A Wi-Fi Direct System Architecture
for Proximity-Based Applications

Amin Mazloumian
Institute of Embedded Systems
Zurich University of Applied Sciences
Winterthur, Switzerland
amin.mazloumian@zhaw.ch

Matthias Rosenthal
Institute of Embedded Systems
Zurich University of Applied Sciences
Winterthur, Switzerland
matthias.rosenthal@zhaw.ch

Abstract—The widespread adoption of Wi-Fi made the need for easy, fast, and reliable ad-hoc networking much more critical. The Wi-Fi Direct standard provides a fast, stable, and secure connection which can be easily established between devices without requiring a wireless access point or an Internet connection. This is especially important as users of mobile phones can keep connection to several devices simultaneously without interrupting their Internet connection. Compared to Bluetooth, Wi-Fi Direct is more secure, operates at data rates of up to 250 Mbps, and covers distances up to 150 meters. We will give a short overview of Wi-Fi direct in general and then describe how it can be used for proximity-based applications such as ticketing systems, localized advertising and dynamic crowd management (e.g. football stadiums). The specialty of our implementation of Wi-Fi direct is that we utilize a star-like network. In this network, our server node works as the group owner in its center. All clients connect to the server node, which takes care of authentication, dynamic IP assignment and blacklisting. This architecture has also the advantage that it can be extended to service more clients by chaining server nodes together. In this paper, we describe the software components of our system and discuss the critical aspects of its design with respect to security, notification, and authentication. Finally, we compare our approach with other systems and investigate its limitations and differences.

Keywords—Wireless; WLAN; Wi-Fi Direct; P2P; D2D; WSC; Proximity-based service; Infrastructure mode; IEEE 802.11; Soft-AP; WPS Provisioning

I. INTRODUCTION

The widespread adoption of Wi-Fi made the need for easy, fast, and reliable ad-hoc networking much more critical. To fulfill this critical need, the Wi-Fi Direct standard (also known as Wi-Fi Peer-to-Peer, or simply P2P) has shown a huge potential. The Wi-Fi Direct standard, proposed by Wi-Fi Alliance, is currently the most prominent Device-to-Device (D2D) communication standard and is widely supported by many device manufacturers [1]. The recent versions of Android (version 4.0 and later), the most popular operating system for smart phones and tablets for example, include support for the Wi-Fi Direct standard. Moreover, latest Linux kernels (kernel version 3.0 and later) added support for the standard. The support of Wi-Fi Direct in Linux kernels implies that the Peer-to-Peer standard can be utilized on industrial Wi-Fi server modules with embedded Linux distributions as their operating systems.

In the following, we list the main features of Wi-Fi Direct that made it popular for content sharing between devices such as smart phones, tablets, printers, game consoles and etc.:

- Devices connect to each other without requiring any access point (similar to IEEE 802.11 ad-hoc mode). This feature is supported by a software implementation of Access Point functionality (Soft AP).
- The standard is fully implemented in software over traditional Wi-Fi radios in IEEE 802.11 infrastructure mode. Therefore, a P2P connection runs over typical WLAN speeds and utilizes the same security and power-saving capabilities that have been developed in over a decade.
- Devices that do not support the Wi-Fi Direct standard see the Wi-Fi Direct device which provides the Access Point functionality (Soft AP) as a normal Access point and can connect to it in exactly the same way they do to an Access Point.

However, recent studies indicate that the standard has only reached a small fraction of its potential and can be used in a whole new range of applications. Pyattaev et al. (2013) demonstrated how cellular traffic can be effectively offloaded onto Wi-Fi Direct Device-to-Device (D2D) links and provided...
the estimated gains in energy efficiency and capacity from such offloading [2].

Sharafeddine et al. (2013) studied capabilities and limitations of smart phones to utilize multiple wireless interfaces simultaneously for advanced wireless networking techniques such as cooperative content distribution with Device-to-Device (D2D) communications, heterogeneous network offloading, or personal area network sharing [3].

In another study, Asadi and Mancuso (2013) assessed the implementation feasibility of D2D communications and its challenges by introducing a protocol using LTE and Wi-Fi Direct technology [4].

In this paper, by focusing the optional concurrent feature of P2P devices, i.e. supporting Wi-Fi Direct, WLAN, and mobile data network concurrently, we show how the standard can be effectively used for proximity-based applications. Although implementing the concurrent feature is optional as specified in the standard, more and more devices are implementing this feature [3].

The paper is organized as follows. Section II is a brief overview of the Wi-Fi Direct standard. In Section III, the network architecture and properties of a proximity-based service provider network is introduced. An implementation of the proposed software architecture is explained in Section IV. Finally, in Section V various aspects of our design are discussed.

II. WI-FI DIRECT OVERVIEW

In this section, we introduce the typical scenario in which Wi-Fi Direct devices establish connection to communicate with each other. However, the detailed description of the Wi-Fi Direct Standard is out of the scope of the current paper (See [1] for the Wi-Fi Direct standard specification by the Wi-Fi Alliance).

Wi-Fi Peer-to-Peer (P2P) devices form P2P groups to communicate with each other. Each P2P group is composed of one Group Owner (GO) and several P2P Clients. The Group Owner of a P2P Group acts similar to an Access Point. It also performs authentication and IP assignment with a Dynamic Host Configuration Protocol (DHCP) server for clients. Each P2P device should be able to take both P2P Group Owner and P2P Client roles.

Group formation between P2P devices is typically composed of the following steps: P2P Discovery procedure, P2P Group Negotiation, P2P Wireless Simple Configuration (WSC) provisioning, and finally IP assignment.

P2P Discovery

In this step, P2P devices try to find and connect to other P2P devices. To exchange device information, P2P devices send Probe Requests and receive Probe Responses. Probe Requests and Probe Responses are wireless beacon frames which include device information and connection-related states of the device.

A P2P device becomes discoverable by going to Listen state. In the Listen state, the device listens to Social Channels (channel 1, 6, and 11) and waits for possible Probe Requests from other P2P devices. In case a device in the Listen state, encounters a P2P Probe Request, it sends a P2P Response beacon frame.

P2P devices discover other devices including Legacy devices (devices without Wi-Fi Direct support) by sending Probe Requests in the Scan phase. The scanning process is defined in IEEE Std. 802.11-2012 [5].

Finally, P2P Find phase ensures that two simultaneously searching P2P devices see each other on the same channel. This is achieved by randomizing the Listen state time on each of the Social Channels. The reason behind choosing only the Social Channels in the P2P Discovery phase is to decrease the time it takes for P2P devices to find each other by the randomization procedure.

P2P Group Owner Negotiation

The P2P Group Owner (GO) of a P2P group and its characteristics are defined over a three-way wireless frame exchange procedure: GO Negotiation Request, GO Negotiation Response, and GO Negotiation Confirmation. In the negotiation procedure, P2P devices express their desire to become the Group Owner with a number, i.e. Intent number. If the intent values which two devices exchange in the GO Negotiation Request and Response are equal, then the Group Owner is defined randomly.

P2P Wireless Simple Configuration (WSC) Provisioning

A secure connection between P2P devices is provided by the Wi-Fi Protected Setup (WPS) standard [6]. The standard is built on the Wi-Fi Protected Access 2 (WPA-2) protocol. The protocol was defined by the Wi-Fi Alliance in 2004 when researchers found serious weaknesses the previous standard, Wired-Equivalent Privacy (WEP).

The defined Peer-to-Peer Group Owner (GO) mainly authenticate the P2P Clients with any of the following two simple methods: Push-Button-Connect, and Personal Identification Number (PIN) method. In the Push-Button-Connect (PBC) method, on the P2P GO a physical button on the device or a virtual software button should be pressed followed by a virtual button press in a P2P Client. In the PIN method, the P2P Client device should send the P2P Group Owner a pre-shared PIN code.

As explained above, Wi-Fi Protected Setup (WPS) uses the Wi-Fi Protected Access together with a PIN or PBC method. However, in December 2011 it was shown that the PIN method is prone to brute-force attack [7, 8]. More specifically, in few hours an attacker can find out the PIN of a client and bypass the WPA2 security. In the Discussion section, it is explained why this flaw is not a concern in the application introduced in this paper.

IP Assignment

The IP assignment phase is not specific to the Wi-Fi Direct standard and therefore not included in the Wi-Fi Direct standard documentation. However, it is obvious that the P2P devices in the same P2P group should have IPs in the same range for their P2P interface to be able to communicate with each other. Therefore, the defined Group Owner device should
first assign an IP to itself and then, run a DHCP server for the other devices in the group (P2P Clients).

III. A SYSTEM ARCHITECTURE FOR PROXIMITY-BASED APPLICATIONS

A system architecture for proximity-based applications is introduced in this section. By proximity-based applications, we mean the applications which provide services, such as e-ticketing or crowd management, within a certain neighborhood for mobile users, i.e. smart phone, tablet, and laptop users.

The system is composed of a wired or wireless network of wireless Peer-to-Peer service provider devices. Each of these service providers acts as a Peer-to-Peer Group Owner (P2P GO) in its local neighborhood to which mobile users connect as Peer-to-Peer Clients (Fig. 1). Therefore, the infrastructure service provider P2P devices not only provide application-specific services to mobile users, but also perform authentication and IP assignment.

The system architecture has three important factors which make its design especially convenient for proximity-based applications: a) In our design the P2P Groups are formed autonomously by service provider devices; b) The Peer-to-Peer Groups work in P2P Persistent mode; c) Mobile users can highly benefit from their concurrent mode if available.

Autonomous Peer-to-Peer Group formation by service provider devices

Every service provider device autonomously starts a Peer-to-Peer Group and becomes its P2P Group Owner. Therefore, the Group Owner Negotiation step with future P2P Clients (mobile users) is always skipped. Bypassing the P2P Negotiation is mentioned as a possible variation in the Wi-Fi Direct standard. This is not a typical P2P group formation procedure, but is best-suited for our purpose. Because, it puts the infrastructure service provider devices in control of all required communications and authentications for mobile users (P2P Clients).

Persistent Peer-to-Peer Groups

The service provider devices start the Peer-to-Peer Groups in P2P Persistent mode. Setting the P2P Groups to persistent mode causes all P2P Clients to store network credentials and the Group Owner (service provider device) data which can be used for quicker future connections [9]. A mobile user in our system can therefore reconnect much faster using a P2P Invitation procedure from the Group Owner (service provider) or P2P Clients (See [1] for a detailed description of the P2P Invitation procedure).

Concurrent Operation mode of mobile devices

The most important and unique feature of our system architecture is that its underlying Wi-Fi Direct standard let the devices which support the P2P Concurrent mode to connect to the service provider without interrupting their WLAN or mobile data network.

To support P2P Concurrent mode, a device should be able to support multiple Media Access Control (MAC) entities. For instance, one MAC entity operates as a P2P Client and the other MAC entity as WLAN. This can be implemented in the device by two separate pairs of MAC and PHY entities, or two virtual MAC entities over one PHY entity.

Support for non-Concurrent P2P devices and Legacy devices

Although our solution is best fitted for P2P Concurrent devices, the devices which do not support P2P Concurrent mode can still connect as P2P Clients. Even the devices which do not support Wi-Fi Direct (Legacy devices) can connect to the service provider devices (P2P Group Owners in our system) in the same way as they connect to WLAN Access Points.

IV. IMPLEMENTATION

The software and hardware components which were used in the implementation of the system architecture are explained in this section. The reader should keep in mind that this implementation is only one of the numerous possible ways to realize such a system.

Moxa AWK-5232 devices (Industrial IEEE 802.11n dual-radio wireless access points manufactured by Moxa) were used as service provider devices. These devices have two Wi-Fi antennas, one of which was used to serve the P2P Clients and the one was used to be chained with other P2P server provider devices.
The Peer-to-Peer feature in the embedded Linux of the Moxa devices was enabled by using WPA Supplicant version 2.1 [10, 11]. WPA Supplicant is an open-source software which lets the devices to work as Soft-APs (software access points).

WPA Supplicant also performs the WPS authentication of P2P standard. The software should be configured to P2P mode (mode = 3), and the P2P group setting should be set to persistent with maximum Group Intent value (intent=15). Moreover, the key management attribute should be set to ‘WPA(2)-PSK’. Interestingly, WPA Supplicant has also a blacklisting feature which enables the service provider devices to block certain MAC addresses among P2P Clients.

Finally, Dnsmasq version 2.6 was used as the DHCP server for automatic IP-assignment to P2P Clients [12]. Dnsmasq is also an open-source software and it can be configured with IP ranges of the P2P Clients.

V. SUMMARY AND DISCUSSION

A Wi-Fi Direct system for proximity-based applications was presented in this paper. The system is especially designed for proximity-based applications. The concurrent devices can most benefit from this system as they can use the provided services without disconnecting from their data network and WLAN connections. It is noteworthy that more and more devices are supporting the concurrent mode. Nevertheless, the system supports the P2P devices which do not support the concurrent mode and even the devices without Wi-Fi Direct (P2P) support.

The underlying Wi-Fi Direct operates at infrastructure Wi-Fi mode and takes the advantage of the over a decade experience in its security. However, as discussed in Section III, the Wi-Fi Protected Setup (WPS) authentication that was mainly developed for minimal user intervention for the P2P standard has security issues, i.e., an attacker in worst case can connect to the service provider devices. However, the service provider devices in our system architecture aim to let any device to establish a connection as simple as possible and mainly protect their one-to-one connections with their P2P Clients using WPA-2. The one-to-one security is therefore ensured with or without any unwanted connection from an attacker. Moreover, as the system is configured in a way that P2P Clients cannot connect to each other. Hence, the attacker as well cannot connect to any other P2P Client. This means WPS authentication does not cause any security concern in our system architecture with the specified configuration.

ACKNOWLEDGMENT

The authors would like to thank Hans Gelke, Matthias Frei, and Tobias Kammacher for their valuable comments.

References