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.

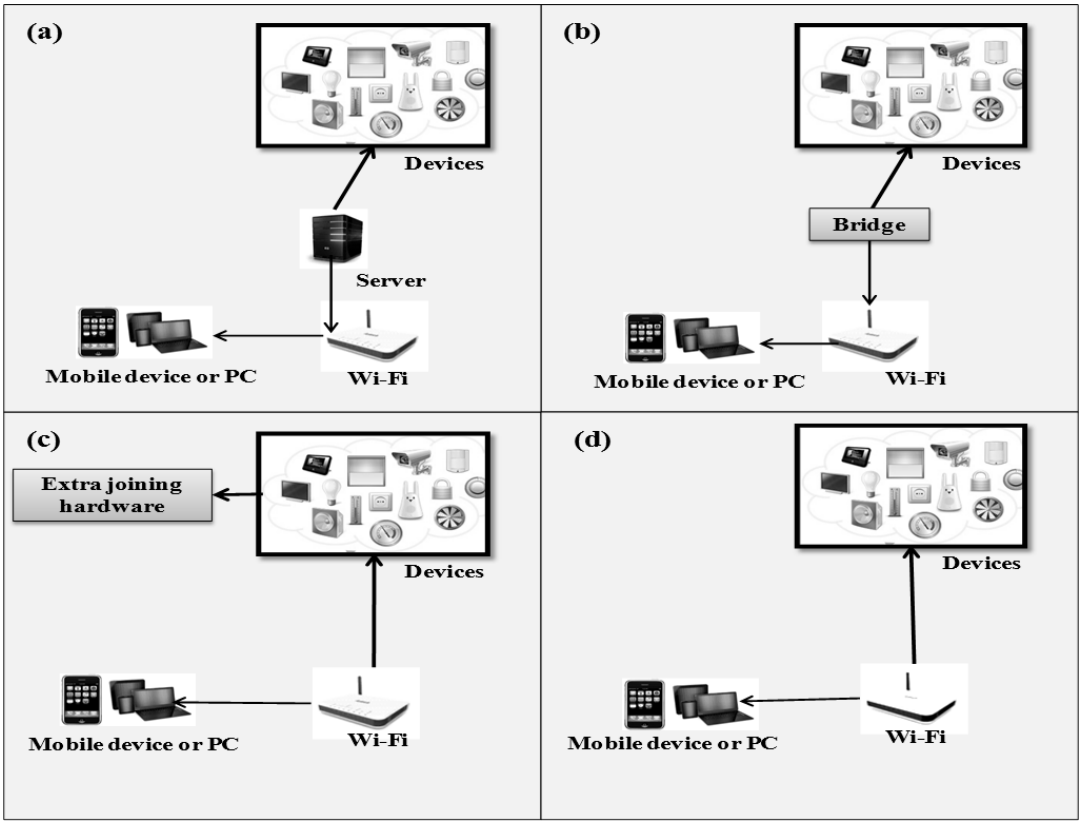

Figure 1 Home Automation Communication Architectures: (a) Server based communication architecture (b) Bridge based communication architecture (c) Extra hardware based communication architecture (d) Proposed minimalist communications architecture.

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 Literature

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.

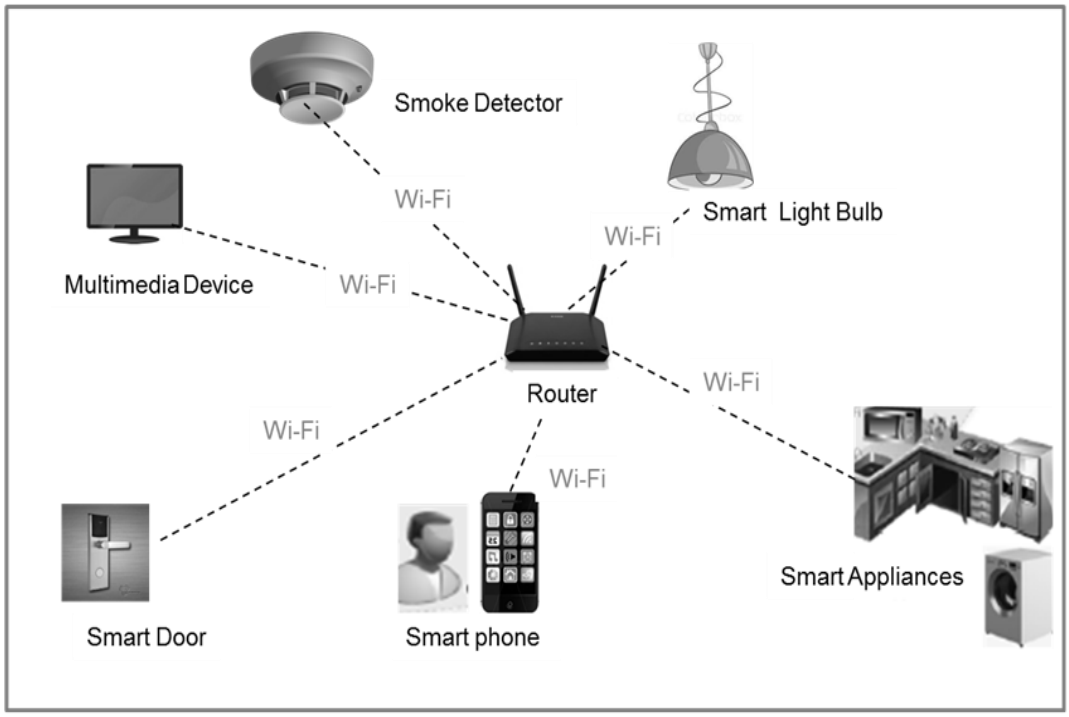

Figure 2 Proposed Home Automation System Architecture

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.

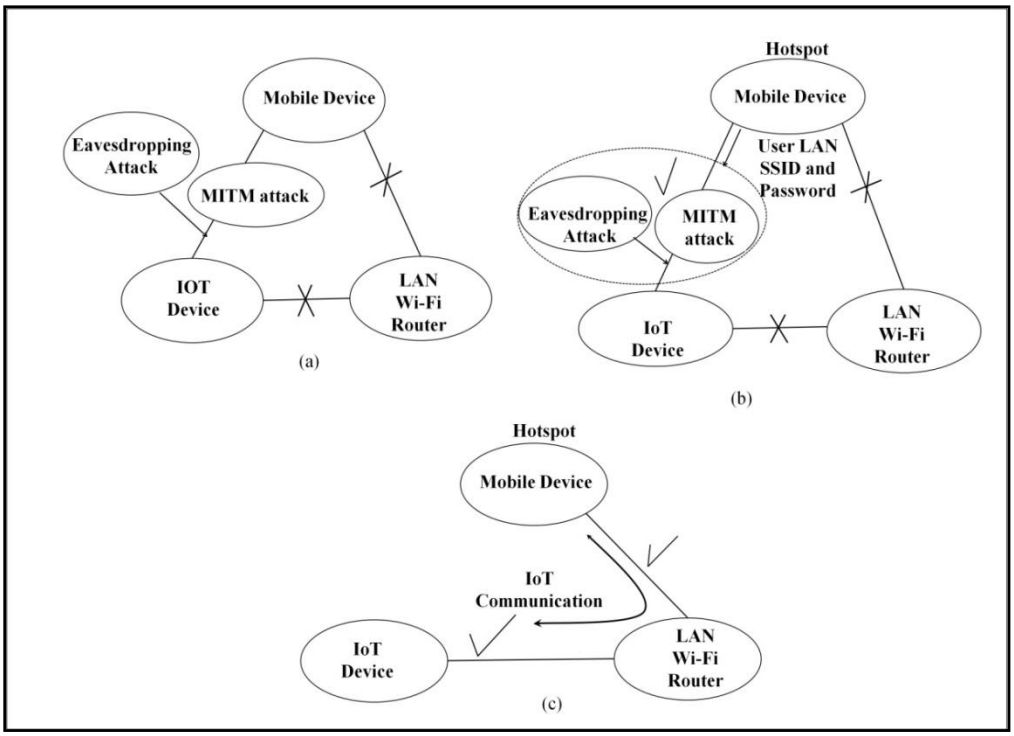

Figure 3 Three stages in IoT joining Protocol: (a) secure mobile to IoT connection established. (b) Transfer of LAN SSID and (c) Final state with IoT device joined to the LAN.

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.

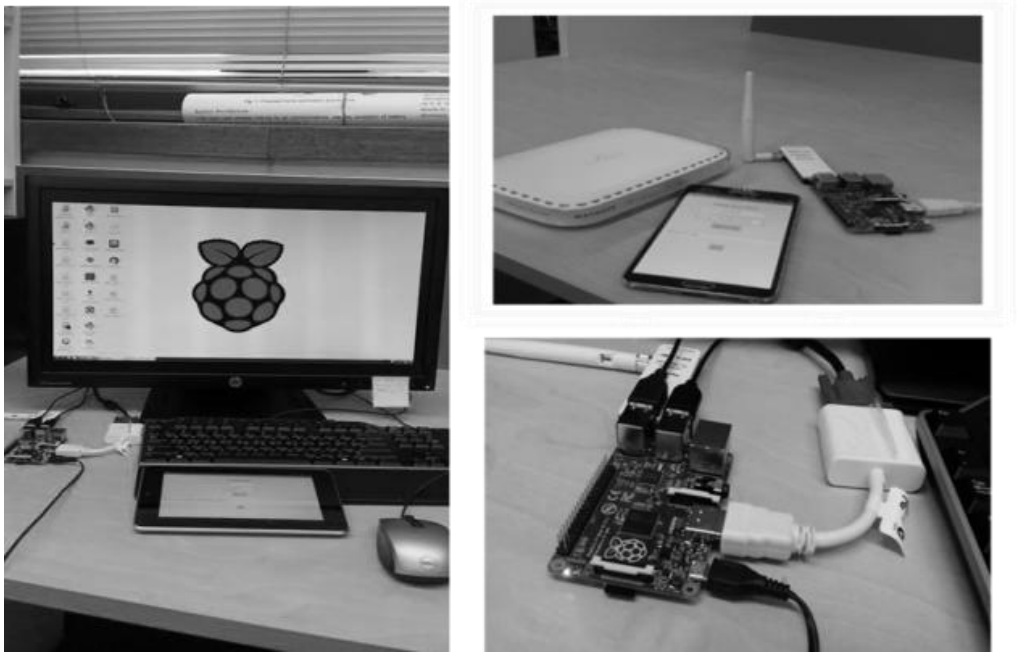

Figure 4 Testing application with IoT device (Raspberry Pi,Wi-Fi router and Android device)

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

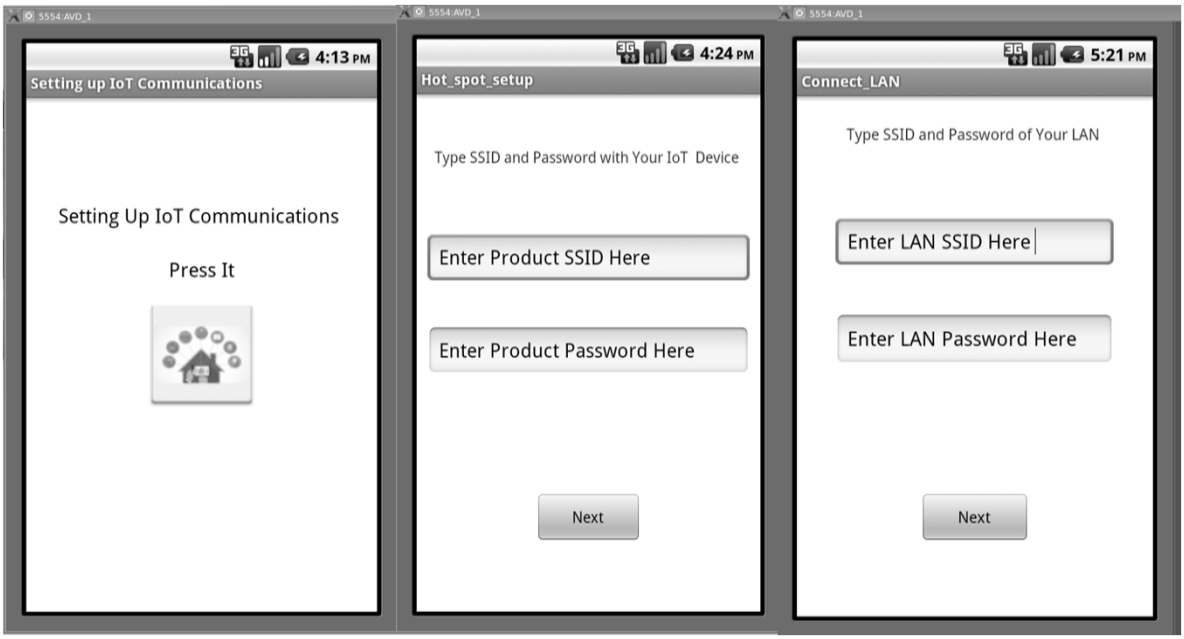

Figure 5 Screenshots of the connection joining mobile application:

(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.

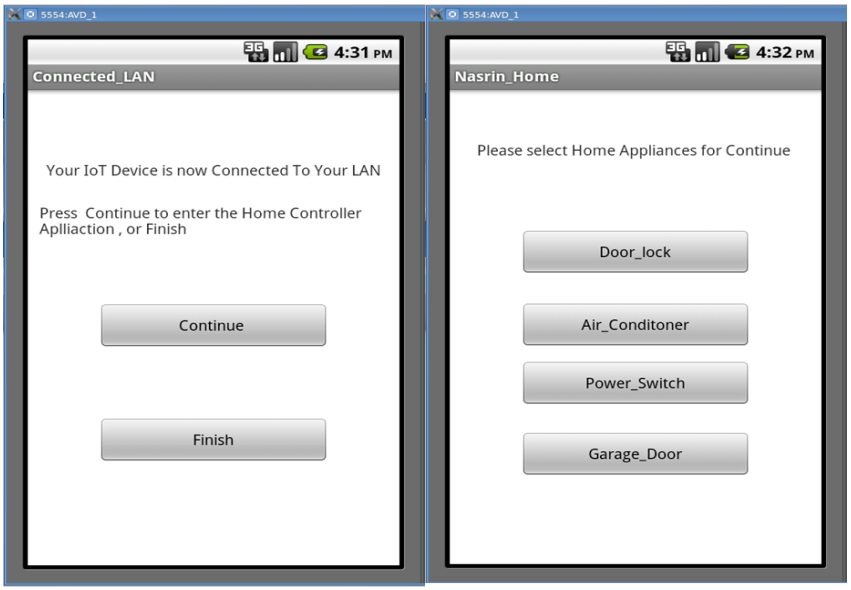

Figure 6 Successfully LAN Connection:

(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., Mohammadzadeh, 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 Networks and 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.

Communication, Information & Computing Technology (ICCICT), Mumbai, India, pp. 1-6.

[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", *International Journal 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.