Wireless and Mobile Communications (WMC)
Mekelweg 4,
2628 CD Delft
The Netherlands
http://ens.ewi.tudelft.nl/

CAS-2012-00

M.Sc. Thesis

Wi-Fi Direct based Smart Set-up (WDSS) in Lighting Systems

Ning Zhang

Abstract

The Wireless Lighting Control System has drawn intensive attention in the recent years due to the potential for huge cost savings as well as increased convenience. Commonly seen Wireless Lighting Control Systems utilize ZigBee, KNX and Z-WAVE, whereas little attention has been given to Wi-Fi because of unsolved limitations. One of the primary limitations of conventional Wi-Fi technology in lighting domain is that the complex setup procedure prevents interface-constrained devices (e.g.lamps) from joining the network. Secondly, the multi-hop Wi-Fi network is not standardized, therefore the common Wi-Fi network bears a star topology with only one-hop coverage.

The contribution of this thesis project is to develop a Wi-Fi Direct based Smart Setup (WDSS) mechanism, which is an newly designed application-layer protocol, aiming to make Wi-Fi an appropriate candidate for the Wireless Lighting Control System.

WDSS is an innovative solution backward compatible with Wi-Fi infrastructure, developed on a newly standardized Wi-Fi technology called Wi-Fi Direct, which is being rolled out as standard in Smartphones and other Internet devices. To overcome the first limitation of conventional Wi-Fi, WDSS defines a protocol to allow easy commissioning of constrained devices (lamps) in a Wi-Fi network, adding a major ease of install element to a traditional Wi-Fi based system. An additional advantage of the WDSS is that it can also be applied to set up a multi-hop network among lamps in infrastructure mode. This feature well addresses the second issue, thereby guaranteeing the effective coverage.

As part of this project, a demo was set up and the WDSS method has been tested on this system. Results showed that the WDSS has significant value in the Wireless Lighting Control System, in terms of easy commissioning, compatibility with standard Wi-Fi infrastructure, applicability on random chipsets, and transparency to the Internet Protocol. The usage of WDSS of course can be easily expanded to other similar applications.

***Keywords*–Networked Lighting System, Constrained devices, Smart Set-up, Multi-hop Wi-Fi Network**

Wi-Fi Direct based Smart Set-up (WDSS) in Lighting Systems

THESIS

submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE

in

TELECOMMUNICATIONS

by

Ning Zhang
born in Shannxi, China

This work was performed in:

Wireless and Mobile Communications (WMC) Group
Department of Telecommunications
Faculty of Electrical Engineering, Mathematics and Computer Science
Delft University of Technology

Delft University of Technology

Delft University of Technology
Department of
Telecommunications

The undersigned hereby certify that they have read and recommend to the Faculty of Electrical Engineering, Mathematics and Computer Science for acceptance a thesis entitled **"Wi-Fi Direct based Smart Set-up (WDSS) in Lighting Systems"** by **Ning Zhang** in partial fulfillment of the requirements for the degree of **Master of Science**.

Dated: May, 15th, 2012

Chairman:

Prof.dr.ir. I.G.M.M. Niemegeers

Advisors:

Prof.dr.ir. I.G.M.M. Niemegeers

Dr.Cheng Guo

Committee Members:

Dr.Huijuan Wang

Jamie Mc cormack

Michael Verschoor

Abstract

The Wireless Lighting Control System has drawn intensive attention in the recent years due to the potential for huge cost savings as well as increased convenience. Commonly seen Wireless Lighting Control Systems utilize ZigBee, KNX and Z-WAVE, whereas little attention has been given to Wi-Fi because of unsolved limitations. One of the primary limitations of conventional Wi-Fi technology in lighting domain is that the complex setup procedure prevents interface-constrained devices (e.g.lamps) from joining the network. Secondly, the multi-hop Wi-Fi network is not standardized, therefore the common Wi-Fi network bears a star topology with only one-hop coverage.

The contribution of this thesis project is to develop a Wi-Fi Direct based Smart Setup (WDSS) mechanism, which is an newly designed application-layer protocol, aiming to make Wi-Fi an appropriate candidate for the Wireless Lighting Control System.

WDSS is an innovative solution backward compatible with Wi-Fi infrastructure, developed on a newly standardized Wi-Fi technology called Wi-Fi Direct, which is being rolled out as standard in Smartphones and other Internet devices. To overcome the first limitation of conventional Wi-Fi, WDSS defines a protocol to allow easy commissioning of constrained devices (lamps) in a Wi-Fi network, adding a major ease of install element to a traditional Wi-Fi based system. An additional advantage of the WDSS is that it can also be applied to set up a multi-hop network among lamps in infrastructure mode. This feature well addresses the second issue, thereby guaranteeing the effective coverage.

As part of this project, a demo was set up and the WDSS method has been tested on this system. Results showed that the WDSS has significant value in the Wireless Lighting Control System, in terms of easy commissioning, compatibility with standard Wi-Fi infrastructure, applicability on random chipsets, and transparency to the Internet Protocol. The usage of WDSS of course can be easily expanded to other similar applications.

Keywords–**Networked Lighting System, Constrained devices, Smart Set-up, Multi-hop Wi-Fi Network**

Acknowledgments

I would like to thank my advisors Prof.dr.ir. I.G.M.M. Niemegeers and Dr.Cheng Guo for their assistance during the writing of this thesis, and my supervisors from Philips Lighting, Jamie Mc cormack and Michael Verschoor, for their help and support of this project. Without them, this would not have been possible.

Ning Zhang
Delft, The Netherlands
May, 15th, 2012

Contents

List of Figures

List of Tables

Glossary

AP: An infrastructure-mode 802.11

Access Point Client: An end Device which connects to a WLAN or virtual Access Point

Credential: A data structure issued by an AP to an Enrolee, allowing the latter to access the network

Constrained Device: A Device without a screen or buttons, making it unable to connect to a legacy WLAN by itself

Commissioning Tool: An advanced device which can be used to connect and control constrained devices

Device: An independent physical or logical entity capable of communicating with other Devices across a LAN or WLAN

Enrolee: A Device seeking to join a WLAN. Once an Enrolee obtains a valid credential, it becomes a Client of the WLAN

Find Phase: A phase in P2P Discovery that is used to ensure that two simultaneously searching P2P Devices arrive on a common channel to enable communication

Listen Channel: The channel chosen from the set of Social Channels, which is used by a P2P Device to be discoverable

Legacy Client: An end device that is Wi-Fi Certified, but not P2P compliant

Migration: Using a Commissioning Tool to move Constrained Devices from a P2P network to a WLAN

P2P Client: A P2P Device that is connected to a P2P Group Owner [2]

P2P Device: WFA P2P certified device that is capable of acting as both a P2P Group Owner and a P2P Client [2]

P2P Discovery: A capability that provides a set of functions to allow a device to easily and quickly identify a device and its services [2]

P2P Group Owner: An "AP-like" entity that may provide and use connectivity between Clients [2]

P2P Network: A network formed by Wi-Fi Direct Devices [2]

Scan Phase: The process in P2P Discovery to collect information about surrounding devices or networks by scanning all supported channels

Search State: A state in the Find Phase in which a P2P Device sends Probe Request frames on the Social Channels

Social Channel: A subset of commonly available channels in the 2.4 GHz band (1, 6, and 11)

SSID: Service Set Identifier, usually used as a name of the WLAN

Virtual AP: A P2P Group Owner with AP functionality, will be seen as an AP by other Clients

WLAN: A Wi-Fi network

WLAN API: Application Programming Interface used to manage WLAN settings, including basic functions such as discovery, connect, disconnect, etc.

WLAN Profile: An xml file which contains the information of the WLAN, including the SSID and Passphrase

Acronym

AES: Advanced Encryption Standard
AODV: Ad hoc On-Demand Distance Vector
AP: Access Point
API: Application Programming Interface
CT: Commissioning Tool
DHCP: Dynamic Host Configuration Protocol
DSR: Dynamic Source Routing
EAP: Extensible Authentication Protocol
GO: Group Owner
GTK: Group Transient Keys
MANET: Mobile Ad-hoc Network
MIC: Message Integrity Code
NAT: Network Address Translation
OLSR: Optimized Link State Routing Protocol
PSK: Pre-shared Key
PTK: Pairwise Transient Keys
P2P: Peer to Peer
SAE: Simultaneous Authentication of Equals
SSID: Service Set Identifier
STA: Station
TKIP: Temporal Key Integrity Protocol
WDSS: Wi-Fi Direct Based Smart Setup
WEP: Wired Equivalent Privacy
WLAN: Wireless Local Area Network
WPA: Wi-Fi Protected Access
WPA2: Wi-Fi Protected Access II
WPAN: Wireless Person Area Network
WPS: Wi-Fi Protected Setup

1 Introduction

1.1 Background

Lighting is an indispensable part of our daily life for both practical and aesthetic usage. In recent years, the LED light has drawn intensive attention due to the benefits in terms of efficiency, color, size and lifetime. The rise of LED offers a great many opportunities for lighting, boosting the deployment of Wireless Lighting Control Systems. It is believed that wireless Lighting is the future of the Lighting industry, offering the potential for huge cost savings as well as increased convenience. As a core component of the Wireless Lighting Control System, Wireless Communication Technologies are receiving new attention thus becoming interesting research topics.

Several Wireless Communication Technologies have been applied to Home Automation and Lighting Systems, for instance ZigBee, KNX and Z-WAVE. Despite fitting the low data rate and low energy consumption lighting networks, they still face issues such as incompatibility with IP protocols, security threads, and lack of support on major consumer electronics.

Among all the Wireless Communication Technologies, Wi-Fi has established itself as the primary one for Internet and networked media access for consumer electronics, smart phones, and IT equipment in both the professional and consumer domains. Due to the strong foothold in these markets, the enormous chipset volumes, and the transparency to the Internet Protocol, Wi-Fi is an interesting option for IP-based Home Automation and Building Control solutions.

Although Wi-Fi has excelled in the field of Internet-based applications, little attention is given to it when it comes to less intelligent networks (e.g. Lighting Systems), because of several unsolved limitations, which are to be explained in next section. Since Wi-Fi is no doubt the main trend of future wireless communications, altering Wi-Fi into an appropriate candidate for lighting control remains a difficult, but worth solving problem.

1.2 Problems

Wi-Fi was originally designed for relatively high data rate applications e.g. the Internet Services, with a typical data rate as high as 54 Mbps. It uses IEEE 802.11 radio technologies, works on 2.4 GHz frequency band (or/and 5 GHz). It is common for us to connect our laptops to a Wi-Fi network to access the Internet, so that we can browse web pages, stream audio/videos, and share files with our friends. It well meets the

communication requirements of PC/smartphone formed wireless networks. However, when it comes to the Lighting System, where most devices (e.g.lamps, sensors) are less intelligent, i.e. without display/buttons, Wi-Fi is not able to be directly deployed using its conventional commissioning methods.

There are several limitations of conventional Wi-Fi technology, which are holding it back from being properly applied to the Lighting Control System.

One of the primary disadvantages of Wi-Fi is the complex network set-up ("network join") procedure, which was designed for devices with graphical user interfaces in mind. The complex set-up process is an inherent result of a relatively high security level, which on the other side, is a major advantage of Wi-Fi. However, when adopted in the Lighting System, this complex set-up process becomes a primary issue, in that it prevents those interface-constrained devices (e.g.lamps and sensors) from joining the network, letting alone establishing a well-connected wireless lighting network.

The second limitation of Wi-Fi is that the multi-hop network is not standardized. Common Wi-Fi network bears a 1:1 or 1:n star topology, with a single hop coverage of typically 30-50m from the Access Point to the end device. This effective coverage can be worse due to obstacles or interference. In a typical lighting application scenario e.g.a 150m∗150m smart store, this single hop coverage would be insufficient to cover the whole deployment area. Therefore this limitation makes Wi-Fi less competitive in the lighting domain than its counterparts that support mesh networking.

1.3 Purpose

In order to overcome the limitations of conventional Wi-Fi stated in previous section, this thesis project aims to:

1) develop a Wi-Fi Direct based Smart Set-up (WDSS) method, to securely connect a constrained device (lamps) to an existing Wi-Fi network, without pushing a button or entering passphrase on the constrained device

2) apply the WDSS method to extend a single-hop Wi-Fi network to a multi-hop Wi-Fi among lamps, thereby guaranteeing network coverage.

1.4 Scope

The primary goal of WDSS is to bring constrained devices into an existing Wi-Fi network in a simple and secured way. The scope of this report is limited to Networked Lighting Systems. Lamps with Wi-Fi chips will be taken as an example of constrained devices without physical input interfaces. This report will explain in detail how lamps can be connected to the legacy Wi-Fi network, with the lamps intact installed on the ceiling. Applications can be easily expanded to other similar constrained devices like printers, game consoles, and sensors.

The protocol used in WDSS supports WPA2-Personal networks and Open (no security) networks. WPA2-Enterprise networks require more sophisticated mechanism. This project is primarily aimed at home and small business Wi-Fi networks.

1.5 Design Approach

WDSS defines a protocol to allow easy commissioning of lamps (and/or other devices) in a Wi-Fi network, adding a major ease of install element to a traditional Wi-Fi based system (without requiring the user interface on lamps). This approach utilizes a third device, namely a Commissioning Tool (CT), to set up a Wi-Fi Direct link to the lamp, and further instruct the lamp to migrate to an existing Wi-Fi Network in a secured fashion.

The architecture of WDSS is shown in Figure 1.1. WDSS is an application protocol developed on the basis of Wi-Fi Direct and Wi-Fi Protected Setup (WPS), which also makes use of TCP/IP protocols. General Wi-Fi chipsets support the lower layer functionalities of Wireless Communication. Wi-Fi Direct is a newly released standard based on legacy Wi-Fi, with software upgrade to support 'Virtual Access Point' function. WPS is a mechanism proposed by Wi-Fi Alliance for the sake of easy network setup. WDSS inherits functions from both Wi-Fi Direct and WPS, meanwhile bringing in new features superior to similar solutions.

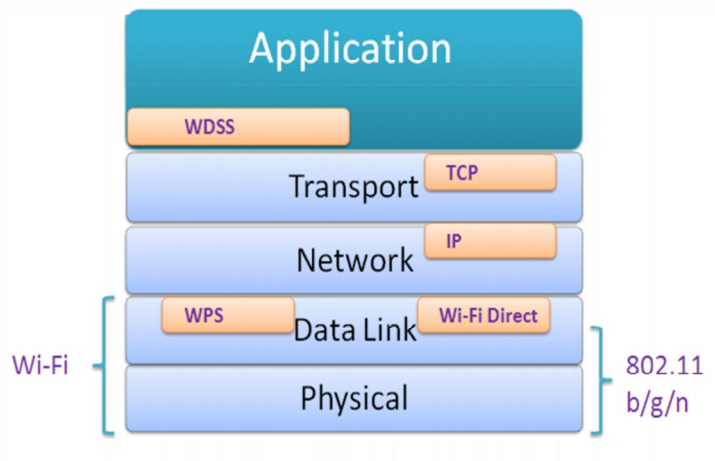

Figure 1.1: Architecture overview of WDSS and other Protocols

The WDSS program was developed in Visual Studio 2008, which can be easily installed in Wi-Fi chipsets. As part of the project, a demo was set up to simulate the functionalities of WDSS. WDSS is a generic solution fully compatible with different types of commodity chipsets. In the demo, a mixture of Wi-Fi chipsets were used, such as AR9271 provided by Atheros and Intel(R) WiFi Link 5100 AGN. AR9271 has an open program source code of Wi-Fi Direct which enables further modification [5]. Intel(R) WiFi Link 5100 AGN is an internal wireless card, which supports Wi-Fi Direct features

on the software layer. All types of devices in the demo were simulated by computers, but the approach can be applied to embedded devices without a user interface.

The primary emphasis of this project is placed on the network set-up, which provides a prototype of a Wi-Fi Networked Lighting System. This mechanism can also be applied to other similar applications; however, they will not be explained in details in this report.

1.6 User Experience

A good technical solution has to be validated by proper user experience. This section introduces two scenarios to illustrate the WDSS user experience. More details will be given in Chapter 4.

1.6.1 Enrol a constrained device into a WLAN

Context 1: the user has a newly purchased lamp and a smartphone. They all bear Wi-Fi chipsets and have WDSS software installed. The user wants to use the smartphone to enrol this lamp into an existing Wi-Fi Network (Figure 1.2).

Steps:

1. User turns on the lamp.
2. User turns on the smartphone. The smartphone discovers the lamp automatically and shows its name in a list.
3. User selects the target lamp to connect. The smartphone prompts the user for the lamp's PIN, found on a label attached to the package. The user enters the PIN on the smartphone to set up a link between the lamp and the smartphone.
4. User selects a name of the Network he/she wants to enrol the lamp into from the Wireless Connection list, and clicks on a virtual button on the software to migrate the lamp to the Wi-Fi Network.
5. After the lamp successfully migrates to the existing Wi-Fi network, a confirmation is shown on the smartphone.

Lamps can also be migrated all at once as a group.

1.6.2 Establishing a Multi-hop Wi-Fi Network

Context 2: the user has a router at home in the study. Lamps in this room are well connected to the router, but a lamp in the living room has no good Wi-Fi reception due to the limited Wi-Fi coverage. Since installing a second router is not handy at this

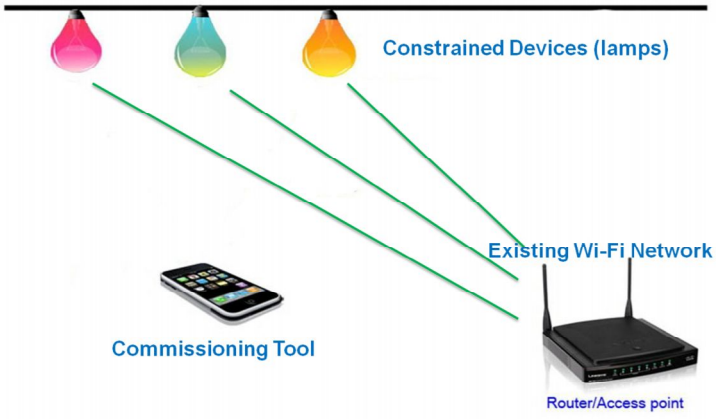

Figure 1.2: User Scenario 1: Using a Commissioning Tool (e.g.smartphone) to enrol lamps into a Wi-Fi Network

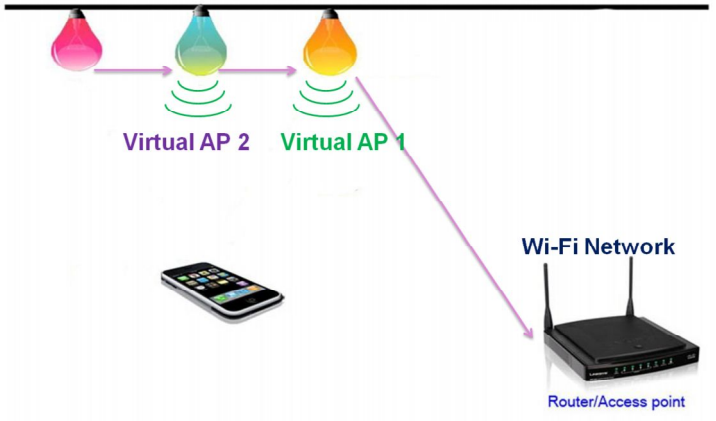

Figure 1.3: User Scenario 2: Using a Commissioning Tool (e.g.smartphone) to establish a multi-hop Wi-Fi network among lamps

moment, he wants to use an intermediate lamp to relay signals to the second lamp in the living room via a multi-hop Wi-Fi network (Figure 1.3).

A multi-hop Wi-Fi network can be established by repeating the process of Context 1, only differentiating at linking the second lamp to the intermediate lamp (Virtual Access Point), instead of the real router, to form up a chain network with devices end to end connected. Operations are similar to the first context. Concrete steps will be introduced in Chapter 4.

1.7 Outline

This report is constructed in 7 chapters. Chapter 1 gives a brief introduction of this thesis project, including the problems we want to overcome, aims and objectives of

the work, and the approach to be used. Chapter 2 provides a literature review on the Wireless Lighting Control System, comparing our approach with previous solutions to specify the innovation. Chapter 3 focuses on the Wi-Fi Direct standard we are making use of. Chapter 4 describes two user scenarios of WDSS mechanism to illustrate how it is applied to the Lighting System. Chapter 5 introduces WDSS method from technical perspective. As part of this project, a demo was set up to validate the applicability of WDSS. Based on this demo, some measurements were conducted and the results are shown in Chapter 6. Chapter 7 summarizes the main achievement of the thesis and the contributions of the work, leading to directions for further research.

Literature Review 2

2.1 Wireless Communication Technologies in the Lighting Control

In the recent years, Wireless Technologies are receiving more and more attention in the Lighting System, due to their power saving, intelligence and convenience. Wireless Lighting Control Systems utilizing ZigBee standard are already well known in the consumer electronics market. ZigBee is an open WPAN (Wireless Personal Area Networks) standard based on the IEEE 802.15.4 protocol. ZigBee standard was created aiming for low data rate, low latency and very low energy consumption for long battery lives and for large device arrays. Nevertheless, a big disadvantage of ZigBee as well as other similar known solutions is the incompatibility with IP protocols. Therefore these Wireless Lighting Control Systems have to rely on a bridge to interoperate with Internet-based services. Besides, other aspects such as security threads and lack of standardized deployment on general electronics also remain as obstacles for more extensive usage.

Originating from 1985, Wi-Fi has become a mature wireless standard over decades of proof. Wi-Fi was originally created to meet the requirements of relatively high bit rate and large bandwidth. Currently Wi-Fi is the primary Wireless Communication Technology which is extensively utilized in the Internet Services because of its excellent capabilities and transparency to Internet protocols [7]. Therefore, Wi-Fi has the potential to make a big contribution to the union of the Lighting Control and the Internet backbone, which is apparently the main trend in the future.

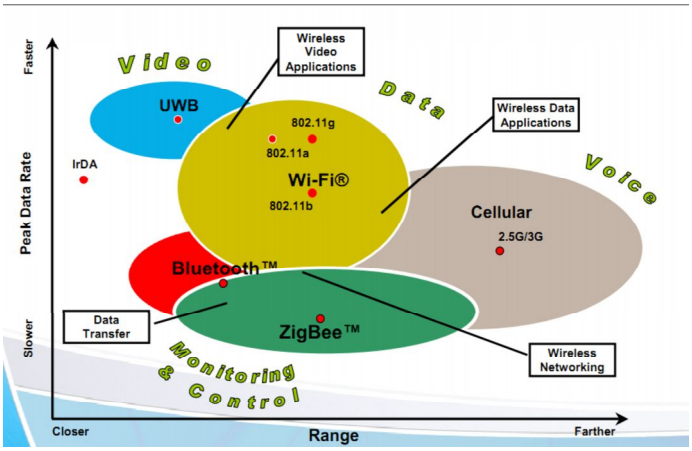

Figure 2.1: Overview of Wirless Communication Technologies

An overview of different Wireless Communication Technologies is shown in Figure 2.1 [4]. As Wi-Fi is extensively available in the market and applicable in a versatile modes and profitable ways, exploring the Wi-Fi Networked Lighting System has significant value in both academic and industrial domains.

2.2 Limitations of Wi-Fi Technology in the Lighting Control

2.2.1 Complex network set-up procedure

Despite the excellent performance in most Internet-based services, Wi-Fi has several limitations which are holding it back from being applied to the Lighting domain. **One of the primary disadvantages of Wi-Fi is the complex network set-up ("network join") procedure, which was designed for devices with graphical user interfaces in mind, makes constrained devices in the Lighting System (e.g.lamps) difficult to join the network.** To illustrate the procedure, the steps to connect a Windows PC or laptop to a Wi-Fi network are described:

1. Wi-Fi Access Points broadcast their SSIDs ("network identifiers") which are detected by each Wi-Fi device in communication range. Windows is able to display the list of detected Wi-Fi networks. Assuming no default network is defined, the user has to select the network he/she wants to connect to and click on "connect".

2. A window may prompt the user to type in the passphrase. After successful authentication, the PC/laptop is connected to the network via the Access Point (router).

The complexity of authentication is an inherent result of the underlying security mechanism of Wi-Fi. Wi-Fi uses WPA/WPA2 mechanisms for security protection. In the phase of access control and authentications, the Personal Mode uses a PSK (Pre-Shared Key) and doesn't require a separate authentication for users, while the Enterprise Mode requires the users to be separately authenticated by using the Extended EAP. It is a paradox that WPA/WPA2 brings strong security protection to Wi-Fi networks while adding complexity to network set-up. Figure 2.2 lists the security mechanisms for Wi-Fi [15].

Strong security is a requirement on Wi-Fi Certified devices, but enabling it has up to now been somewhat difficult. According to a survey from the Wi-Fi Alliance, 2 in 5 consumers still have not activated the security on their Wi-Fi network. 44% of consumers described activating security on a Wi-Fi network as moderately to very difficult (2007). As more and more consumers adopt Wi-Fi, ease of setup and protecting networks is more important than ever. Especially when we want to adopt Wi-Fi in the Lighting System, the paradox has to be smartly addressed, of course without sacrificing security.

	802.1x Dynamic WEP	Wi-Fi Protected Access (WPA)	Wi-Fi Protected Access 2 (WPA2)
Access Control	802.1X	802.1X or Pre-Shared Key	802.1X or Pre-Shared Key
Authentication	EAP methods	EAP methods or Pre-Shared Key	EAP methods or Pre-Shared Key
Encryption	RC4	TKIP (RC4)	AES / TKIP

Figure 2.2: Security Mechanisms of Wi-Fi

2.2.2 No standard Multi-hop Wi-Fi network

The second issue of conventional Wi-Fi in lighting usage is that the multi-hop network is not standardized. A normal Wi-Fi or Wi-Fi Direct Network has a 1:1 or 1:n star topology, with a single hop coverage of typically 30-50m from the AP to the Client.

Methods have been developed to use Wi-Fi repeaters relaying signals of each AP, in order to extend the effective coverage of Wi-Fi. A Wi-Fi repeater, also called range extender, is used to broaden the range of a Wi-Fi network. A Wi-Fi repeater works by receiving the Wi-Fi signal from a router and then amplifies and rebroadcasts it around locally. With a Wi-Fi repeater, computers and printers that are out-of-the-range of an AP can still access the extended Wi-Fi network. This method, however, is not efficient, due to the requirement of a large number of Wi-Fi repeaters (routers), and an increased cost on hardware.

2.3 Previous Solutions

2.3.1 Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) was proposed by the Wi-Fi Alliance in 2010 to simplify the setup and management of secured Wi-Fi networks. WPS in an extent addresses the complex network set-up issue mentioned at the beginning of this chapter. WPS has a separate certification program and support for WPS is not mandatory for Wi-Fi certification. WPS is in general well-adopted by the latest Wi-Fi chipsets, but a significant number of devices/chipsets, including some access points/routers, does not support it.

There are three logical components involved in WPS mechanism: the Registrar, the Access Point (AP), and the Enrollee shown in Figure 2.3 [1]. In some cases these logical components may be co-located. The WPS specification introduces two configuration methods for easy setup: **Pin Configuration** and **Push button Configuration** (Figure 2.4).

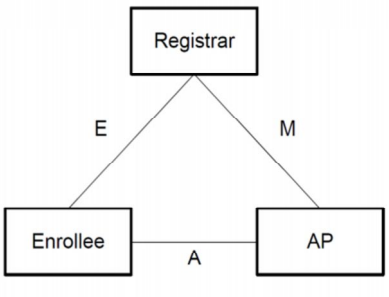

Figure 2.3: Three logical components of Wi-Fi Protected Setup (WPS)

Legacy Process	Wi-Fi Protected Setup: PIN Method	Wi-Fi Protected Setup: Push-Button Method
1. Power-on AP	1. Power-on AP/registrar	1. Power-on AP
2. Access AP	2. Power-on client device	2. Power-on client device
3. Set network name (SSID)	*Network name generated automatically and broadcast to client devices*	*Network name generated automatically and broadcast to client devices*
4. Activate security	3. Access registrar	3. Push button on AP
5. Set passphrase	4. Enter PIN	4. Push button on client device
6. Power-on client device		
7. Select network name (SSID)		
8. Enter passphrase		

Figure 2.4: Comparisons between Legacy setup process and WPS process

Push button Configuration requires the user to push a button on both the AP and the Enrollee (the device which is to join the network, e.g.lamp) within a specific time window (usually 2 minutes).

The PIN Configuration method enables the connection of Enrollees to a Wi-Fi network by entering both the PIN of the Enrollee and the PIN of the AP on a third logical entity referred to as the Registrar (e.g.smartphone). If the AP and the Registrar are co-located, only Enrollee's PIN is entered. The Registrar has to be authorized by the AP to "accept" other devices into the network on the AP's behalf. This authorization procedure is part of WPS. The method allows the use of a device with a suitable user interface (e.g.smartphone), to bring constrained devices (e.g.printer) into a Wi-Fi network (Figure 1) [1].

The PIN used in WPS PIN Configuration is an numeric code. Two types of PIN can be implemented:

- Static PIN: A factory-new device has a unique PIN e.g. printed on a label attached to its box. This PIN can be manually set by the user afterwards. PIN remains

static over the lifetime of the product unless the user changes it.

- Dynamic PIN: Auto-generated every time a new network is set up and shown on the screen of the device. PIN is different every time hence more strongly secured against hacks.

Note: if a device can generate a dynamic PIN and show it on a display but also has a label with a static PIN, it is recommended to use the dynamic PIN shown on the display although it is allowed to use the PIN from the label [1].

By means of using the registrar, WPS is capable of pushing the complexity from the enrollee (usually a constrained device) to the Registrar (usually a more advanced device), thereby solving the problem of constrained devices joining a Wi-Fi network.

The **disadvantage** of WPS is that all three devices are required to support WPS protocols, which basically requires upgrades on legacy Wi-Fi devices. As mentioned before, a significant minority of Wi-Fi devices do not support WPS, including some Access Point and router models of major vendors, limiting the practical applicability of WPS method. Therefore WPS is not an ideal solution for the first issue.

2.3.2 Wi-Fi Direct standard

Wi-Fi Direct is a newly released standard defined by Wi-Fi Alliance, to allow Wi-Fi devices to connect to each other without having to involve a wireless AP as shown in Figure 2.5. Simply speaking, it is a software upgrade on legacy Wi-Fi, which enables devices to play the role of a 'Virtual AP'; hence a wireless local network can be set up without the dependence on a real AP. The network formed by Wi-Fi Direct devices is also called a P2P network. Currently Wi-Fi Direct has already been integrated to some operating systems of PC and tablets [2].

Wi-Fi Direct has integrated some of WPS features, hence is capable to enrol constrained devices (e.g.lamps) to a P2P network by using a more advanced device (e.g.smartphone). In principle, once the smartphone and the lamps are in the same

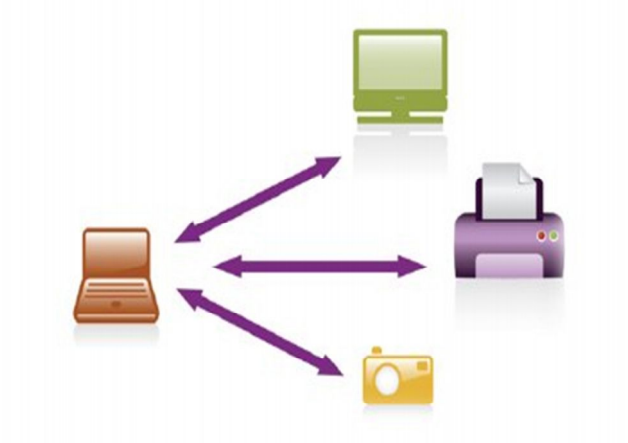

Figure 2.5: Wi-Fi Direct enables devices to talk directly without an Access Point (e.g.router)

P2P network, the smartphone is able to work as a controller to temporarily control the lamps via the P2P links using certain lighting control applications. Whereas this is not an ideal solution for Lighting Automation, simply because this P2P network has too much dependence on the smartphone which is assuming the role of a 'Virtual AP'. Once the smartphone leaves the room/house, this network is lost. Even though network-recovery is possible when the smartphone comes back, it may take up to tens of seconds till the P2P network resets up. This, however, can be somewhat unacceptable in practice. These limitations of P2P network will be explained in more details in Section 4.1. Therefore Wi-Fi Direct does not well solve the first issue neither.

2.3.3 Mobile Ad hoc Network (MANET)

Multi-hop network is not new in wireless communications. Since the mid 1990s, MANET (Mobile Ad hoc Network) has become a popular research topic due to the growth of laptops and 802.11/Wi-Fi wireless networking [16]. In MANET, each device should be able to forward traffic unrelated to its own use, leading to a primary challenge that each device should continuously maintain the information required to properly route traffic. Intelligent routing protocols have been invented to help optimizing the MANET traffic, including [17]:

- OLSR (Optimized Link State Routing Protocol)
- AODV (Ad hoc On-demand Distance Vector)
- DSR (Dynamic source routing)

The routing protocols are located in the network layer of the OSI model. They can be applied to a multi-hop network after the network is set up. The architecture of routing protocols are shown in Figure 2.6.

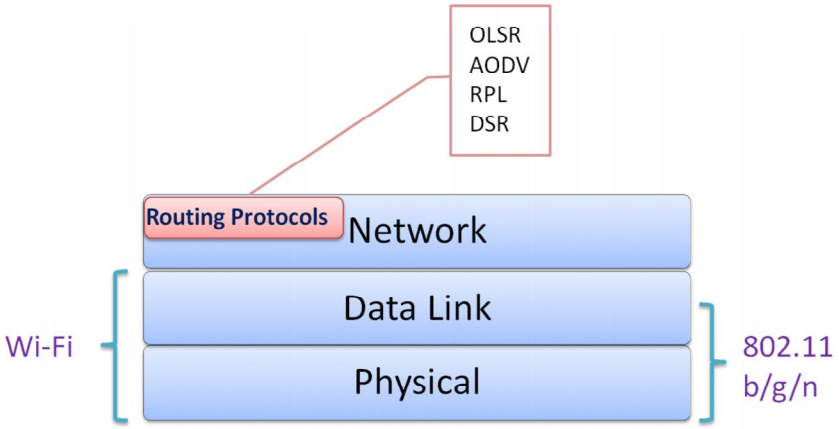

Figure 2.6: Architecture of routing protocols in a multi-hop network

The independence of any pre-defined network infrastructure makes MANETs suitable for environments and situations where such infrastructure does not exist. One example scenario is disaster areas in which communication between rescue workers, search teams, and medical personnel needs to be established despite the destruction of network infrastructure. MANETs should excel in terms of ease of use as well as flexibility because no wireless infrastructure must be set up and administered. However, MANETs are rarely seen in daily life. This may due to: 1) Special-purpose devices, such as medical equipment, but also smartphones do not necessarily support the 802.11 ad-hoc mode or do not provide user interfaces to enable it. 2) Supporting ad-hoc mode is insufficient for partaking in a MANET since every device must also support additional specialized MANET protocols for routing and address resolution [8]. Furthermore, it should be noted that MANET focuses on routing protocols in the Network Layer after a network is set-up, which does not solve our second issue, namely setting up a multi-hop Wi-Fi lighting network.

2.3.4 IEEE 802.11s

During the last decade, IEEE 802.11s has been proposed as an amendment for mesh networking, defining how wireless devices can interconnect to create a WLAN mesh network, which may be used for static topologies and ad-hoc networks. 802.11s inherently depends on one of 802.11a, 802.11b, 802.11g or 802.11n carrying the actual traffic. One or more routing protocols suitable to the actual network physical topology are required [6]. To build a mesh network, the 802.11s standard adds mesh node discovery and MAC-based routing capabilities into the 802.11 wireless protocol. This addition gives wireless devices the ability to see the other mesh nodes, as well as the ability to push traffic to the nearest connection in the network. There are no defined roles in a mesh - no clients and servers, no initiators and responders. Security protocols used in a mesh must, therefore, be true peer-to-peer protocols where either side can initiate to the other or both sides can initiate simultaneously [14].

802.11s defines two approaches, one aimed at Outdoor use and one aimed at Indoor use cases. However, neither of the two currently enjoys significant industry adoption, due to the extra complexity and slow organization. Therefore 802.11s, although being an approved standard, cannot be regarded as “the” standard Wi-Fi multi-hop solution in the market.

2.4 Wi-Fi Direct based Smart Setup (WDSS)

WDSS is an upper layer application developed on top of Wi-Fi Direct and WPS specifications. The relations between WDSS, Wi-Fi Direct and WPS is illustrated by Figure 2.7.

WDSS inherits features from both Wi-Fi Direct and WPS, like P2P link, Virtual AP, and easy setup configuration methods. Meanwhile, WDSS has added new features to its own protocol:

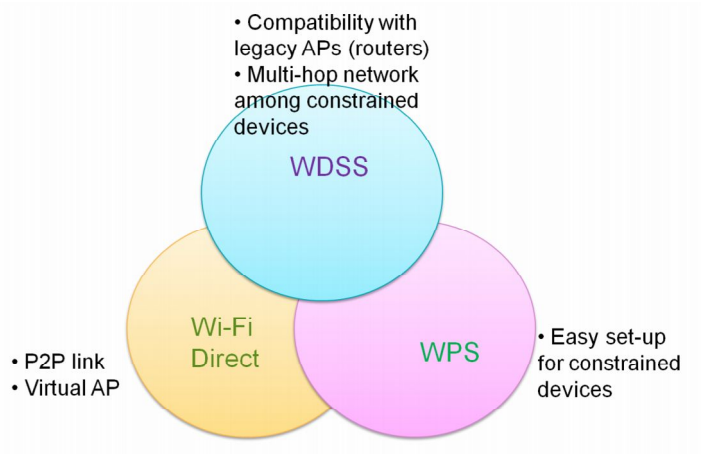

Figure 2.7: Relations between WDSS, Wi-Fi Direct and WPS

1). WDSS describes a method to securely connect a constrained device to an existing Wi-Fi network through the involvement of a third device, without pushing a button or entering security credentials on the constrained device and without any required support for "beyond standard Wi-Fi" features on the AP.

Therefore WDSS effectively overcomes the drawbacks existing in the current Wi-Fi as well as in WPS, meanwhile does not require any changes on the AP. Therefore WDSS gives a simple and generic solution to build up a well connected living ambience fully compatible with current Wi-Fi Infrastructure.

It should be noted that WPS was developed by the Wi-Fi Alliance for exactly the same purpose (i.e., easy network set up) as the method described in WDSS. WPS' approach however relies on WPS support in all three devices (Enrollee, Registrar and AP); a big disadvantage which is overcome by WDSS. The fact that the Wi-Fi Alliance themselves, in an effort to address easy network setup, created a standard that is inferior to the present idea is a strong indication for the inventiveness/ non-obviousness of the claimed WDSS method.

On the other hand, WDSS takes one step further than Wi-Fi Direct, to migrate lamps to an existing Wi-Fi network in order to achieve better longevity, scalability and connectivity; therefore overcomes the problems encountered in a P2P network (described in Section 2.3.2)

2). An add-on value of WDSS is that it extends the single-hop Wi-Fi to multi-hop Wi-Fi, thereby guaranteeing network coverage.

WDSS defines an easy way to establish a multi-hop network, by virtualizing wireless network interfaces on a single network card on the software layer. One interface works as a Wi-Fi Station (STA), another one as a 'Virtual AP'. Therefore one network card can simultaneously connect to two networks. The STA interface receives signals from its AP while the 'Virtual AP' interface relays signals to its sub-network (Figure 2.8). In this way a multi-hop network is formed among devices themselves without involving

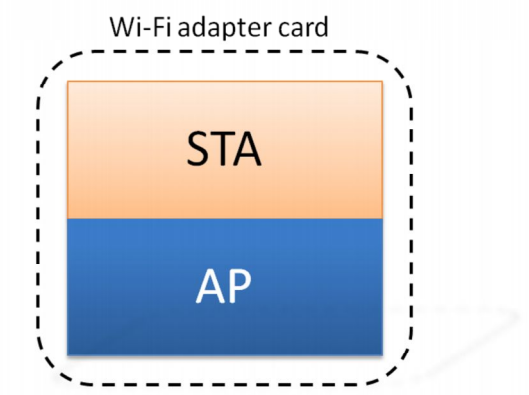

Figure 2.8: Virtualizing the Wi-Fi adapter into a STA interface and an AP interface

multiple external APs, therefore making it superior the existing method described in Section 2.2.

A straightforward approach to associat to multiple networks is to use multiple network cards per device. Although the use of multiple cards offers better mobility handling and throughput maximization [9], typical mobile devices only feature one physical network card. In principle, mobile devices can use a single physical network card to simultaneously act as AP and station by defining virtual network interfaces. Chandra et al. first introduced the concept of virtualizing wireless network interfaces on a single network card to connect to multiple networks simultaneously and transparently to the operating system [10]. Their work is realized in the VirtualWiFi [13] project and is included in the Windows 7 operating system as Native 802.11 Virtual Wireless Fidelity.

While also using network virtualization, none of these approaches targets networked lighting systems formed by interface-constrained devices (e.g. lamps, sensors) but they instead focus on the extension of AP-based networks that already operate in infrastructure mode. As such, WDSS approach novels at solving the multi-hop network set-up problem for interface-constrained devices.

There are two major differences between MANETs and WDSS multi-hop networks:

1. MANETs works in an ad-hoc network, with each device supporting ad-hoc mode and being equal. While WDSS establishes an infrastructure mode ad hoc network, in which devices simultaneously function as an AP and as a station to mesh with other AP devices. Therefore in WDSS multi-hop networks devices are connected to APs or Virtual APs, perceiving the network as a typical one-hop Wi-Fi network.

2. MANET techniques lay a large part in network layer routing protocols in order to optimize the multi-hop functions; while WDSS targets on network setup of interface-constrained devices. Once an infrastructure mode ad hoc lighting network is set up using WDSS, those MANET routing protocols can be applied to WDSS multi-hop network as well.

IEEE 802.11s standard defines Mesh Access Points that provide an infrastructure mode network to clients in addition to the mesh backbone network between Mesh Points. This approach is similar to ours; however, WDSS multi-hop network is formed by

multiple P2P links, with each link using Wi-Fi Direct protocol. This is different from 802.11s mesh network, which defines a secure password-based authentication and key establishment protocol called "Simultaneous Authentication of Equals" (SAE) for Peer authentication.

It should be noted that WDSS focuses on network setup, instead of defining network layer routing protocols. However, after the WDSS multi-hop network is established, more intelligent routing mechanisms, including those defined in MANETs, can be applied to it to optimize the traffic flow. However, this further step will not be discussed in this report.

3 Wi-Fi Direct

WDSS mechanism is developed on the basis of Wi-Fi Direct and WPS standards, aiming to:

1. Develop a method to securely connect a constrained device to an existing Wi-Fi network
   - without pushing a button or entering passphrase on the constrained device
   - without any required support for "beyond standard Wi-Fi" features on the AP (router)
2. extends the single-hop Wi-Fi to multi-hop Wi-Fi, thereby guaranteeing network coverage

Wi-Fi Direct is a newly released standard defined by Wi-Fi Alliance, to allow Wi-Fi devices to connect to each other with no need of a wireless Access Point (AP). Simply speaking, it is a software upgrade on legacy Wi-Fi, which enables a device to play the role of a "Virtual AP"; hence a wireless local network can be set up without the dependence on a real AP. The network formed by Wi-Fi Direct devices is also called a P2P network. Currently Wi-Fi Direct has already been integrated to some of the operating systems of PCs and tablets.

3.1 Components of Wi-Fi Direct (P2P) network

The most significant feature of Wi-Fi Direct is that it enables devices to talk directly without having to involve an Access Point (router), just like the name "Direct" implies. Figure 3.1 depicts a Wi-Fi network and a Wi-Fi Direct network (P2P network). There are two roles in a P2P network: **P2P Group Owner** and **P2P Client**. Usually the device which assumes the role of a Virtual Access Point stands in the middle as a P2P Group Owner, other devices connect to it as P2P Client, perceiving ont hop connected to a router. The functions of different P2P components are defined as [2]:

P2P Device:

- Wi-Fi Direct device, just like normal Wi-Fi devices, but with software upgrade
- Supports both P2P Group Owner and P2P Client roles
- Supports Wi-Fi Protected Setup (WPS) and P2P Discovery mechanism

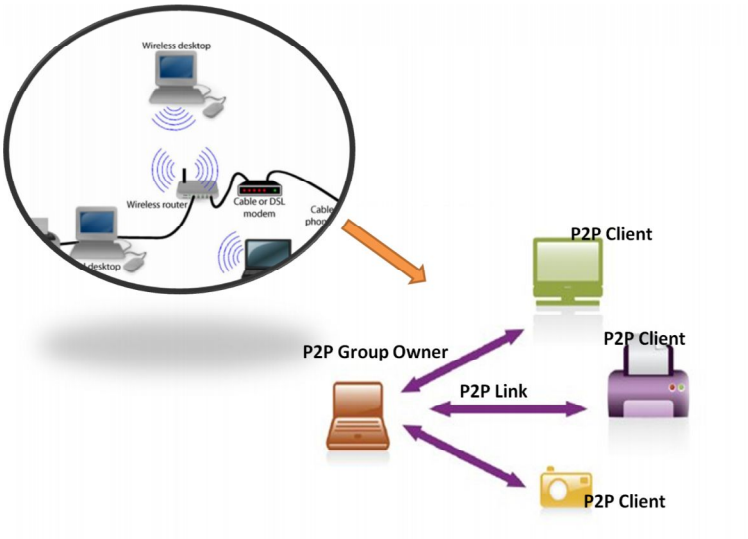

Figure 3.1: Wi-Fi network (upper left) v.s. P2P network (right bottom)

P2P Group Owner:

- "AP-like" entity that provides BSS functionality and services for associated Clients (P2P Clients or Legacy Clients)
- Provides WPS Internal Registrar functionality

P2P Client:

- Implements non-AP STA functionality
- Provides WPS Enrolee functionality

3.2 Set up a P2P network

There are three major steps to set up a P2P network:

1. Device Discovery

P2P Devices in range find each other, arrive on a common channel and exchange device information using Probe Request and Probe Response. There are mainly two phases in Discovery process, Scan Phase and Find Phase.

Scan Phase uses the scanning process defined in IEEE Std 802.11-2007. It may be used by a P2P Device to find P2P Device or P2P Groups and to locate the best potential Operating Channel to establish a P2P Group. In the Scan Phase, devices collect information about surrounding devices or networks by scanning all supported channels [2].

Find Phase is used to ensure that two simultaneously searching P2P Devices arrive on a common channel to enable communication. This is achieved by cycling between states

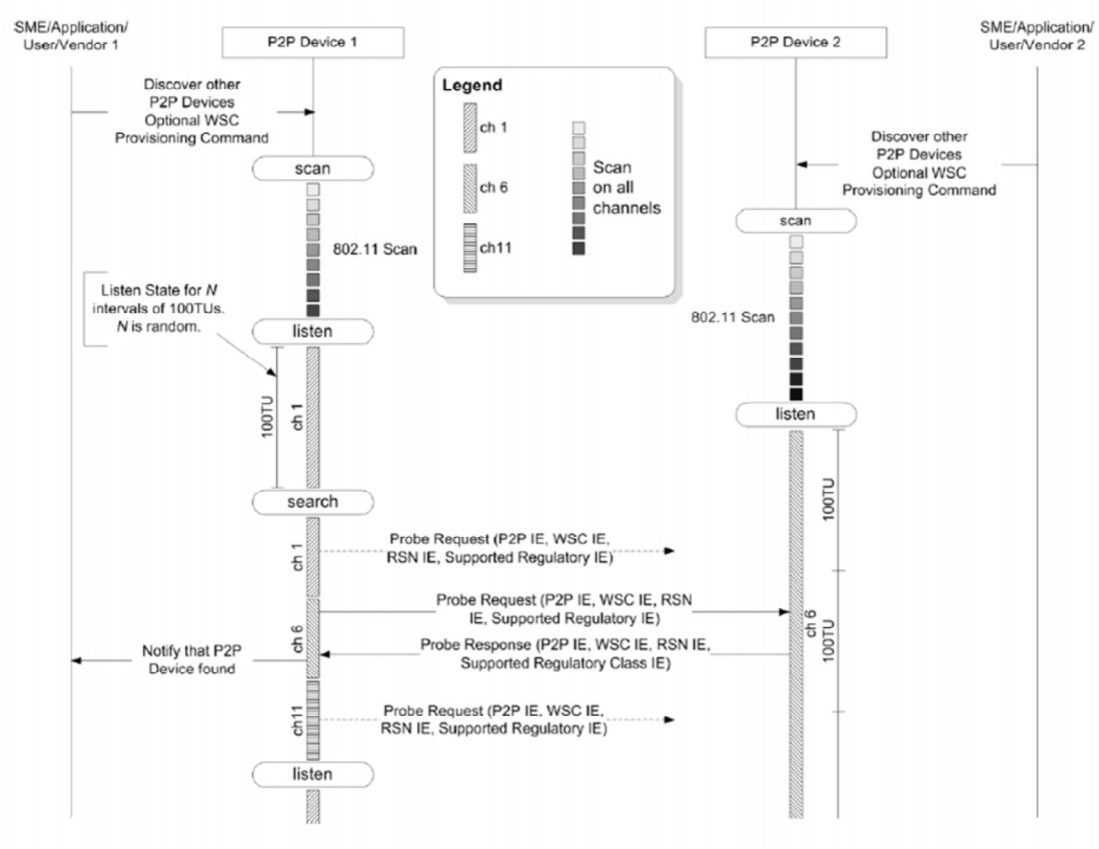

Figure 3.2: Device Discovery procedures for a P2P Device

where the P2P Device waits on a fixed channel for Probe Request frames (the Listen State) or sends Probe Request frames on a fixed list of channels (the Search State). Convergence of two devices on the same channel is assisted by randomizing the time spent in each cycle of the Listen State [2]. The procedure is shown in Figure 3.2.

2. Group Owner Negotiation

A three way frame exchange is used to agree which P2P Device shall become P2P Group Owner and to agree on characteristics of the P2P Group. In this process the Group owner Intent attribute is exchanged, which measures the desire to be P2P Group Owner. The Intent value ranges from 0 to 15. A device, for instance, with an intent value 15, has a strong desire to be the Group Owner. Only one P2P Group Owner exists in each P2P Group, the rest of devices serve as P2P Clients. The Group Owner determines network name, credentials and channel information, etc [2].

3. Provisioning

Using Wi-Fi Protected Set-up to establish connections. The P2P Group Owner shall serve the role as the AP with Internal Registrar. It shall only allow association by the P2P Device that it is currently in Group Formation with. The P2P Client shall serve the role as the STA Enrolee [2].

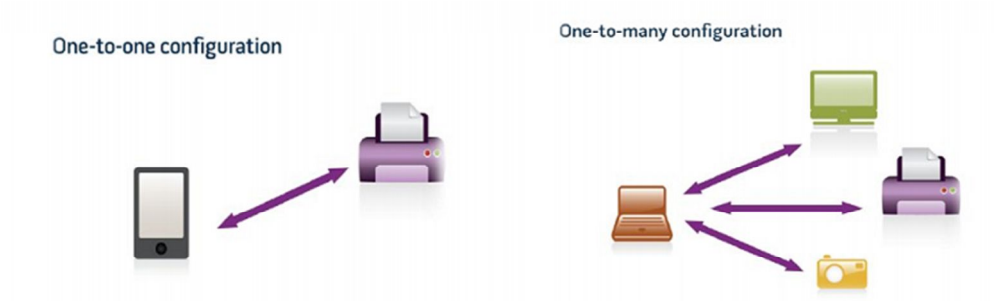

Figure 3.3: P2P Network Topology can be 1:1 or 1:n

3.3 P2P Network Topology

A P2P network consists of one Group Owner which serves as a 'virtual AP', and several Clients. Clients talk to Group Owner directly in a star network. The P2P network topology can be 1:1 or 1:n (Figure 3.3).

4 Main Components of WDSS

The highlights of WDSS can be specified in two user scenarios:

- Using the CT (e.g.smartphone) to instruct the constrained device (e.g.lamps) to migrate to a legacy AP (router)
- Using this method to establish a multi-hop Wi-Fi network among constrained devices in a lighting system

These two user scenarios are to be described in details in the following sections.

4.1 WDSS User Scenario 1: Migrating the constrained device to a legacy AP

In User Scenario 1, WDSS method makes use of Wi-Fi Direct and WPS technologies, to securely connect a device to an existing Wi-Fi network through the involvement of a third device, without pushing a button or entering security info on the device and without any required support for "beyond standard Wi-Fi" features. The envisioned User Scenario 1 includes two major tasks as shown in Figure 4.1. These **two tasks** will be explained respectively in this section.

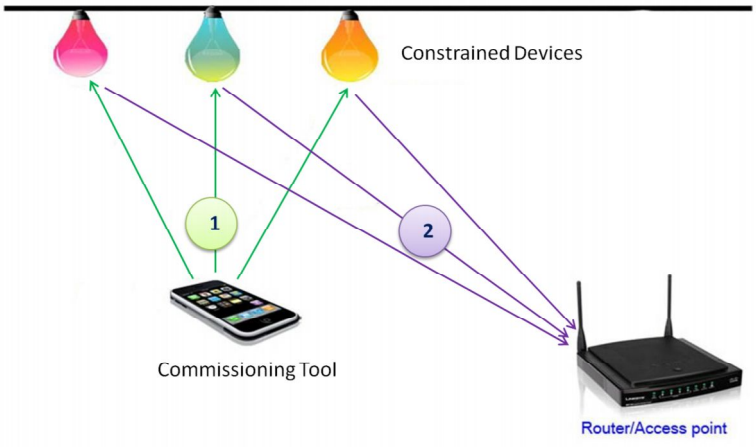

Figure 4.1: User Scenario 1 of WDSS, including Task 1 and Task 2

1. Setting up P2P connections between the lamps and the CT (e.g.smartphone) using WPS PIN Configuration
2. Using the CT to migrate lamps from the P2P network to an existing Wi-Fi Network

4.1.1 Task 1

As introduced in Chapter 2, traditional Wi-Fi networks are merely intended for devices that bear a user interface to join, therefore constrained devices like lamps and sensors are difficult to be enrolled into this network. Wi-Fi Direct has integrated WPS to enable easy set-up of a P2P link between a CT and a constrained device. WDSS makes use of this feature to extend WPS method into a larger scale, including the usage of legacy APs.

A significant feature of WPS is that it gives the option to type the PIN on the registrar side, instead of the enrolee. The conventional mechanism used for Authentication and Access Control in 802.1x is shown in Figure 4.2.

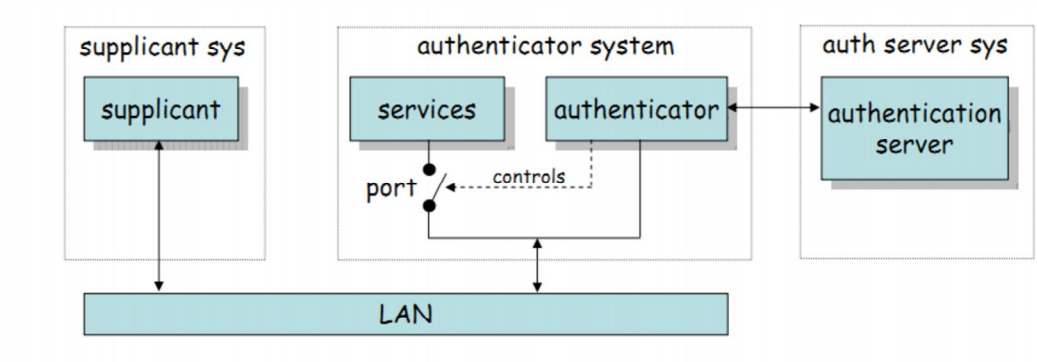

Figure 4.2: 802.1x Authentication and Access Control Mechanism

Supplicant: Mobile Device (STA)

Authenticator: Access Point (AP)

Authentication Server: Server application running on the AP or on a dedicated machine

The supplicant authenticates itself to the authentication server. If the authentication is successful, the authentication server instructs the authenticator to switch the port on. A four-way handshake is going on in the underlying protocol (shown in Figure 4.3). In the four-way handshake, the following activities are taking place:

- Confirms the Pre-shared key between the STA and the AP

- Establishes the temporal keys (PTK) to be used by the confidentiality protocol
- Authenticates the negotiated security parameters

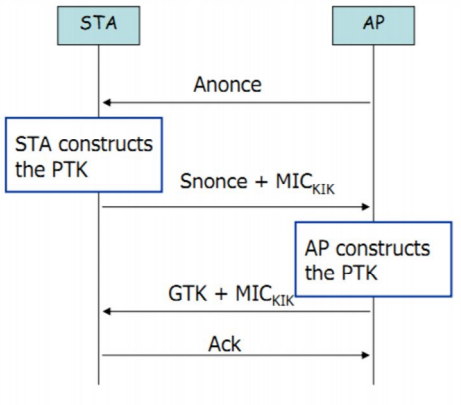

Figure 4.3: Four-way handshake in authentication

PTK: Pairwise Transient Keys

GTK: Group Transient Keys

MIC: Message Integrity Code (computed by the mobile device using the key-integrity key)

WDSS uses WPS for easy authentication, namely the Pre-shared Key is not necessarily hold by the AP and input by the STA to authenticate itself. More flexibly, either the AP or the STA could generate this shared key, and each of them can authenticate itself to another. This is the fundamental improvement over the conventional Wi-Fi authentication mechanism, which allows the constrained devices in the Lighting System to join a secured Wi-Fi network. The authentication process of WPS in-band setup using a standalone AP/Registrar is shown in Figure 4.4. This scenario applies both for adding Enrolees with APs with built-in Registrar capabilities as well as wireless external Registars [1].

As introduced in Chapter 2, WPS mainly defines two methods for easy security configuration, PIN method and Push Button method. In this project, we are going to focus on PIN method, which is relatively more secured than Push Button method. WPS supports WPA2-Personal networks and Open networks. Wi-Fi Direct has integrated 'Virtual AP' functions into Wi-Fi devices, the WPS Registrar in P2P network is enroller itself. Task 1 takes the following steps for us to link a lamp to a CT (smartphone) using Wi-Fi Direct. The process is well depicted from Figure 4.5 to Figure 4.8.

1. A static 8 digit numeric PIN is assigned to each interface-constrained device (e.g., a lamp or sensor) prior to their installation, e.g., in the factory. The notion of

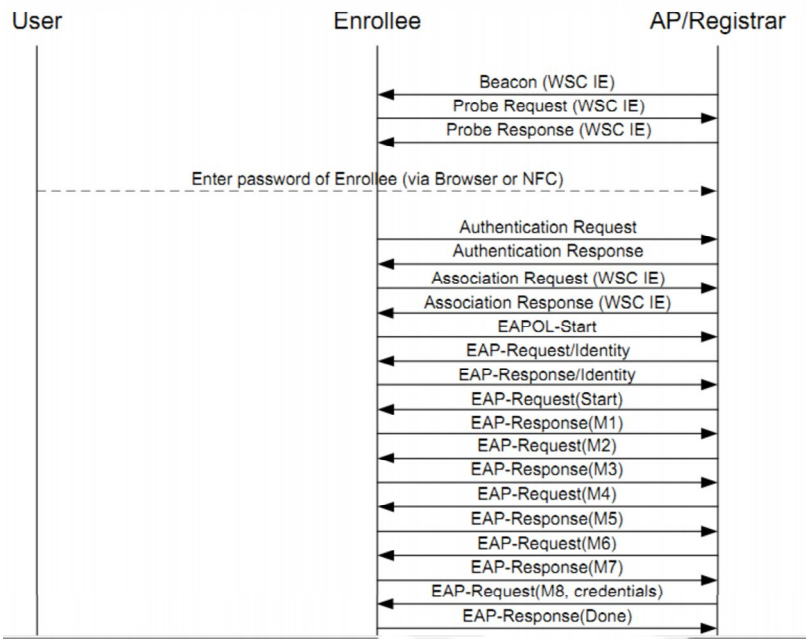

Figure 4.4: Authentication process of WPS in-band setup using a standalone AP/Registrar

using pre-defined static PINs to enable secure and easy network setup is not novel; existing standards such as Wi-Fi Direct and Bluetooth rely on this feature for P2P network setup.

2. When the lamps are powered up, the incorporated Wi-Fi transceiver automatically starts the Wi-Fi Direct "listen-search" cycle for a pre-defined amount of time.

3. The smartphone uses the beacons that are transmitted during the "listen-search" cycle to set up a P2P link to the constrained device, as defined by the Wi-Fi Direct specification. The link set-up is secured by means of entering the PIN associated with the lamp on the smartphone. A WPA2 encrypted one-to-one network is thus created. Notice that this process does not require manual operations on the lamp, offering the opportunity to connect devices without displays or buttons.

Figure 4.5: Lamps broadcast their names in order to be discovered

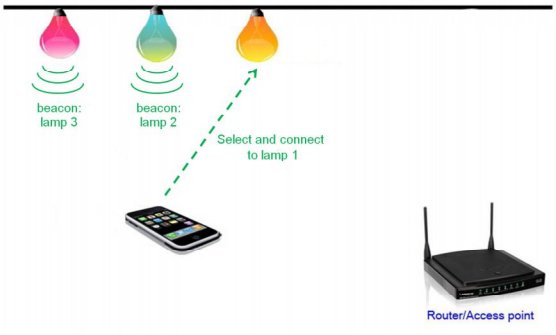

Figure 4.6: Smartphone discovers the lamps, user selects one to connect

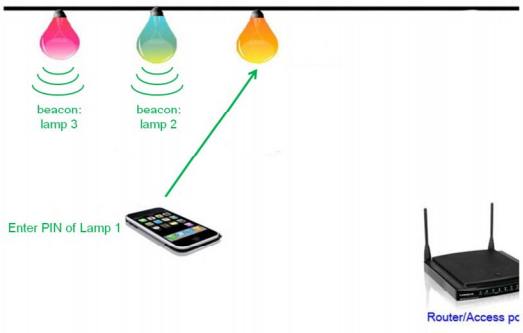

Figure 4.7: User enters the PIN of lamp on the smartphone to set up the link

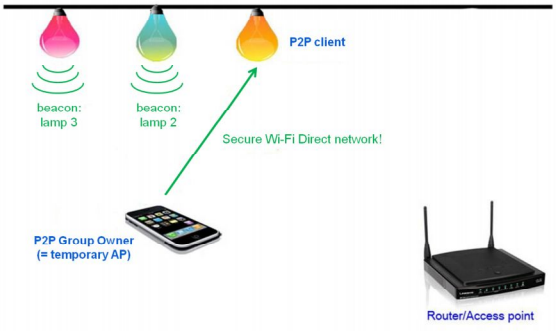

Figure 4.8: A P2P link is set up between the smartphone and the lamp

Up to here we have successfully linked a lamp to a laptop using Wi-Fi Direct. With WPS mechanism, we push the authentication operations to the smartphone side, leaving the constrained device intact. Since they are now in the same P2P group, later on this smartphone can be used as a CT to migrate this lamp to a WLAN, without breaking down the security level.

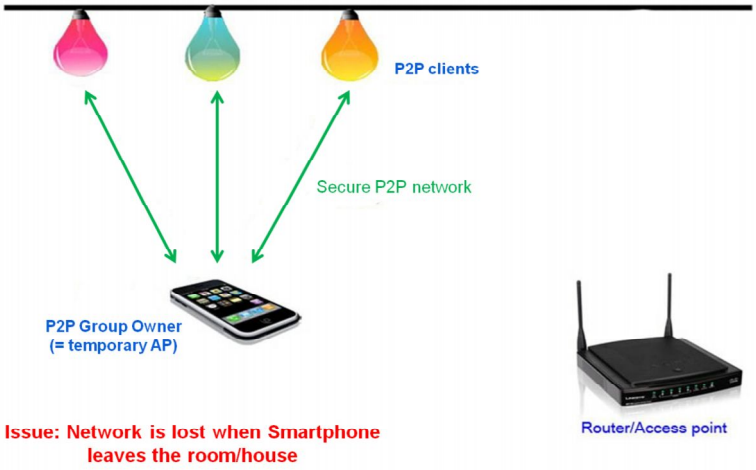

Figure 4.9: A P2P network can be set up using this method

In principle, once the CT and the lamp are in the same P2P network (Figure 4.9), the CT is able to temporarily control the lamp via the P2P link using certain lighting control applications, whereas this is not an ideal solution for Lighting Automation. The reasons are:

- A P2P network is dependent on the Group Owner (usually the CT) - when the Group Owner is powered off or leaves the network, the network is automatically dissolved. This is a fundamental limitation imposed by WPA2, which relies on the presence of a Security Authority (a role which is assumed by the Group Owner) to maintain a secure network. For reasons of security, no mechanism was defined

to migrate the role of Group Owner from one device to another.

- A P2P network can only encompass a limited number of devices (significantly less than a regular Wi-Fi network), because the Group Owner has to provide the routing functionality which is normally afforded by a router/Access Point using hardware acceleration.
- A P2P network is an independent Wi-Fi network using a private SSID and Key, which is isolated from the common WLAN if no further configuration is done. Therefore the Lighting control is to an extent split into small segments, each relying on a Group Owner. This will be a big obstacle for network scalability and central controlling.
- A P2P network can only connect to an existing legacy Wi-Fi network via the Group Owner, which has to establish and bridge (share) a connection to an existing AP. If we let the CT serves as Group Owner, the procedure to establish and bridge a connection to the Wi-Fi infrastructure network is defined by the Wi-Fi Direct specification. However, again this P2P network would have to depend on the bridge (CT) to communicate with the Wi-Fi infrastructure network. This is unlikely to be practical since the CT is usually a mobile device.

In short: Wi-Fi Direct enables easy network setup, but the resulting P2P Wi-Fi network does not provide sufficient longevity, scalability and a connectivity (to existing Wi-Fi infrastructure) to meet the requirements of networked Lighting systems.

4.1.2 Task 2

Therefore we want to take one step further, to migrate the lamps to an existing Wi-Fi network so as to achieve better persistence. This has been put forward as task 2 defined by the following content:

1. In principle, during the link set-up process one of the involved devices is selected as 'Group Owner'. In normal circumstances the most capable (in terms of computing resources and power availability) device will assume the role of Group Owner, as the Group Owner is responsible for a number of resource-and power-intensive tasks. These tasks include relaying traffic between other devices that are part of the P2P network (which leaves little room for power saving in the form of sleeping) and managing the security credentials as the network's WPA2 Security Authority. Based on insights obtained during our investigation, we assign the Group Owner role as follows:

a. When all interface-constrained devices that are to be connected to an existing Wi-Fi network are within communication range of an existing Wi-Fi Access Point, either the CT or the constrained device can assume the role of Group Owner and the other one becomes a 'Client'.

b. When some of the to-be-commissioned constrained devices are out-of- range of the existing Wi-Fi Access Points, the constrained device assumes the role of Group

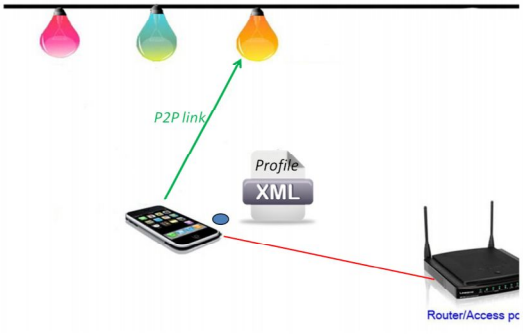

Figure 4.10: The CT generates a WLAN profile of the AP

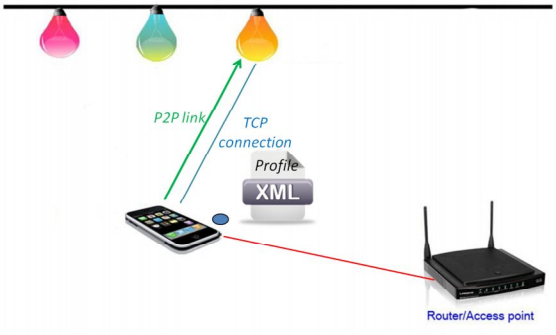

Figure 4.11: A socket connection is set up between the CT and the lamp

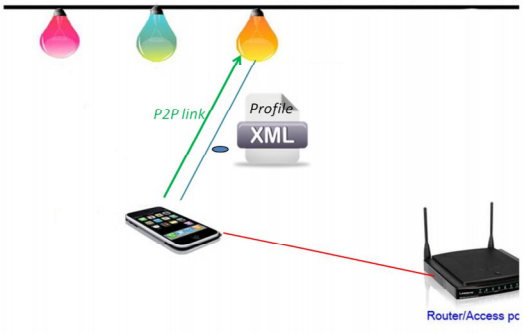

Figure 4.12: The WLAN profile is sent to the lamp via the socket connection

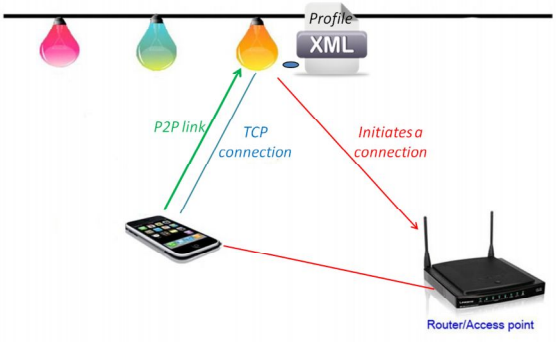

Figure 4.13: Upon receiving the profile, the lamp initiates a connection to the AP

Owner and the CT becomes the 'client'. The reason for this choice becomes apparent in section on **Multi-hop Wi-Fi Networks** (User Scenario 2)

For the sake of coherence in two scenarios, we assign the Group Owner role as described in **b**. In another word, the constrained device is pre-configured to work as a Virtual AP, hence assuming the role of P2P Group Owner. The CT becomes a P2P Client automatically once linked to the GO. Therefore the process of P2P link setup between the constrained device and the CT is simplified compared to the one defined in the Wi-Fi Direct Specification (as explained in Section 3.2).

2. To overcome the aforementioned limitations in Task 1, we take one step further, to instruct the constrained devices in the P2P network to migrate to an existing Wi-Fi infrastructure network (WLAN). To achieve this, the CT executes the following steps in order (Figure 4.10 to Figure 4.14):

a. The CT establishes a connection to the WLAN to which the constrained device(s) should migrate and store the SSID of the network and the security credentials (passphrase) of this network as a so-called WLAN profile. Alternatively, the CT might already be preloaded with the relevant profile information.

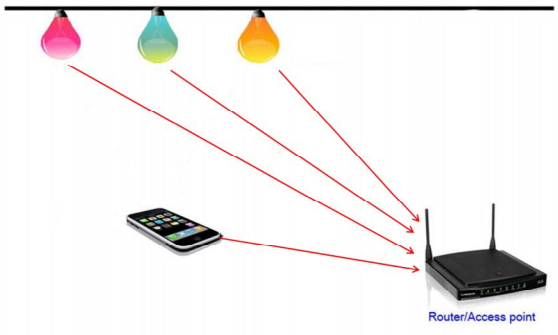

Figure 4.14: After migration, the CT can join the same WLAN for lighting control

b. The CT sets up a socket (TCP) connection on top of the P2P link between the CT and the constrained device.

c. The CT uses the socket connection to transfer the profile information (including the SSID) to the constrained device and instruct the device to migrate to the network defined by the WLAN profile.

The WLAN profile is a XML file which is understandable by PCs formatted as shown in Figure 4.15. The XML profile contains the necessary information about the WLAN, such as the name of the network (SSID) e.g.WLAN-PUB, and the authentication type e.g.open. The lamp will read this file and use this information to join the described WLAN.

Depending on different security levels (open, WEP, WPA or WPA2) of the WLAN, the profile would be slightly different in terms of authentication and encryption. The profile

```
<?xml version="1.0"?>
- <WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
    <name>WLAN-PUB</name>
  - <SSIDConfig>
      - <SSID>
          <hex>574C414E2D505542</hex>
          <name>WLAN-PUB</name>
        </SSID>
        <nonBroadcast>false</nonBroadcast>
    </SSIDConfig>
    <connectionType>ESS</connectionType>
    <connectionMode>manual</connectionMode>
  - <MSM>
      - <security>
          - <authEncryption>
              <authentication>open</authentication>
              <encryption>none</encryption>
              <useOneX>false</useOneX>
            </authEncryption>
        </security>
    </MSM>
</WLANProfile>
```

Figure 4.15: The WLAN profile of an unsecured network

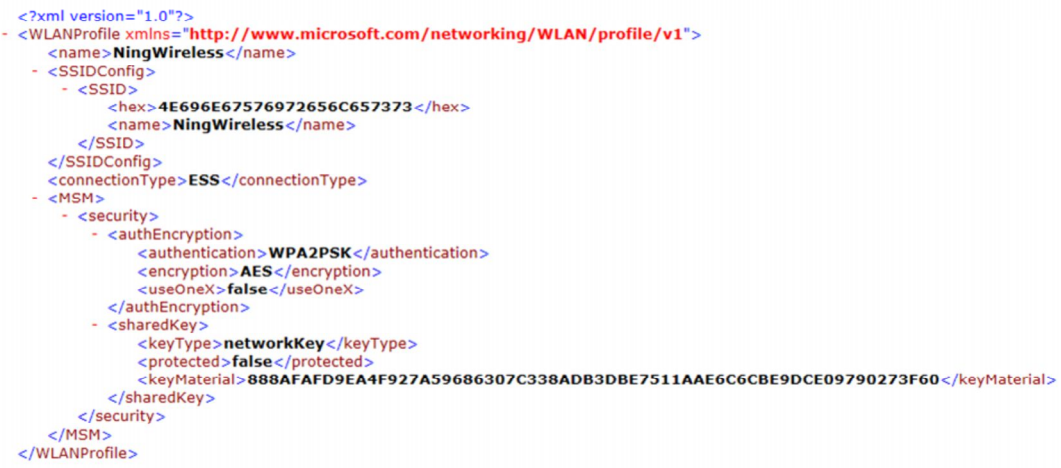

Figure 4.16: The WLAN profile of a secured network

shown in Figure 4.15 is retrieved from a non-secured (open) WLAN named "WLAN-PUB". Figure 4.16 shows a profile of a WPA2-secured network named "NingWirelss".

The WLAN "NingWireless" deploys an authentication method of "WPA2PSK", which is short for Wi-Fi Protected Access 2 - Pre-Shared Key, and also called WPA or WPA2 Personal. It is a method of securing the network using WPA2 with the use of the optional Pre-Shared Key (PSK) authentication, which was designed for home users without an enterprise authentication server. The "keyMaterial" indicates the Pre-Shared Key used in this WLAN. In this case we use the key "NingWireless" which is identical with the network's name. It can be observed that the keyMaterial displays 64 digits of codes instead of a plain text "NingWireless". This is due to the rules of "WlanGetProfile" function in Window Operation System. The "WlanGetProfile" function retrieves information about a WLAN. The output of is the XML file shown in Figure 4.16. The keyMaterial (sharedKey) element contains a network key or passphrase. If the protected element has a value of 'TRUE', this key material is encrypted; otherwise, the key material is unencrypted. In the example of Figure 4.16, the protected element has a value of 'false'; hence the 64 digit codes are not encrypted key, but merely a 64 hexadecimal characters expression of the key which can be shared among PCs.

The range of valid values for the keyMaterial element varies by the type of authentication and encryption used, as specified by the authentication and encryption elements. It also varies by keyType. Table 4.1 shows valid keyMaterial values for some authentication and encryption pairs.

Our case is in line with the last row, the networkKey is expressed by 64 hexadecimal characters instead of the plaintext. Once this profile is transferred from the CT to the lamp, these 64 hexadecimal characters can still be understood and translated to a valid key to join the WLAN "NingWireless".

Here is a small tip: Generally if we retrieve the WLAN profile in

- Windows XP with SP3 and Wireless LAN API for Windows XP with SP2: the

authentication value	encryption value	keyType value	Valid keyMaterial values
open or shared	WEP	networkKey	This element contains a WEP key of 5 or 13 ANSI characters, or of 10 or 26 hexadecimal characters.
WPAPSK or WPA2PSK	TKIP or AES	passPhrase	This element contains a passphrase of 8 to 63 ASCII characters, that is, 8 to 63 ANSI characters in the range of 32 to 126. Key values must comply with the requirements specified by 802.11i.
WPAPSK or WPA2PSK	TKIP or AES	networkKey	This element contains a key of 64 hexadecimal characters.

Table 4.1: Valid keyMaterial values for some authentication and encryption pairs

key material is never encrypted (e.g.64 hexadecimal characters). This key material can be shared by other devices.

- Window 7, Window Server 2008 or Windows Vista: the key material is by default encrypted (e.g.256 characters), and usually not allowed to retrieve the plaintext of the key. This key material can only be understood by the source PC. Other PCs are not able to decrypt it even though this profile is transferred successfully to them.

Therefore, in the demo of our project, a Window XP laptop was used as a CT to retrieve the profile of the WLAN in order to get an unencrypted key for the lamps to share. In practice, an embedded system is integrated in the lamp to execute the "GetProfile" function, which won't have complex encryption mechanism as that in Window 7. Therefore the keymaterial won't be an issue in the Lighting System.

3. When a constrained device receives the WLAN profile over the socket connection, it is triggered to connect to the corresponding WLAN using regular Wi-Fi technology (Figure 4.12). The CT (and any other types of controllers) can now connect to the same AP to control the lamps via the existing Wi-Fi network. The P2P link can therefore be dissolved without affecting the connectivity.

Notice that step 2 and 3 of this sequence do not require any adaptations in the Wi-Fi stack; rather a small commissioning application/protocol is defined on top of Wi-Fi and IP.

4.2 WDSS User Scenario 2-Establishing a Multi-hop Wi-Fi Network among lamps

Wi-Fi Direct standard has defined the protocols for P2P communications and mainly focused on one-hop network. According to the Wi-Fi Direct specification, a P2P Client

is seen as an end device which talks directly with the P2P GO, and sometimes can be bridged to inter-communicate with a WLAN. However, not much information has been given to describe how to extend the network into a multi-hop topology. User Scenario 2 of WDSS gives a novel idea, which is beyond Wi-Fi Direct Specification, to alter the P2P Client to a potential intermediary device of a multi-hop Wi-Fi Network. Multi-hop Wi-Fi is especially helpful in deployments where the Access Point network is not sufficiently dense to cover the entire deployment area of a Networked Lighting System.

WDSS deploys interface virtualization to allow one single Wi-Fi chipset to connect to multiple networks, thereby scaling to a multi-hop network. In our project we utilized the internal Wi-Fi chipsets of laptops (random modes) for interface virtualization, which proves WDSS to be a generic solution for commodity Wi-Fi chipsets. Each virtual network interface is then separately configurable and appears as a normal interface to applications, with the restriction of using the same channel on all interfaces. However, such parallel operation requires the network card drive to iterate between the different networks, i.e. switch the card in time to serve or listen to each network [8]. It should be noted that by deploying Virtual AP, WDSS multi-hop network is also able to work independently with the infrastructure Wi-Fi network in a local scale, therefore also suitable for MANETs user scenarios i.e. communicate in areas where the network infrastructure is not available.

We design a multi-hop networked lighting system, in which lamps close to the infrastructure Wi-Fi network serve as APs for other lamps out of the effective range of the source router. At the same time, these AP lamps establish associations to infrastructure networks provided by other APs / Virtual APs. While providing a traditional infrastructure mode network that is supported by all types of devices, WDSS allows multi-hop communication through these interconnections. By establishing the multi-hop network in such a way, devices without special software or ad-hoc functionality can associate to devices that serve as APs and participate in the network. The only requirement for Station Devices is to be able to associate to a Virtual AP device using a single 802.11 association in infrastructure mode. This enables a more generic usage, in that Google disables ad-hoc networking in Android by default while the iPhone 4 only connects to ad-hoc networks in Wi-Fi fashion, i.e. spanning a single hop [8].

The multi-hop network is established using the following steps:

a. The first step is identical with User Scenario 1: the CT instructs the first lamp to migrate to the WLAN. It should be noted that in Scenario 2 the CT is configured to assume the role of Client during the link set-up process, thus pushing the role of GO to the constrained device. As mentioned in step 1.**b** of Task 2 in Scenario 1, in multi-hop lighting system, the lamp has to assume the role of GO, due to the reason that Lamp 1 is going to act like a Virtual AP (only capable as a GO) in a multi-hop network later on.

b. During step **a**, the CT requests the SSID and security credentials (passphrase) from the Virtual AP (first lamp) via the P2P link, and creates a WLAN profile. This WLAN profile is a profile of the Virtual AP, instead of a real infrastructure Wi-Fi

network. However, the format is the same. Therefore other Wi-Fi Devices are able to understand it and treat it as a normal WLAN profile.

c. At a later stage, the CT sets up a P2P link to a secondary constrained device (e.g., second lamp) which is out-of-range of the Wi-Fi Access Point. Using the WLAN profile obtained in step **b**, this device is instructed to migrate to the intermediary constrained device (first lamp). This is simply effectuated by transferring the WLAN profile created in step **b** to the secondary constrained device.

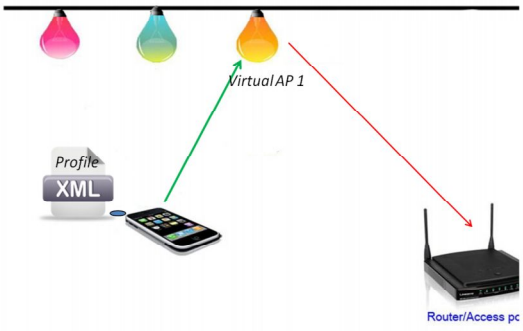

Figure 4.17: CT generates a WLAN profile of the Virtual AP 1

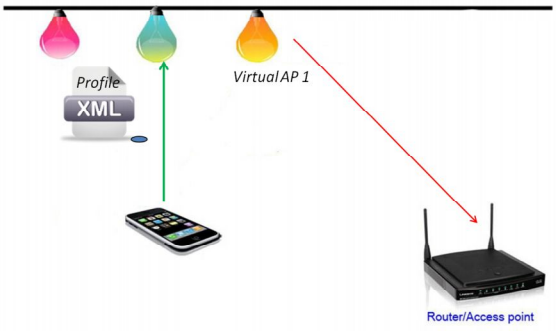

Figure 4.18: CT sends the WLAN profile to Lamp 2

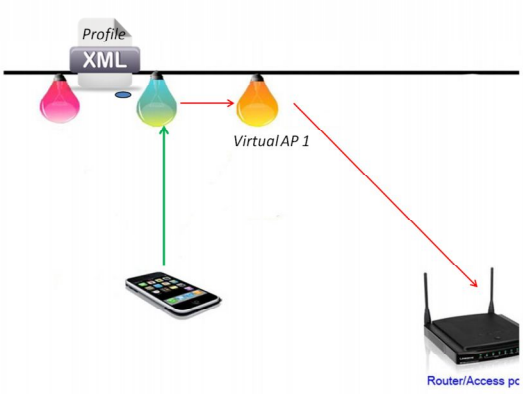

Figure 4.19: Upon receiving the profile, Lamp 2 initiates a connection to Lamp 1

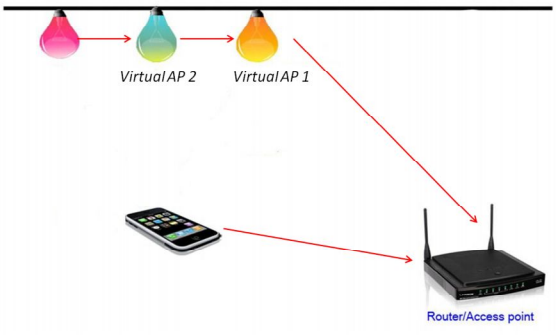

Figure 4.20: More hops can be added using this method to establish a multi-hop network

Note: Step **a** and **c** are quite similar, only differing in the target AP the lamp migrates to. More hops can be added to this network by repeating step **c**.

For unconstrained devices, step **b** and **c** can be combined into one, since the user interface on the device itself can be used to acquire the WLAN profile and initiate the connection to the virtual AP, hence no external CT is necessary for migration.

Step **a**, **b** and **c** are only necessary for factory-new devices. After the first set-up, WLAN profiles are stored in devices so they remember which AP or Virtual AP to connect to. Links may temporarily break if the lamps are powered off, but they will

automatically connect again when they are powered on, therefore no extra configuration is required for the network recovery.

5 Design of WDSS protocol

5.1 WDSS usage models

WDSS program was designed to support the following usage models:

1. Setting up a new secured P2P network using Wi-Fi Direct without having to involve an AP
2. Setting up a secured P2P network with constrained devices, by operating on a CT (usually an advanced device)
3. Controlling constrained devices by the CT for temporary usage
4. Using the CT to obtain the AP information (SSID, passphrase, etc) of an existing WLAN
5. Using the CT to instruct constrained devices to migrate to an existing WLAN
6. Expanding the network - Adding additional members
7. Controlling constrained devices via Internet-based applications
8. Multi-hop Wi-Fi network with devices themselves working as relaying nodes

Our project was conducted mainly for two goals to overcome the issues explained in Section 1.3:

1. develop a Wi-Fi Direct based Smart Set-up (WDSS) method, to securely connect a constrained device to an existing Wi-Fi network, without pushing a button or entering passphrase on the constrained device.
2. apply the WDSS method to extend single-hop Wi-Fi to multi-hop Wi-Fi among lamps, thereby guaranteeing network coverage.

These usage models and goals are well illustrated by the two User Scenarios introduced in Chapter 4.

5.2 Mental Model of WDSS

A mental model is an explanation of people's thought about how something should work in real world. A good technical design should comply with a proper mental model in order to be well accepted by end users. WLAN uses the "lock and key" mental model to imply the relationship between a secured WLAN and the information needed to access. A secured WLAN is compared to a lock which requires a certain key to access. The credential used in this WLAN is equivalent to the key of the lock.

WDSS uses the mental model of WLAN, but in an indirect way. WDSS adopts a third device (CT) to work as an intermediate device to pass the key to a constrained device, and instruct it to open the lock. This is quite comparable to a parent giving the key to the child and teaching him/her to open the lock. A CT first enrols those constrained devices into a P2P network and then instructs them to migrate to a WLAN by passing them the key of the specific lock. The CT here plays the role of a trusted entity that holds the key of the WLAN and is allowed to authorize other constrained devices. Security on each step is ensured by the "lock and key" mental model.

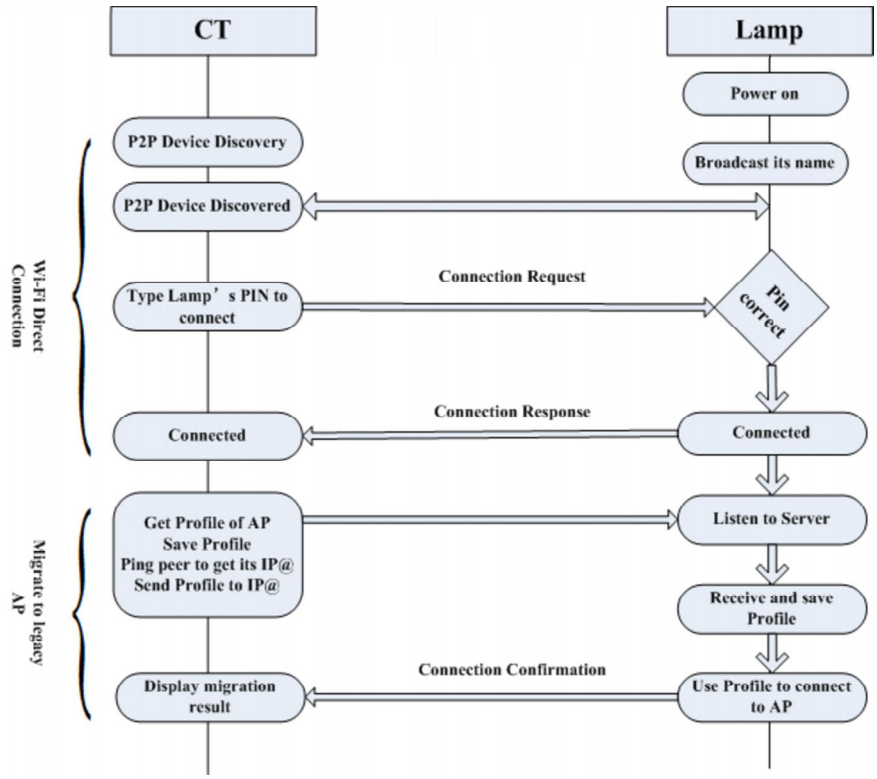

Figure 5.1: The workflow of WDSS method

5.3 Workflow and Program design

5.3.1 Workflow of WDSS program

The work flow of WDSS protocol is shown in Figure 5.1. User Scenario 1 illustrates the basic function of WDSS program. User Scenario 2 describes an extended function. In order to integrate two functions into one program, we let the lamp be the Group Owner, hereby acting like a Virtual AP. The CT connects to the Virtual AP via a P2P link, and further more instructs the client to migrate (Scenario 1) or form a multi-hop network (Scenario 2).

5.3.2 WDSS program design

The WDSS program was implemented in VisualStduio 2008, with a user interface shown in Figure 5.2. The user interface is divided into two sections, the upper half is intended for Client (constrained devices e.g.lamp), while the lower half is meant for the CT (laptop, smartphone, etc). Only one virtual button "Start up to be configured" is designed for the Client . Taking a lamp for example, this button simulates the switch of the lamp. When the lamp is switched on, it equals pushing this virtual button to get ready for configuration. The lamp will open its AP interface and start to broadcast its name. Two buttons were designed for the CT, "Get Profile of the AP" and "Configure the Client". "Get Profile of the AP" uses WLAN APIs to retrieve the profile of a WLAN. By triggering this button on the CT, the names of available wireless networks will show in a list. User selects the target AP. Then the information about this AP will be formatted in a XML file and stored in a local file. "Configure the Client" commands

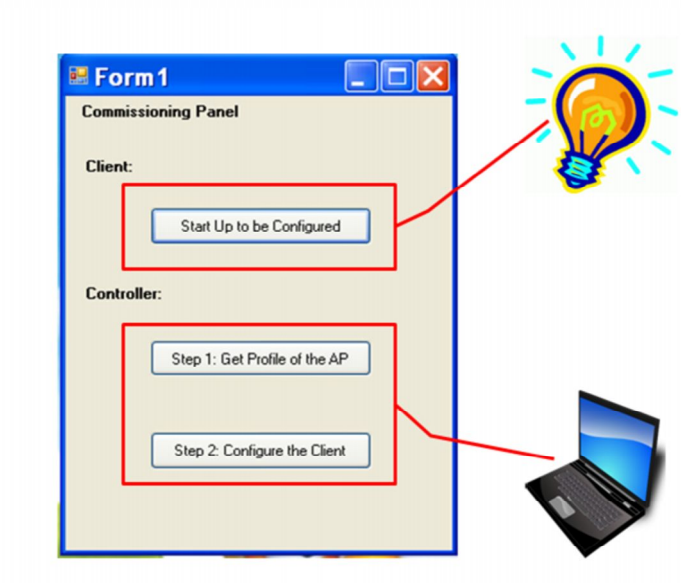

Figure 5.2: The User Interface of WDSS program

the CT to open a socket connection to the Client, send the profile retrieved from the early step to the Client, and instruct it to initiate a connection to the AP described by the profile.

5.3.3 WDSS subprograms

The following subprograms were included in WDSS software.

1. **Wlan_server.exe** (used by the CT)

   Function: Get info of available Access Point

   - EnumInterface ()→ get the GUID of local interface
   - GetProfileList ()→ get the profile list on the local interface
   - GetProfile ()→ create a XML file of target WLAN

   Output: SSID.txt and Profile.xml are saved in local folder

2. **Socket Function: ServerMain ()**

   Function: Used by the CT to open a socket to associate with the Client and execute the migration, including:

   - Ping the IP address of client
   - Open a socket to client
   - Send SSID.txt and Profile. xml to client

3. **Socket Function: ClientMain ()**

   Function: Used by the Client to open a socket to associate with the CT and get ready for the migration, including:

   - Listen to Server and accept the connect request
   - Open a socket to receive files
   - Save received files in local folder

4. **Wlan_connect.exe (used by the Client)**

   Function: Connect to Access Point using cached SSID and Profile

   - EnumInterface ()→ get the GUID of local interface
   - SetProfile ()→ deploy received profile.xml
   - Connect ()→ connect to Access Point

5.4 Additional techniques

Two additional techniques of WDSS program make it complete and functional:

- Opening Virtual Wi-Fi interface on the Wi-Fi chip set to split it into two entities, namely a basic STA and one Virtual AP. The Virtual AP entity brings Wi-Fi Direct functions.
- Configuring Internet Connection Sharing (ICS) among devices to bring small intranets into a joint network, allowing Internet services being shared by each of them.

5.4.1 Virtual Wi-Fi interface

In WDSS user scenarios, we mentioned opening a Virtual AP interface on the lamp. This is actually effectuated by splitting the single wireless adapter into one basic wireless adapter plus at most two virtual interfaces. In our user scenario, we are using only the basic wireless adapter and one virtual AP interface. These two logical interfaces are used respectively to assume [22]:

- A station interface (STA) for use by client or ad hoc wireless applications. The STA inherits all the settings of the original physical wireless adapter as identical to the physical adapter after virtualization. The STA interface is always in the system as long as the corresponding wireless physical adapter is present
- A P2P adapter for use by the P2P device. A P2P Group Owner uses this adapter to host a Virtual AP. Other devices will see it as a normal AP. A P2P Client uses this interface to form a P2P link with the GO also via its P2P interface. A Virtual AP can handle multiple clients, depending on the capability of the chip set. The P2P interfacer is present only when Wi-Fi Direct related software is running.

With these two logical entities, one device is able to connect to two networks at the same time, assuming the role of a Virtual AP meanwhile being a client of another WLAN. The method to open a Virtual AP interface in Windows 7 is to use the **netsh wlan** commands:

Netsh wlan set hostednetwork mode=allow ssid=VirtualAP key=zhangning

This command opens a Virtual AP interface. Mode is set to be 'allow', which means enabling this wireless hosted network. SSID and Key values can be manually set by users. By using the above command, we have opened a Virtual AP using the name "VirtualAP" and the Key "zhangning". Type the command as administrator in the command shell:

Netsh wlan start hostednetwork

Command	Description
netsh wlan start hostednetwork	Start the wireless Hosted Network.
netsh wlan stop hostednetwork	Stop the wireless Hosted Network.
netsh wlan set hostednetwork [mode=]allow|disallow	Enable or disable the wireless Hosted Network.
netsh wlan set hostednetwork [ssid=]<ssid> [key=]<passphrase> [keyUsage=]persistent|temporary	Configure the wireless Hosted Network settings.
netsh wlan refresh hostednetwork [data=] key	Refresh the wireless Hosted Network key.
netsh wlan show hostednetwork [[setting=]security]	Display wireless Hosted Network information.
netsh wlan show settings	Display wireless LAN global settings.

Table 5.1: Netsh wlan commands in Windows 7

The Virtual AP will start to function, broadcasting its name. Other Wi-Fi devices can detect its signals locally. More commands are shown in Table 5.1.

A P2P link between two P2P devices utilizes the Virtual AP interface of the host and the STA interface of the client. The STA interface of the host is still available for another WLAN. The connections between interfaces are shown in Figure 5.3. A multi-hop network of a tree topology is obtainable if we scale this type of links to a larger network.

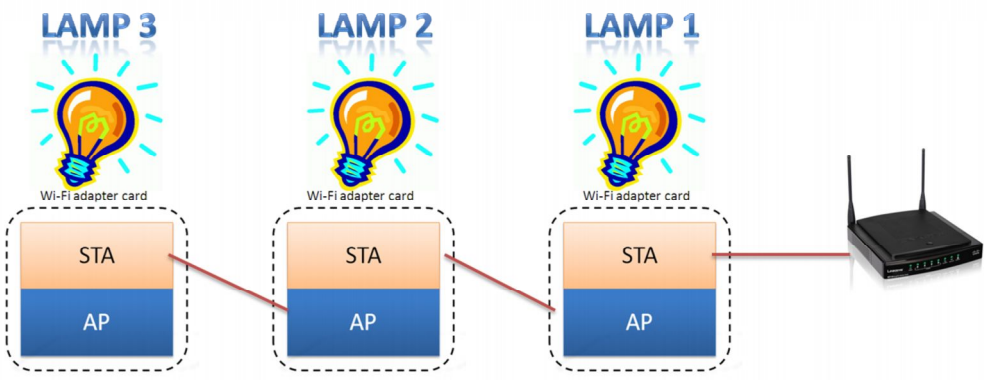

Figure 5.3: A multi-hop Wi-Fi network established by interface virtualization

5.4.2 Internet Connection Sharing

After configuring lamps to form a basic multi-hop network (Figure 5.3), each hop is an independent link, using a pair of specific SSID and Key. From IP's point of view, Lamp 1 assigns an IP address to Lamp 2 using its DHCP protocol, while the IP address of

Lamp 3 is assigned by Lamp 2 using Lamp 2's DHCP protocol, which is irrelevant to the network between Lamp 1 and Lamp 2. In another word, the hops are disjoint so that devices in the branches are invisible to those on the top. For example, lamp 2 can talk to both Lamp 1 and Lamp 3 via P2P link; however Lamp 1 and Lamp 3 are hidden to each other.

This disjoint issue can be well solved by enabling the Internet Connection Sharing (ICS) on each of the devices, so that Internet services will cover all of them, each lamp can be reached and controlled from any of the other controllers in this network via Internet based applications.

Internet Connection Sharing (ICS) is the use of a device with Internet access such as 3G cellular service, broadband via Ethernet, or other Internet gateway as an access point for other devices. It was implemented by Microsoft as a feature of its Windows operating system (as of Windows 98 Second Edition and later) for sharing a single Internet connection on one computer between other computers on the same local area network. It makes use of DHCP and Network Address Translation (NAT) [18].

ICS routes TCP/IP packets from a small LAN to the Internet. ICS maps individual IP addresses of local computers to unused port numbers in the TCP/IP stack. Due to the nature of the NAT, IP addresses on the local computer are not visible on the Internet. All packets leaving or entering the LAN are sent from or to the IP address of the external adapter on the ICS host computer. On the host computer the shared connection is made available to other computers by enabling ICS in Network Connections, and other computers that will connect to and use the shared connection. Therefore, ICS requires at least two network connections. Normally ICS is used when there are several network interface cards installed on the host. In special cases, only one network interface card is required and other connections may be logical (e.g.virtual interface) [18].

It takes the following steps in sequence to configure the ICS on Lamp 1 in Figure 5.3:

a. Right click on the basic Wireless Network Connection icon of lamp 1, open 'properties'.

b. Choose 'Sharing' column, check the box in front of "Allow other network users to connect through this computer's Internet connection". In the drop list select the connection we want to share Internet with (Wireless Network Connection of Virtual AP). In our case, there are only two wireless connections available, the STA interface and the Virtual AP interface. Since the STA interface is externally connected to the Internet, there is only one option left in the list. Therefore the default wireless connection appearing in the dropbox is the Virtual AP network.

c. Configure the STA interface to automatically obtain IP address and DNS server address

d. In Windows 7, after these configurations on the host network, the Virtual AP is automatically assigned an IP address of 192.168.137.1. The subnet of this Virtual AP would obtain IP addresses in the 192.168.137.x range.

The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. A Domain Name Service translates queries for domain names (which are meaningful to humans) into IP addresses for the purpose of locating computer services and devices worldwide. An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses. For example, the domain name *www.example.com* translates to the addresses 192.0.43.10 (IPv4) and 2620:0:2d0:200::10 (IPv6) [19].

Normally a device would obtain a DNS server address automatically from the local ISP; alternatively we can use the Google Public DNS 8.8.8.8/8.8.4.4. Google Public DNS is a free, global Domain Name System (DNS) resolution service.

Devices in the subnet of the Virtual AP would use their STA interface to connect to the Virtual AP's P2P interface, and their IP addresses are automatically assigned by the Dynamic Host Configuration Protocol (DHCP) of the host device.

Since devices in the subnet of the Virtual AP all obtain internet services through the Virtual AP, they will use the Virtual AP device as a Gateway to communicate with the external network. Therefore they have a default Domain Name System (DNS) and Gateway address both as 192.168.137.1, which is the IP address of the Virtual AP.

Recursively, the Virtual AP of lamp 2 would have a default address of 192.168.137.1 as well. Its subnet will obtain IP addresses in the 192.168.137.x range, associated to lamp 2's DHCP service, while being irrelevant to Lamp 1. The hierarchy of the IP addresses in the multi-hop lighting system is illustrated in Figure 5.4:

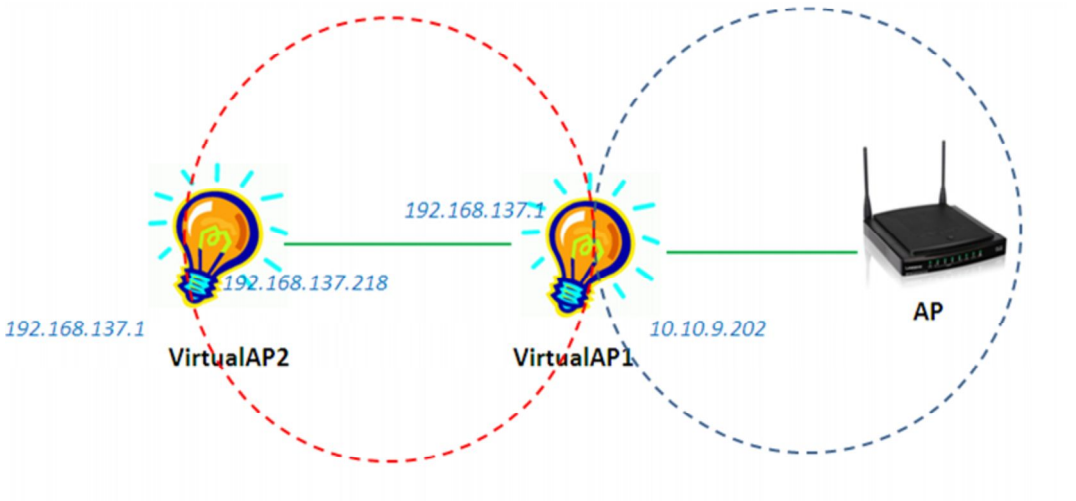

Figure 5.4: Hierarchy of the IP addresses in a ICS enabled multi-hop network

More concretely, ICS makes use of Port Forwarding technique. Port forwarding is a name given to the combined technique of:

1. translating the address and/or port number of a packet to a new destination
2. possibly accepting such packet(s) in a packet filter (firewall)
3. forwarding the packet according to the routing table.

Port forwarding allows remote computers (for example, computers on the Internet) to connect to a specific computer or service within a private local-area network (LAN) [20].

In a typical residential network, nodes obtain Internet access through a DSL or cable modem connected to a router or network address translator (NAT/NAPT). Hosts on the private network are connected to an Ethernet switch or communicate via a wireless LAN. The NAT device's external interface is configured with a public IP address. The computers behind the router, on the other hand, are invisible to hosts on the Internet as they each communicate only with a private IP address.

When configuring port forwarding, the network administrator sets aside one port number on the gateway for the exclusive use of communicating with a service in the private network, located on a specific host. External hosts must know this port number and the address of the gateway to communicate with the network-internal service. Often, the port numbers of well-known Internet services, such as port number 80 for web services (HTTP), are used in port forwarding, so that common Internet services may be implemented on hosts within private networks.

In order to observe the port forwarding actions on the multi-hop network, we have set up a multi-hop Wi-Fi network with a router and three laptops. Two laptops were linked in a string to the router, another one connected alone to the router. The system set-up is shown in Figure 5.5, with corresponding IP addresses indicated in the picture.

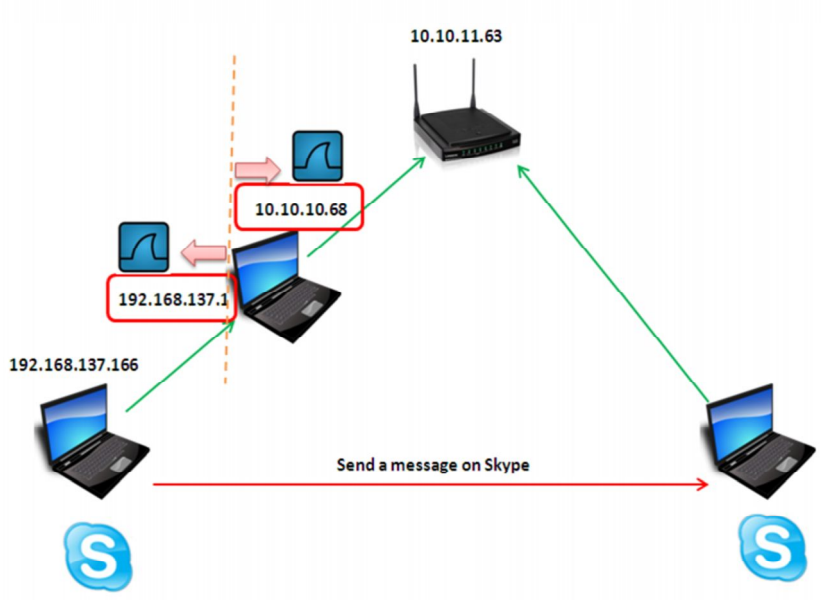

Figure 5.5: Using Wireshark to observe the port exchanges in ICS

Observing Interface	Left interface (192.168.137.1)	Right interface (10.10.10.68)
IP address exchange	192.168.137.166 –>10.10.11.63 (router)	10.10.10.38 –>10.10.11.63 (router)
port exchange	61118–>5242	62113–>5242

Table 5.2: Port exchanges in an ICS enabled network

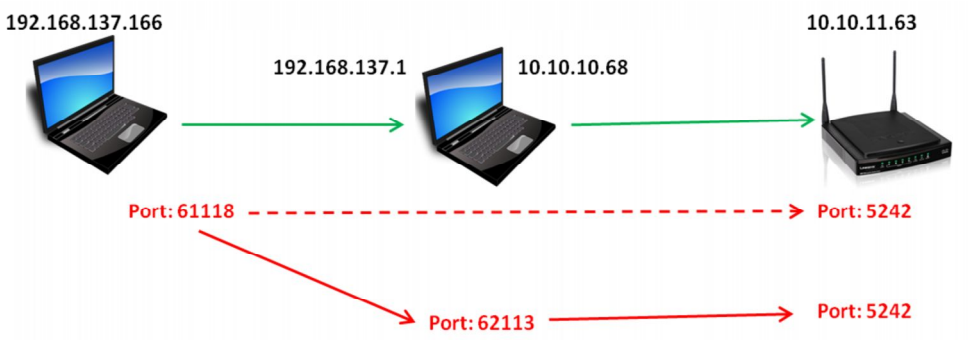

Figure 5.6: Port exchanges in an ICS enabled network

We opened a skype user end on each end device, and sent a message from the left end to the right end. On the intermediary laptop, Wireshark was used to capture packets passing by. Since there were two interfaces on the intermediary laptop (a STA and a Virtual), we opened two Wireshark windows to listen to both interfaces to the left and to the right. When a Skype message was sent from the left end laptop to the right end laptop, TCP packet was captured on Wireshark. The traffic is shown in Table 5.2.

We observed that the intermediary laptop relayed packets for the left end one. When the left end laptop sent out a TCP packet from Port 61118 with a destination IP address of 10.10.11.63 (router) which belonged to the external WLAN, the intermediary laptop checked the destination IP address and port number, transferred the packet to Port 62113 and relayed it to the router. The port forwarding process is shown in Figure 5.6. The bonding of forwarding port number and the target IP address is automatically executed when ICS is enabled.

6 Performance Analysis

6.1 Performance of router-formed multi-hop network

A router formed multi-hop network is the prototype of multi-hop Wi-Fi networks, which can be used as a standard reference for other variations. The WDSS multi-hop network is a type of the variations of multi-hop Wi-Fi networks, with the adoption of virtual APs. In order to assess the performance of the WDSS multi-hop network, we first look at the performance of the basic multi-hop Wi-Fi network formed by routers.

A router formed multi-hop network can be set up with routers working as signal repeaters. A test system was set up by Philips working group. In the test,10 Access Points (AP) E2000 from LinkSys / Cisco were used. Those APs can work as repeaters using DD-WRT, a third-party router firmware released under GPL license [21]. A chain network was set up (Figure 6.1). A message was sent out from one laptop to a given AP, and then passed to the next specified AP, and so on to the end PC. Each AP broadcast its own SSID. All E2000 routers, except the one connecting to the source notebook, were configured as repeater bridges using DD-WRT v24-spp2 K2.6. They all used a 40 MHz wide channel in the 5 GHz band.

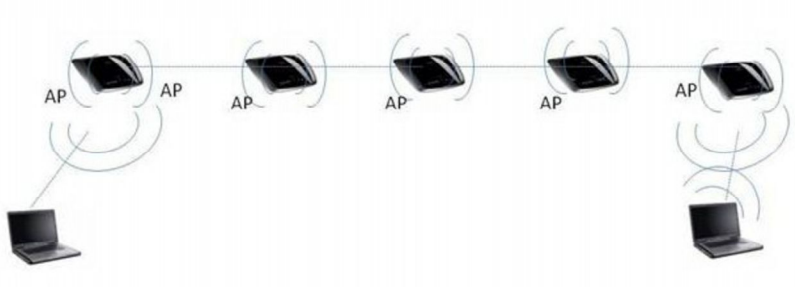

Figure 6.1: A multi-hop network formed with routers

6.1.1 Throughput over a string of routers

Data was transmitted over a string of 7 routers spaced over 115 m. The throughput is shown in Table 6.1. The throughputs of TCP and UDP are identical, only UDP has larger variation. One reason is the difference of their fundamental mechanisms. TCP has a congestion window to regularize the buffer size in the system, hence the available output data rate is smoothed over time. TCP uses end-to-end acknowledgement. The corresponding mechanism is called end to end closed-loop flow control [11]. The sender

Protocol	Throughput	Variation
TCP	$6Mbit/s$	$\pm 0.5Mbit/s$
UDP	$6Mbit/s$	$\pm 3Mbit/s$

Table 6.1: Throughput of a string of 7 nodes over 115 m

transmit packets to the receiver via multiple hops. Each packet is acknowledged by the receiver so the sender knows it was successfully transmitted. If everything goes smoothly, sender will increase its bit rate until a negative feedback is transmitted back. The sender will then tune down its bit rate to mitigate the congestion. The end-to-end flow control helps TCP traffic to reach a stable throughput after a short start-up time. An interesting property of TCP is that, any type of reasons which causes packet loss will be interpreted as traffic congestion [12]. Once traffic congestion is detected, the packet sending rate will be cut down in order to maintain a smooth traffic.

UDP, on the contrary, doesn't have any congestion control method, or acknowledgement of packets, therefore systems maybe congested sometimes, inducing an obvious variation in throughput.

6.1.2 Throughput versus Number of Hops on a String of Closely Packed Routers

Here the number of routers varies, expecting to show a declining throughput with an increased number of hops. The test results are shown in Figure 6.2 and Figure 6.3.

The measurements of UDP and TCP traffic were slightly different. When the TCP traffic was tested, amount of data was was sent out, it would tune the bit rate itself and reach a stable value at the end. Whereas, when the UDP traffic was tested, multiple times trials had to be made with different bit rate values at the same number of hops. There was a threshold of bit rate, transmissions below this value went smoothly,

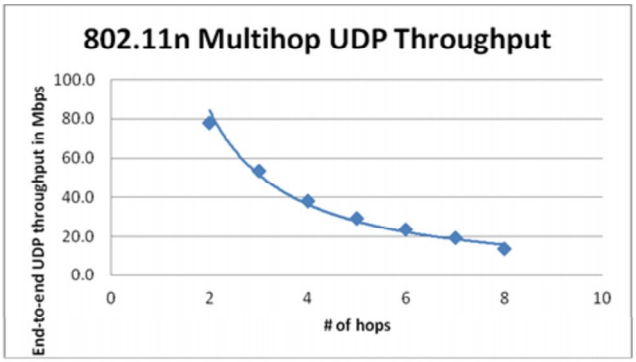

Figure 6.2: UDP throughput versus number of hops

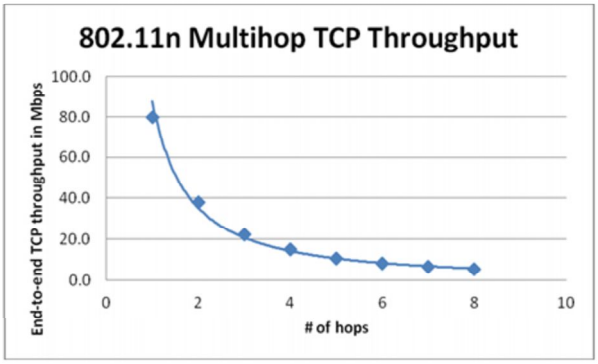

Figure 6.3: TCP throughput versus number of hops

but when data was transmitted above this value, a dramatic drop appeared in throughput. The value depicted in Figure 6.2 was this threshold being tried out, namely the maximum throughput achievable at a certain number of hops.

Figure 6.2 shows the throughput decreases with increased number of hops when using UDP. The average packet loss was measured to be between 1% to 10%. Figure 6.3 shows the same measurements with all conditions being equal, but for the use of TCP. No losses occur but the TCP throughput is half that of the UDP throughput due to: (1)TCP packets having larger packet headers; (2)TCP acknowledgements add to the load.

6.1.3 Roundtrip Delay

The round-trip delay was tested on this closely packed network, by sending ping messages over the string of APs. Two packet sizes of 32 bytes and 1024 bytes were used. For a given number of hops 100 ping commands were executed with an interval of 1 second. The results are illustrated in Figure 6.4.

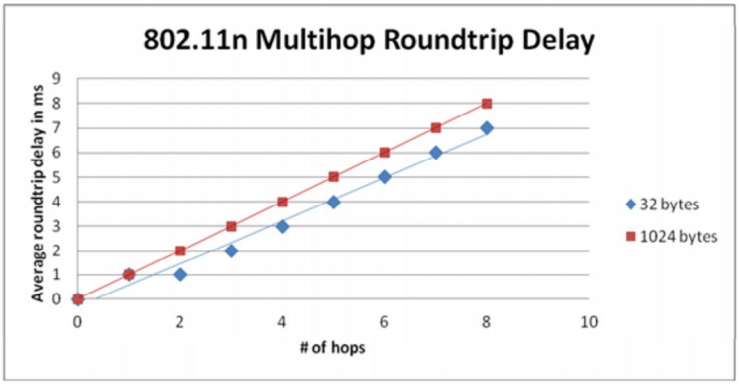

Figure 6.4: Round-trip delay as function of number of hops

6.2 Performance of WDSS netowrk

Based on a demo we have set up, some measurements have been conducted to analyze the performance of the WDSS system.

6.2.1 Setup time of P2P link

As introduced in Section 3.2, the Wi-Fi Direct specification has defined a standard network setup procedure, including device discovery, group owner negotiation, and provisioning. When two P2P devices come into range, it usually takes a couple of seconds to finish these steps. Among all the steps, scan and find phase take up the main part of setup time. In the measurement, we tried to adjust the scan related parameters and beacon interval values, to test the effects on setup time of a P2P link. The results are shown in Table 6.2.

Beacon Interval (ms)\Scan Mode	Full scan	Only scan social channels
100	5.1 ms	3 ms
50	5 ms	4.2 ms
10	5.3 ms	3 ms

Table 6.2: Setup time of a P2P link

As observed from the results, scanning only the social channels (channel 1, 6 and 11) has slightly shorter setup time than that when all the channels are scanned. While beacon interval values do not have obvious effect on setup time. This may due to no sleeping mode is deployed on the P2P devices, in another word, devices are awake listening all the time.

In practice, when power saving mechanisms are adopted, devices may fall into sleep mode periodically. A parameter DTIM defines how often a device may wake up to listen. For instance DTIM=1 means a device wakes up every one beacon interval, while DTIM=5 means it wakes up every five beacon intervals. A large DTIM means a device wakes up less frequently. On the upside, a large DTIM saves power, however, it may add to setup time because it takes longer for a device to hear beacons from others.

If we set up the P2P link in Wi-Fi infrastructure mode, instead of ad hoc mode, in the sense that an AP role is pre-assigned. The AP device will start to broadcast while the others detect its beacons and connect to it. Intuitively, this type of directional link would be faster than the pure P2P link. In our demo, we preferred to adopt the infrastructure mode links. It proved that an instant discovery was possible. The main setup delay came from user interaction (user entering passphrase, etc). After entering the passphrase, it took several seconds for provisioning.

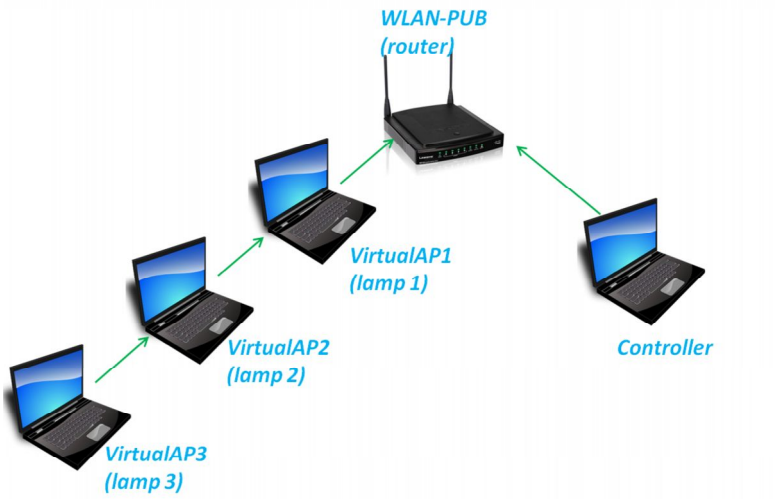

Figure 6.5: Demo system setup

6.2.2 Roundtrip latency in WDSS multi-hop network

A multi-hop network as shown in Figure 6.5 has been set up using WDSS method. Based on this network, we measured the roundtrip latency from the router to the clients via 1 hop, 2 hops and 3 hops. Two types of messages were used, one was of a size of 1024 bytes, and the other one of 32 bytes. Results are displayed in Table 6.3 and Figure 6.6.

Number of hops\Message size	1024 bytes	32 bytes
1	2 ms	1 ms
2	9 ms	6 ms
3	11 ms	10 ms

Table 6.3: Round-trip latency between AP and clients via multiple hops

We also measured the roundtrip latency from the controller which was directly connected to the AP to the Clients via 2 hops, 3 hops and 4 hops. The results are shown in Table 6.4 and Figure 6.7.

Number of hops\Message size	1024 bytes	32 bytes
2	8 ms	6 ms
3	15 ms	12 ms
4	21 ms	19 ms

Table 6.4: Round-trip latency between the controller and clients via multiple hops

Comparing with Figure 6.4, which depicts the round-trip delay measured from a router-formed multi-hop network, we can observe an increase of the round-trip delay in the WDSS multi-hop network. This may due to the difference at processing capability between the devices in WDSS demo and the routers.

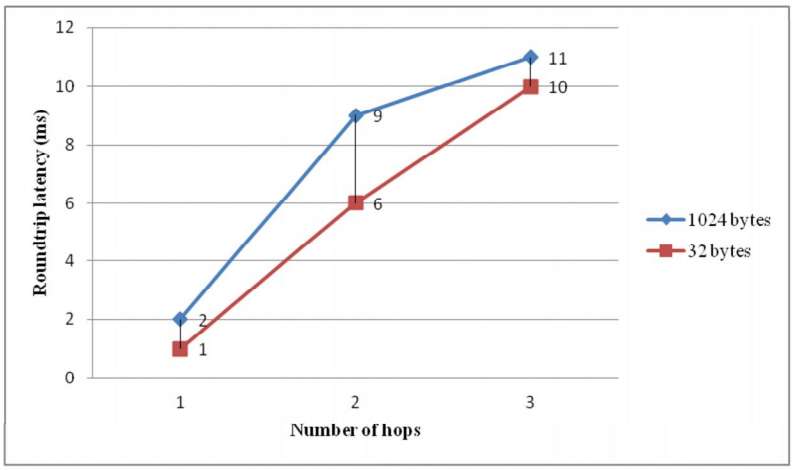

Figure 6.6: Round-trip latency between AP and clients via multiple hops

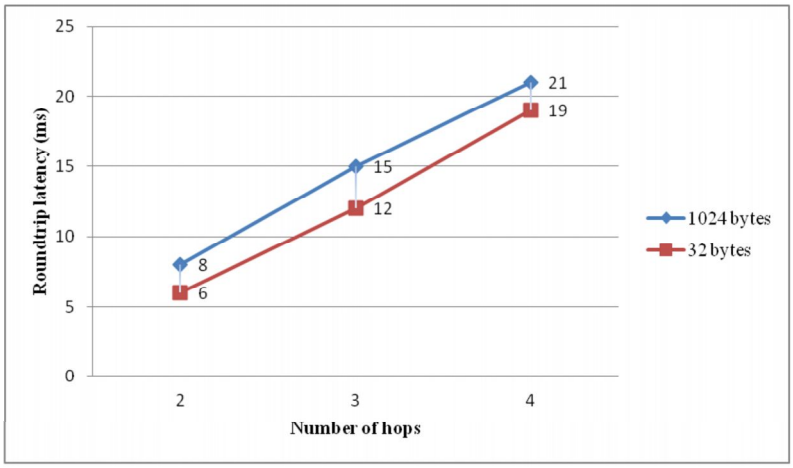

Figure 6.7: Round-trip latency between the controller and clients via multiple hops

6.2.3 Throughput in WDSS multi-hop network

We used 'Iperf' to test the throughputs of top-tier device, second-tier device and third-tier device. TCP packets and UDP packets were sent between the controller and clients. The values are listed in Table 6.5 and depicted in Figure 6.8.

Number of hops\Traffic type	TCP	UDP
2	12.2 Mbits/s	54 Mbits/s
3	6.09 Mbits/s	13.9 Mbits/s
4	4.54 Mbits/s	3.02 Mbits/s

Table 6.5: Throughput over multi-hops

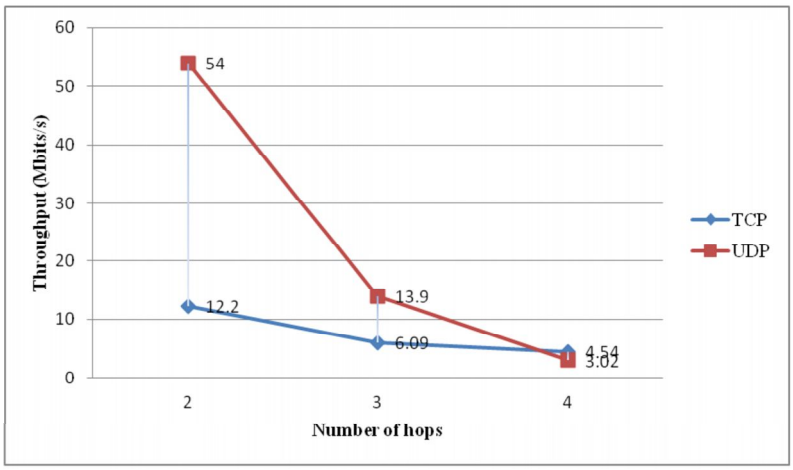

Figure 6.8: Throughput over multi-hops

Operating multiple interfaces and switching between associated networks claims a performance penalty. Measurement results show that the roundtrip latency via multiple hops is in the order of 10 millisecond. Though showing an apparent drop over multiple hops, the throughput on the WDSS multi-hop network remains relatively high, at a value well above 1 Mbits/s for both TCP and UDP traffics.

[8] has shown that running a netbook with virtualized interfaces does imply a, rather small, performance penalty. It compares the Wi-Fi infrastructure mode ad hoc network with ad-hoc mode network in terms of throughput. The former one consistently achieves higher throughput than transmissions in ad-hoc mode, thus validating the approach of connecting autonomous networks over infrastructure mode links. This is due to the use of directed links in 802.11 infrastructure mode in contrast to the broadcast-centered transmissions at a low data rate in ad-hoc mode.

7 Conclusion

In this thesis, we designed an innovative solution, Wi-Fi Direct based Smart Setup (WDSS), which was developed on a newly standardized Wi-Fi technology called Wi-Fi Direct. To overcome the limitations of conventional Wi-Fi technology for lighting applications, WDSS contributed at defining a protocol to

1. securely connect a constrained device (e.g.lamp) to an existing Wi-Fi network, without pushing a button or entering passphrase on the constrained device.
2. apply the WDSS method to extend single-hop Wi-Fi network to multi-hop Wi-Fi network among lamps, thereby guaranteeing network coverage.

This project was primarily aimed at home and small business Wi-Fi networks. The protocol used in WDSS supports WPA2-Personal networks and Open (no security) networks. WDSS protocol well solves the problems of conventional Wi-Fi technology in lighting usage. With the WDSS program developed as part of this project, we have successfully achieved the objectives of this thesis project, namely making Wi-Fi an appropriate candidate for Lighting Control.

The applicability of WDSS has been tested and validated by a demo set up as part of this project. In the demo, a 3-hop network was built up. For a typical lighting application, e.g.a 150m $*$ 150m smart store, this extended coverage is sufficient to cover the whole deployment area. Tests showed that a good performance was achievable on the this type of multi-hop network.

Compared with other similar solutions, WDSS mechanism has the following **advantages**:

- Generic solution based on Wi-Fi Direct standard, fully compatible with legacy Wi-Fi infrastructure network, transparent to Internet protocols.
- Implemented in a small application layer software, which can be easily installed on intensive electronic devices, without the requirements for hardware upgrade.
- Remaining high security levels of Wi-Fi, as well as high data rate and large bandwidth.
- Multi-hope Wi-Fi network is possible to be established in infrastructure mode, instead of ad hoc mode; thereby more universally supported by commodity chip sets, and further more outperforms ad hoc network in terms of throughput, latency and simplicity.

- Open solution with full potential to be combined with other protocols, e.g.routing protocols, to optimize the multi-hop traffic flow.
- Suitable for Lighting Control Systems, also can be easily expanded to other similar applications.

On the other side, WDSS has its **limitations** due to the fundamental Wi-Fi standard being used:

- Wi-Fi chipset is rather expensive. Currently it costs about 5 dollars per chipset. Suppliers anticipate it will drop to 2 dollars.
- Wi-Fi consumes more power compared to other low-power oriented wireless standards. Power saving mechanisms are expected to be developed and applied to the system.
- If there are a number of lamps, it might be difficult to identify the target lamp we want to commission. Wi-Fi Direct has defined 'service discovery' as an optional function in its specification. This may help distinguish types of devices. Identifying individual lamps still has to rely on better solutions, for example coded light.

As a primitive solution, WDSS can be made more sophisticated in terms of:

- The WLAN profile used in the WDSS demo was generated in Windows Operating System in a certain XML format, which is understandable by Windows PCs. In practice, this profile may be generated by various devices (PC, smartphone,etc). The format can be standardized in order to be understandable by a variety of devices.
- Assuming no pre-designed topology is available, the WDSS multi-hop network is rather difficult for end users to configure. To make it easier, more intelligentm routing protocols can be adopted to self-optimize the network distribution.
- In a more intelligent Lighting System where sensors are adopted, intra-communications between sensors and lamps can be made possible for Lighting Automation.

These aspects are interesting topics for future research.

Bibliography

[1] Wi-Fi Alliance, (2010). *Wi-Fi Simple ConfigurationTechnical Specification Version 2.0.0.*

[2] Wi-Fi Alliance, (2010). *Wi-Fi Peer-to-Peer (P2P) Technical Specification Version 1.1.*

[3] ZigBee Alliance, (2010). *ZigBee Home Automation Public Application Profile*

[4] Raoul van Bergen, (2008), *ZigBee Mesh Networking*, Field Application Engineer Embedded - EMEA Digi International.

[5] Atheros, (2011). *Programmer Guide to Atheros Direct Connect API for Windows*

[6] IEEE P802.11s^{TM}/D12.0 Part 11: *Wireless LAN MAC and PHY specifications, Amendment 10: Mesh Networking*, (2011)

[7] IEEE Std 802.11n Part 11: Wireless LAN and PHY specifications, Amendment 6: *Enhancements for Higher Throughput*, (2009)

[8] Hanno Wirtz, Tobias Heer, Robert Backhaus, Klaus Wehrle*, (2011). *Establishing Mobile Ad-Hoc Networks in 802.11 Infrastructure Mode*

[9] Bahl, P., Adya, A., Padhye, J., And Walman, A. Reconsidering wireless sytems with multiple radios. *SIGCOMM Comput. Commun, Rev. 34* (October 2004), 39-46

[10] Chandra, R., Bahl, P., and Bahl, P. Multinet: Connectiong to multiple ieee 802.11 networks using a single wireless card. In *IEEE INFOCOM* (2004)

[11] *Data Communication Networking* Technique Press, Amsterdam, 2006, ISBN -90-8594-008-7.

[12] Jochen H. Schiller. *Mobile Communications*. Second Edition.

[13] Microsoft. VirtualWiFi Project. [Online] Available `http://research.microsoft.com/enus/um/redmond/projects/virtualwifi/`, May 18, 2011

[14] `http://en.wikipedia.org/wiki/IEEE_802.11s`

[15] `http://www.slideshare.net/ENGMSHARI/wpa2`

[16] `http://en.wikipedia.org/wiki/Mobile_ad_hoc_network`

[17] `http://en.wikipedia.org/wiki/List_of_ad_hoc_routing_protocols`

[18] `http://en.wikipedia.org/wiki/Internet_Connection_Sharing`

[19] `http://en.wikipedia.org/wiki/Domain_Name_System`

[20] http://en.wikipedia.org/wiki/Port_forwarding

[21] http://www.dd-wrt.com

[22] http://msdn.microsoft.com/en-us/library/windows/desktop/dd815243(v=vs.85).aspx