M., Metin, S.K., and Korkmaz, I. (2013), "An Android based home automation system", Proc. Int. Conf. *High Capacity Optical Networksand Emerging/Enabling Technologies,* Magosa, pp. 121-125.

[7]. Milton, M.A.A., and Khan, A.A.S. (2012), "Web based remote exploration and control system using android mobile phone", Proc. Int. Conf. Informatics, Electronics & Vision (ICIEV), Dhaka, Bangladesh, pp. 985-990.

[8]. Teymourzadeh, R., Ahmed, S.A., Chan, K.W., and Hoong, M.V. (2013), "Smart GSM Based Home Automation System", Proc. Int. Conf. Systems, Process & Control (ICSPC2013), Kuala Lumpur, Malaysia. pp. 306-309.

[9]. ElKamchouchi, H., and ElShafee, A. (2012), "Design and Prototype Implementation of SMS Based Home Automation System", Proc. Int. conf. Electronics Design, Systems and Applications (ICEDSA), Kuala Lumpur, Malaysia, pp. 162-167.

[10]. Efendi, A.M., Kyo, O.S., Negara, A.F.P., Hoang, T., and Choi, D. (2013), "Routing Approach in Ipv6 Ubiquitous Internet-Based Home Automation Network", *Future Information Communication Technology and Applications*, 235: 189-197.

[11]. ElShafee, A., and Hamed, K.A. (2012), "Design and implementation of a Wi-Fi based home automation system", *World Academy of Sci. Eng. Technol*. 68:2177-2180.

[12]. Caytiles, R.D., and Park, B. (2012), "Mobile IP-Based Architecture for Smart Homes", *International Journal of Smart Home*, 6:29-36.

[13]. Sultan, M.R.G.M., Abdullah, A.M.K., Mohammad, N.H., and Abu, F.M. (2013) "Design and Implementation of a GSM Based remote home security and appliance control system", Proc. 2nd Int. Conf. Advances in Electrical Engineering, Dhaka, Bangladesh, pp. 291-295.

[14]. Sharma, U., and Reddy, S.R.N. (2012), "Design of Home/Office Automation Using Wireless Sensor Network", *International Journal of Computer Applications*, 43:53-60.

[15]. Baviskar, J., Mulla, A., Upadhye, M., Desai, J., and Bhovat, A. (2015), "Performance Analysis of Zigbee Based Real Time Home Automation System", Proc. Int. Conf.

[16]. Withanage, C., Ashok, R., Yuen, C., and Otto, K. (2014), "A Comparison of the Popular Home Automation Technologies", Proc. Int. conf. Innovative Smart Grid Technologies - Asia (ISGT Asia), Kuala Lumpur, Malaysia, pp. 600 – 605.

[17]. Al-Ali, A.R., Qasaimeh, M., Al-Mardini, M., Radder, S., and Zualkernan, I.A. (2015), "ZigBee-Based Irrigation System for Home Gardens", Proc. Int. Conf. Communications, Signal Processing, and Their Applications (ICCSPA), Sharjah, pp.1-5.

[18]. Malhotra, J. (2015), "ZigBee technology: Current status and future scope", Proc. Int. conf. Computer and Computational Sciences (ICCCS), Noida, pp. 163-169.

[19]. Obaid, T., Rashed, H., Abou-Elnour, A., Rehan, M., Salah, M.M., and Tarique, M. (2014), "ZigBee technology and its application in wireless home automation systems", *International Journal of Computer Networks & Communications (IJCNC)*, 6(4): 115-131.

[20]. Shewale, A.N., and Bari, J.P. (2015), "Renewable energy based home automation system using ZigBee", *International Journal of Computer Technology and Electronics Engineering (IJCTEE)*, 5(3): 6-9.

[21]. Panigrahy, S., and Wahile, S. (2015), "Home Automation–Analysis of Current", *InternationalJournal of Advances in Computer Science and Technology (IJACST)*, 4(1): 08–14.

[22]. 'Philips. Hue', https://www.meethue.com, Accessed on 23 December 2015.

[23]. Ur, B., Jung, J., and Schechter, S.(2013), "The Current State of Access Control for Smart Devices in Homes", Proc. Workshop on Home Usable Privacy and Security (HUPS), Newcastle, UK., pp. 1-6.

[24]. WORKS, H. (2016), "KwiksetSmartcode 914 Deadbolt with Home Connect", [Online] Available at: http://www.kwikset.com/products/details/electronic-locks/914-trl-zw-15-ul.aspx?productseo=914-trl-zw-15-ul (accessed on 23 December, 2015)

[25]. Longbiao, C., Gang, P., and Shijian, L. (2012), "Touch driven interaction via an NFC-enabled Smartphone", Proc. Int. Conf. Pervasive Computing and Communications Workshops (PERCOM Workshops), Lugano, Switzerland, pp. 504-506.

[26]. Kumar, S., and Lee, S.R. (2014), "Android based smart home system with control via Bluetooth and internet connectivity", Proc. Int. Sym. *Consumer Electronics (ISCE 2014)*, JeJu Island, Korea, pp.1-2.

[27] https://nest.com, accessed on 23 December 2015.

[28] http://www.wikihow.com/Reset-a-Netgear-Router, accessed on 23 December 2015.

[29] http://www.wikihow.com/Turn-Your-Android-Phone-Into-a-Wi-Fi-Hotspot, accessed on 23 December 2015.