An Overview and Experiment on Wi-Fi Direct Connection Behaviour with Network Analysing Tools

Thian Seng Lee[1(✉)], Paul Gardner-Stephen[2], Riza Sulaiman[1], and Nazlena Mohammad Ali[1]

[1] Institute of Visual Informatics, National University of Malaysia, 43600 Bangi, Malaysia
thianseng01@yahoo.com, {riza,nazlena.ali}@ukm.edu.my
[2] College of Science and Engineering, Flinders University, Adelaide, South Australia 5001, Australia
paul.gardner-stephen@flinders.edu.au

Abstract. In the context of Wireless Collaboration Network (WCN), mobile devices with the wireless connection capability connect and communicate with each another for data exchange or resource sharing. The wireless technology used in forming the wireless network has been upgraded and improved throughout the years. Wi-Fi Direct is one of the well-established Wi-Fi P2P standards which can be found in almost all Android OS based mobile devices. In this work, the performance and operations of the Wi-Fi Direct standard when forming a P2P connection was reviewed by utilizing the network analysing tools. A systematic review was conducted by comparing the Wi-Fi Direct operations theoretically and practically. An overview of Wi-Fi Direct was presented, followed by experimental testing on the real-time P2P connection using physical mobile phones. The laptops and smartphones with the network traffic analyzer software (Wireshark and Wi-Fi Analyzer) installed were used to record and analyse the performance of the P2P connection activity. Finally, the findings and conclusions were discussed base on the statistical data collected from the experiment. It has been observed that there is a fixed pattern of SSID formed by Wi-Fi Direct framework regardless of the mobile devices brand, and the size of the Wi-Fi probes are device-dependent.

Keywords: Wireless Collaboration Network · Peer-to-peer · Device-to-device · Manet · Ad-hoc network · Android · Wi-Fi Direct · Network analyser · Wireshark

1 Introduction and Background

Every year, mobile devices with improved capabilities and intelligence are introduced to the market. The devices are being used for many purposes such as communication, information searching, entertainment, financial transaction, and many other intelligence functionalities. Most of the functionality of a mobile device required network connectivity, in online or offline mode. Base on the forecast updated by Cisco [1], there

© Springer Nature Switzerland AG 2019
H. Badioze Zaman et al. (Eds.): IVIC 2019, LNCS 11870, pp. 368–379, 2019.
https://doi.org/10.1007/978-3-030-34032-2_33

will be 1.5 mobile device per capita or 12.3 billion mobile-connected devices by 2022. The rapidly growing number of mobile devices in the market is among the factor of innovation in cellular communication technology. The 2G cellular technology has evolved to the latest 5G with higher bandwidth, broader coverage, and ultra-low latency to ensure the eminent quality of network connectivity [2]. The cellular communication technologies required a robust and stable backbone infrastructure with an intermediary agent at a high cost. It is inevitable that such infrastructure-based communication might be unavailable sometimes. For example, during a disaster or when the device is out of the coverage area. Besides, the cost of the data traffic subscription, the availability of the technology in the region, and the compatibility of the mobile devices to the new technology are the other factors where some mobile users could not enjoy the new technology in the short term. [1] reported that the offload traffic generated by mobile devices which connect to the fixed network will be higher than cellular traffic from the mobile devices by 2022. The public Wi-Fi hotspots are expected to grow from 124 million in 2017 to 549 million by 2022, and the Wi-Fi homespots (hotspots at home) is expected to grow from 115 million in 2017 to 532 million by 2022. This shows that the local Wireless Collaboration Network (WCN) as suggested in [3] is a potential supplementary to complement cellular communication technology.

The WCN is an ad-hoc peer-to-peer (P2P)[1] network formed by the end user's mobile devices through common wireless technologies like Bluetooth and Wi-Fi interfaces. For decades, the wireless technologies have been revised and upgraded to support better network connectivity. The new Bluetooth (5.0) standard was introduced to the market in 2016, with the improved bandwidth, connectivity range and the maintained low energy consumption [4]. The Wi-Fi standard was well established and has been upgraded from 802.11a to 802.11aq with device mobility support, broader coverage area and connection stability [5]. Unfortunately, it is not always available in every mobile device. At the point of writing, there is no standard protocol which could efficiently integrate the wireless technologies to form a robust WCN. The main challenges of forming the working WCN has been reported in [3].

As mentioned above, Wi-Fi and Bluetooth are the common wireless interface available in the end user's mobile devices. Comparison of different approaches used to form the WCN has been conducted and presented by [6] and [7]. The outcome from the comparison shows that the Bluetooth standard is more stable and established when forming WCN. However, due to the limitation of Bluetooth standard in terms of range and bandwidth, Wi-Fi standard has become the preferable standard in forming WCN. The term mobile devices in a WCN covers a wide range of mobile products. In this work, the scope of mobile devices was narrowed to focus only on a smartphone, considering the ubiquity nature of mobile phones. There are many brands of the smartphone in the market, with different types of Operating System (OS). All smartphones are equipped with at least one or more Wi-Fi interfaces which support basic Wi-Fi connectivity. However, the implementation of P2P Wi-Fi connectivity function is OS-dependent. For example, Apple Inc. has integrated MultipeerConnectivity

[1] Peer-to-peer (P2P) is also known as device-to-device (D2D) by some researchers.

framework[2] (also known as Apple Wireless Direct Link, AWDL) to their proprietary OS (iOS). For the Android OS-based devices, the P2P connection standard is known as Wi-Fi Direct[3]. At the point of writing, the integration of P2P Wi-Fi connectivity between the two abovementioned OS is not possible. We have chosen to focus this research on Android's Wi-Fi Direct standard. This is because Android is an open-source OS, and according to the survey report by [8], Android has been the leading OS since 2011. Wi-Fi Direct has been introduced to the market for many years. However, there is no one standard solution which could efficiently exploit the wireless technologies to form a robust WCN. Therefore, a standardized approach for all mobile devices when forming WCN is needed. But first, the architecture and the functionality of the wireless technology must be explored thoroughly. In this work, comparison was done on the operations of the Wi-Fi Direct connection theoretically as specified in the technical documentation [9], with the connection practically formed by physical devices. The stations (Laptops) with network analyser installed were set-up to analyse the performance and flow of connections.

2 Overview of Wi-Fi Direct Standard and Operations

Wi-Fi Direct, formally known as Wi-Fi Peer-to-Peer certified by Wi-Fi Alliance is a wireless mode which builds upon the Wi-Fi infrastructure mode [9]. However, unlike the common infrastructure mode, Wi-Fi Direct mode does not require an Access Point (AP). The participating devices will negotiate to designate a device to take over the AP-like role. The device with the AP-like role is referred to as the Group Owner (GO), and the devices connected to the GO is referred to as Clients. The clients that connecting to the GO could be a legacy client[4] or a P2P client base on Wi-Fi Direct standard. Figure 1 depicts the P2P topology formed between GO and two clients. The concurrent operation as shown in Fig. 2 is possible if the GO supports multiple Wi-Fi interface either physically or virtually. The GO in the concurrent operation acts as the middle entity between two Wi-Fi groups. In the first group, the GO performs the role as a

Fig. 1. Different types of P2P topology formed by Wi-Fi Direct standard.

[2] 'MultipeerConnectivity Framework', *MultipeerConnectivity, Apple Developer Documentation*, Apple Inc., 2019, https://developer.apple.com/documentation/multipeerconnectivity (accessed 1st July 2019).

[3] 'Discover Wi-Fi, Wi-Fi Direct', *Wi-Fi Diect, Wi-Fi Alliance*, Wi-Fi Alliance, 2019, https://wi-fi.org/discover-wi-fi/wi-fi-direct (accessed 1st July 2019).

[4] A legacy client connects to the Wi-Fi Group using conventional 802.11 Wi-Fi standard, as if the client is connecting to an AP in Wi-Fi infrastructure mode.

Fig. 2. Concurrent operation of a P2P device (middle).

Wireless LAN Client which connecting to an AP. In the second group, the same GO performs the AP-like role and form a connection with other clients. The concurrent ability of a P2P device allows connectivity expansion for resources sharing and transmission [6].

2.1 P2P Group Formation

The devices will go through several stages when forming the P2P Group. Depends on the pre-condition, the group forming stages normally include Discovery, GO negotiation, Wi-Fi Protected Setup (WPS) Provisioning, and Address Configuration. During the Group formation, the P2P devices communicate by sending network frames such as Beacons, Probe Requests and Probe Responses. Initially, the devices with the Wi-Fi P2P mode enabled will be turned to Listen State. The device in the listen state will randomly pick one of the Listen Channel from the list of Social Channels. The Social Channel include channel 1,6 or 11 for devices operating in the 2.4 GHz band. The minimal period of a P2P Device in the Listen State is at least a contiguous period of 500 ms every 5 s so that other P2P devices can discover it. Figure 3 demonstrates the sample simplified process of forming a P2P Group.

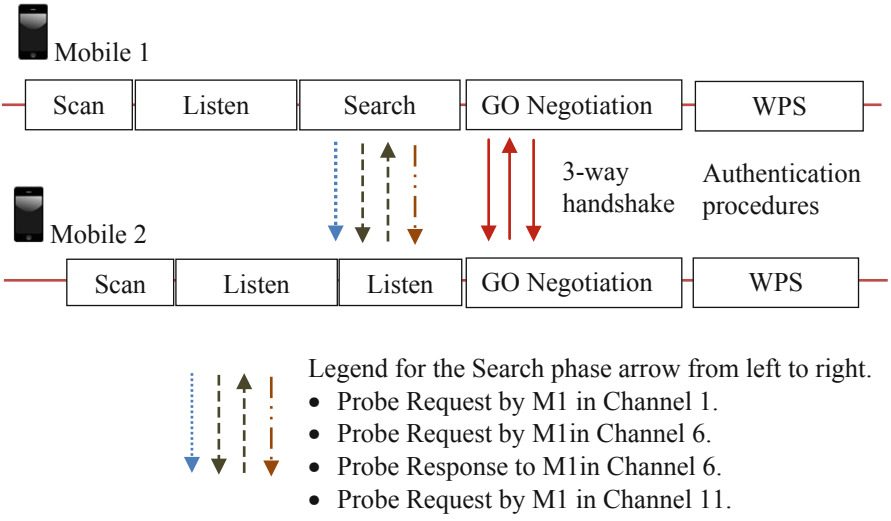


Fig. 3. Sample P2P group formation process.

P2P Devices Discovery. Along the Listen State, the devices will alternate between Scan and Find phases. During the Scan Phase, the devices will scan all Social Channels to collect information about surrounding devices. The objective of the Scan Phase is to find a P2P or P2P Group and fix the channel to establish a P2P Group. During the Find Phase, the device will alternate between the Listen State and the Search State at a random integer N interval of 100 TUs. The device in the Find phase will waits (Listen State) or send (Search State) for Probe Request or Discovery Beacon frames on each of the Social Channels.

GO Negotiation and WPS Provisioning. Assume that it is the first time the P2P devices attempt to form the P2P group; the GO Negotiation stage will begin after the Discovery stage ended and the neighbour P2P devices have been identified. During this stage, the P2P devices will negotiate the GO role using a three-way handshake procedure. The procedure requires the transmission of GO request, response and confirm frames.

After the GO role has been confirmed, the P2P devices will move on to the WPS Provisioning stage. WPS provisioning is compulsory in Wi-Fi Direct standard and normally requires minimal user intervention (e.g. Pressing a button displayed on the screen). The WPS procedure utilizes WPA-2 security and uses Advanced Encryption Standard (AES)-CCMP as cipher and a randomly generated Pre-Shared Key (PSK) to form the authentication credential. The authenticated credential will be used by the P2P devices to skip the GO Negotiation stage and link back to the previously connected GO directly. WPS Provisioning is out of the scope of this work and therefore we do not further explain the details here.

3 Experimental Environment Setup

After the Wi-Fi Direct architecture was reviewed, the experiment was conducted on physical smartphones for comparison between theory and reality. The hardware used in the experimental platform includes two laptops and two smartphones. The software used is the network analyser-Wireshark Desktop[5] and Wi-Fi Analyzer[6] from Google Play. Wireshark was installed in the two laptops and Wi-Fi Analyzer was installed in the two smartphones. The specification details of the hardware and software are listed in Table 1. The smartphones were used to form the P2P connection and the laptops were used as the station to capture the frame transmission between the smartphones.

[5] Wireshark download page, Wireshark, 2019, https://www.wireshark.org/download.html (accessed 1st July 2019).

[6] Wifi Analyzer Classic download page, Google Play, 2018, https://play.google.com/store/apps/details?id=com.farproc.wifi.analyzer.classic&hl=en (accessed 1st July 2019).

Table 1. Hardware and software used for experimentation

Hardware	Specifications (model, OS, Wi-Fi interface)
PC 1	HP Pavilion dv4, Ubuntu version 16.04 LTS, Intel Wi-Fi card Pro/Wireless 5100AGN
PC 2	HP Pavilion 14, Ubuntu version 16.04 LTS, USB Wi-Fi dongle TP-Link TLWN727 N
Smartphone 1	Samsung Galaxy J1 mini Android 6.0.1, Wi-Fi b/g/n
Smartphone 2	Lenovo A5000, Android 4.4.2, Wi-Fi b/g/n
Software	Details (name, version, type)
Network traffic analyser	Wireshark, 2.6.6, Third-party freeware (wireshark.org)
Wi-Fi analyser	Wifi Analyzer Classic, 3.11.2, Third-party freeware (Google Play)

3.1 Preliminary Setup

The distance between laptop-to-smartphone and smartphone-to-smartphone were fixed based on the signal strength range within −30 dBm to −67 dBm. This is the reliable Wi-Fi signal strength as suggested by [10]. The signal strength was measured using the Wi-Fi Analyser (Wifi Analyzer Classic) installed in the smartphones. Wifi Analyzer Classic is a free mobile application on Google Play. It is normally used to scan the and display the strength of the Wi-Fi channels surrounding the smartphone. To improve accuracy, both smartphones were used for measurement. A signal broadcast station is needed so that the receiving device(smartphone) can receive the signal for signal strength measurement. To achieve this, the built-in mobile hotspot feature of the HP Pavillion 14 laptop and the tethering feature of the Samsung smartphone were utilized to form the broadcast stations.

To get an ideal distance with good signal coverage between laptop-to-smartphone, the Lenovo phone with the Wi-Fi Analyser was used to measure the SoftAP signal strength based on the broadcast signal by the HP Pavillion 14 laptop. The measurement result's screenshot can be found in Fig. 4a. Referring to the screenshot, The signal with the highest signal strength was transmitted by the Laptop on channel 11, with SoftAP name begin with "DESKTOP". With the signal strength around −50 dBm, the distance between the smartphone and the laptop was approximately 210 cm.

For the smartphone-to-smartphone distance, the Samsung smartphone's tethering service was activated to form the SoftAP name "AndroidAP". Then, the signal strength of the signal transmitted by the SoftAP was measured by the Lenovo smartphone. The measurement result's screenshot can be found in Fig. 4b. Referring to the screenshot, the signal with the second-highest signal strength on channel 6 was transmitted by Samsung's SoftAP named "AndroidAP". Same as the previous measurement, the distance between the two smartphones was fixed at approximately 210 cm, with the signal strength −50 dBm.

a) smartphone-to-laptop b) smartphone-to-smartphone

Fig. 4. Wi-Fi signal strength measurement with a Wi-Fi Analyser.

3.2 The Wireshark Analyser

Wireshark is a free and open-source network traffic analyser software under GNU GPLv2 license. It is normally used to capture and analyse the packet flow between network devices. Before we begin the packet capture activity, three initial configuration steps were performed.

Step 1. Wi-Fi Operational Mode Configuration. The type of packets flowing in a network could be either unicast, multicast or broadcast. The default operation mode of a Wi-Fi interface is promiscuous (or managed). In promiscuous mode, only unicast packets can be captured by the Wi-Fi interface. The Wi-Fi interface must be configured into the monitor mode to capture the multicast and broadcast packets. However, unlike the promiscuous mode, which is supported by all Wi-Fi interface, the monitor mode is interface-dependent. That is the reason why we included the external dongle (refer Table 1) in the PC2 package. No additional dongle is required for PC1 as the built-in Wi-Fi interface supports Wi-Fi operations in monitor mode. The Ubuntu terminal command to configure the Wi-Fi operation mode is listed in Table 2.

Step 2. Wi-Fi Channel Configuration. The specific channel in which the Wi-Fi interface operates must be configured so that Wireshark will capture only the packets transmitted on the specific channel. As described in 2.1 the Wi-Fi P2P connection operates on channel 1, 6 and 11. Therefore, we alternated the Wi-Fi interface on both PC1 and PC2 to operates on the three channels, one channel at a time for each test case. Refer Table 2 for the Ubuntu terminal command to configure the Wi-Fi channel. After the monitor mode and the channel has been configured, the Wireshark software was launched in both PCs.

Step 3. Wireshark Capture Filter. The capture filter parameter on the main page of Wireshark was set so that each PC was responsible to record the wireless frame related to a specific smartphone only. In our case, PC1 was configured to capture wireless frame belongs to Lenovo smartphone only and PC2 was configured to capture the wireless frame of Samsung smartphone only. The format of the capture filter has been listed in the third row of Table 2.

Table 2. Commands related to the initial setup.

Purpose	Configuration environment	Command
Configure Wi-Fi operation mode	Ubuntu terminal	*root@username: ~# iwconfig xxx* (interface name) *mode monitor*
Configure Wi-Fi channel	Ubuntu terminal	*root@username: ~# iwconfig xxx* (interface name) *channel n* (channel number)
Configure capture filter	Wireshark front page, with the specific Wi-Fi interface selected	*Capture filter: wlan host xx:xx:xx:xx:xx:xx* (mac address)

After the three initial configuration steps were performed, the "Start capturing packet" button has been clicked to start the capture process.

3.3 Test Cases

Two simple test cases were designed for Wi-Fi Direct connection testing. The two cases included enabling the Wi-Fi Direct feature and forming a connection between the two smartphones. The step by step procedures performed for each test case are listed in the following section.

Enable Wi-Fi Direct. This test case was designed to test the scanning and searching operations. After the initial configuration (explained in Sect. 3.2) steps were performed, begin the step:

i. Enable Wi-Fi interface for around 5 s.
ii. Enable Wi-Fi Direct feature for around 10 s.
iii. Disable the Wi-Fi interface to stop the Wi-Fi connection.
iv. Switch the Wi-Fi interface channel of both PC with the command listed in Table 2.
v. Repeat step 1 to 4 until all channel was switched.

The Connection Between the Two Smartphones. This test case was designed to test the GO Negotiation and WPS Provisioning operations. After the initial configuration (explained in Sect. 3.2) steps were performed, begin the step:

i. Enable the Wi-Fi Direct feature on both smartphones.
ii. Click P2P device found on the list for Samsung smartphone.

iii. Click accept invitation received on Lenovo smartphone.
iv. Disconnect after the P2P connection was established.
v. Disable the Wi-Fi interface to stop the Wi-Fi connection.
vi. Switch the Wi-Fi interface channel of both PC (command listed in Table 2)
vii. Repeat step 1 to 6 until all channel was switched.

4 Result and Discussion

The files captured by Wireshark are of the extension ".pcapng". Following the test cases listed in Sect. 3.3, there were a total of 12 PCAPNG files generated. The first 6 PCAPNG files were the Wi-Fi Direct activation session captured on every single channel (ch1,6,11) using both smartphones. The other 6 PCAPNG files were the Wi-Fi Direct P2P connection captured on the 3 channels by the 2 smartphones.

4.1 Wi-Fi Direct Activation Test Case Captured

Figure 5 depicts one of the Wireshark session captured on channel 1, with the capture filter fixed with Lenovo smartphone MAC address only. It was observed that when operating in P2P mode, a temporary SSID labeled as "*DIRECT-*" was generated. The display filter command "*wlan.ssid contains DIRECT*" was applied to the capture session to list only the Wi-Fi Direct frames. Figure 6 shows the result after the display filter was applied.

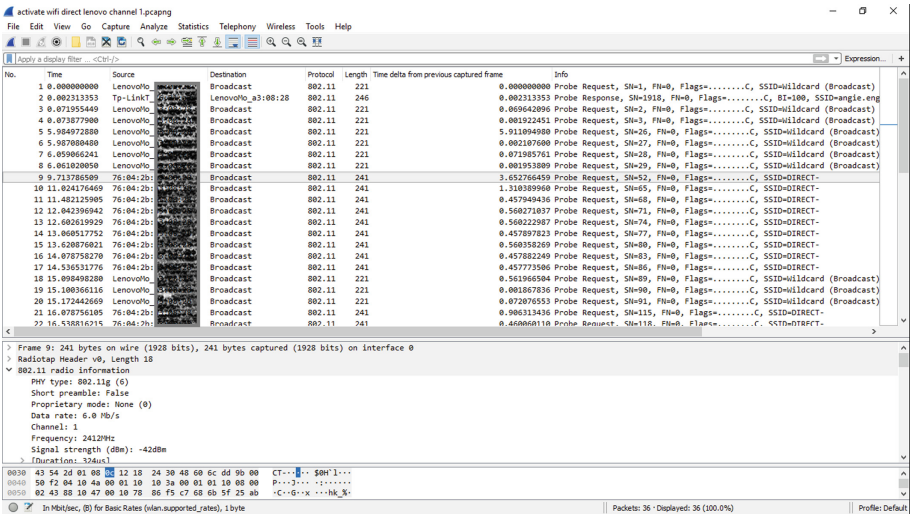


Fig. 5. Screenshot of Wireshark capturing wireless frame.

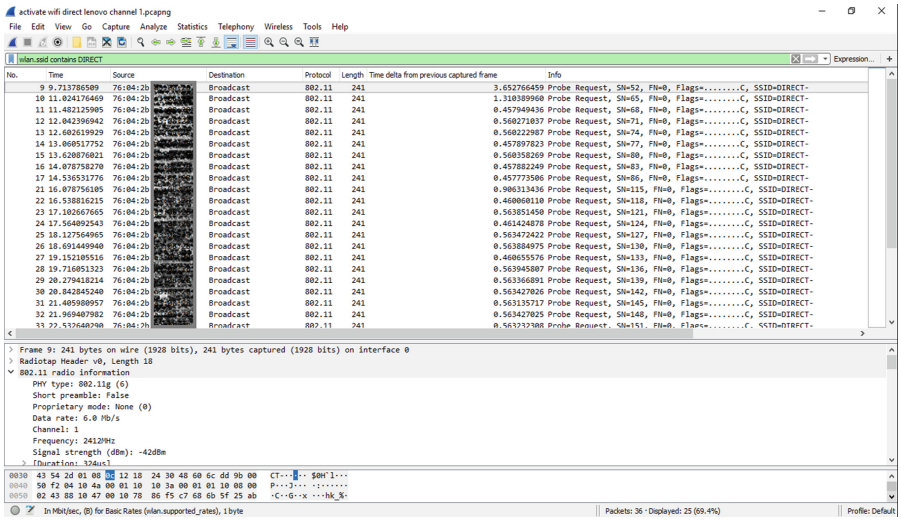
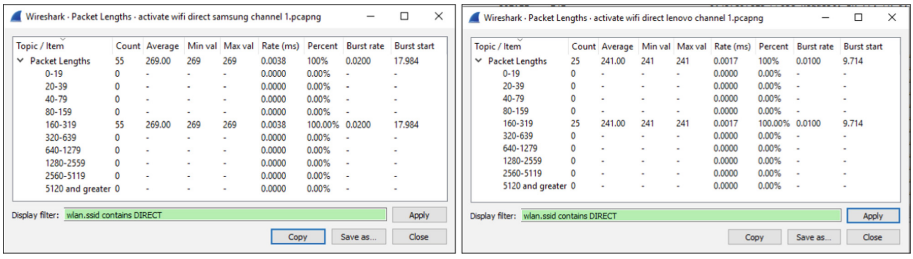


Fig. 6. Screenshot of Wireshark session captured with display filter applied.



a) Samsung b) Lenovo

Fig. 7. Summary of the packet length captured.

It is also observed that when the Wi-Fi Direct feature was activated, the smartphone started to broadcast a series of probe request with a serial number (SN) labeled. Figure 7 depicts the summary of the total packet captured. The screenshot on the left (a) shows that the probe request size generated by Samsung smartphone was 269 bytes. However, the size of the probe request recorded on Lenovo smartphone was 241 bytes. This shows that the probe request size is not fixed and device-dependent.

4.2 Wi-Fi Direct P2P Connection

Figure 8 depicts one of the Wireshark session captured on channel 1 when forming the P2P connection. The capture filter was to capture frames related to Samsung smartphone MAC address only. It is observed that when the P2P GO was identified; the GO will form a new SSID based on the device name (e.g. DIRECT-kF-Galaxy J1 mini

prime). After the new SSID was formed, the GO will continuously broadcast the beacon frame so that the other mobile devices can discover the new SSID.

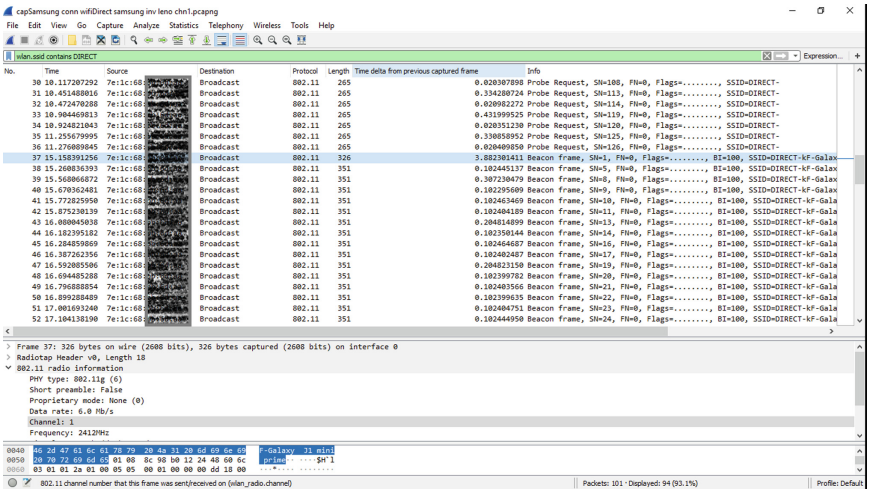


Fig. 8. Screenshot of Wireshark session captured during the P2P connection process.

Figure 9 depicts the summary of the frames transmitted between two smartphones (or known as a conversation between smartphones). When Wi-Fi Direct was activated, the smartphones created a new virtual MAC for the P2P activity. This can be seen in Fig. 9 under the column "Address A", the original MAC address started with "74" and the new MAC address started with "76". A total of 32 frames transmission were recorded between the two smartphones during the P2P group formation and connection.

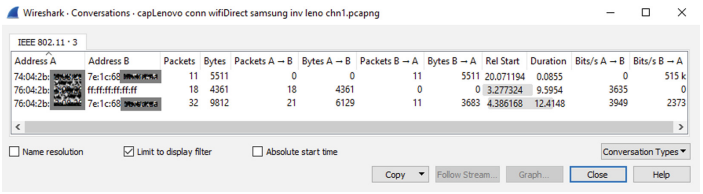


Fig. 9. Summary of the frames transmitted between two smartphones.

5 Conclusion

In this paper, we compared the theoretical and practical group formation operations of the Wi-Fi Direct standard. For the theoretical operations, we presented an overview of the Wi-Fi Direct standard based on the technical documents. Next, we had set up an

experimental platform and designed 2 simple test cases for testing. Two smartphones were used for the P2P connection testing and 2 laptops were used as the station to record the frame transmission process. The recording was done using Wireshark Analyzer. When the Wi-Fi Direct was activated, a temporary SSID "DIRECT-" was generated. A new virtual MAC address was issued to the Wi-Fi interface for the Wi-Fi Direct operations. The size of the probe request or response frame is not fixed, and it is device-dependent. The details flow of frames between smartphones are difficult to visualize as the frame was recorded in bundle and we can't rule out the possibility where some frames were dropped or not captured by the Analyzer. However, the pattern of the formation and frame details have been visualized using the analysis tools available in Wireshark Analyzer. The experimental environment has been set up in an ideal and static condition. There are times where Wi-Fi Direct has stopped functioning and the connection cannot be formed. The smartphones were placed on a fixed location which might not reflect the mobility nature of a smartphone. For future work, more devices can be added to collect more sampling data for comparisons. In addition, a better experimental approach could be developed to review the connection between mobilized smartphones.

References

1. Cisco: Cisco Visual Networking Index (VNI) Global Mobile Data Traffic Forecast Update, 2017–2022 (2019)
2. Jiang, D., Liu, G.: An overview of 5g requirements. In: Xiang, W., Zheng, K., Shen, X. (eds.) 5G Mobile Communications, pp. 3–26. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-34208-5_1
3. Lee, T.S., Sulaiman, R.: Preliminary analysis of wireless collaborative network on mobile devices. J. Inf. Commun. Technol. **18**(3), 327–343 (2019)
4. Woolley, M., Schmidt, S.: Bluetooth 5 go faster. Go further (2016)
5. IEEE: 802.11aq-2018 - IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area network–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Spe. IEEE (2018)
6. Lee, T.S., Sulaiman, R., Ali, N.M.: A peer to peer internet sharing technique on MANET through Wi-Fi interface. In: 4th Visual Informatics International Seminar (VIIS 2018), pp. 1–12 (2018)
7. Shah, N., Abid, S.A., Qian, D., Mehmood, W.: A survey of P2P content sharing in MANETs. Comput. Electr. Eng. **57**, 55–68 (2017)
8. Holst, A.: Global smartphone sales to end users from 1st quarter 2009 to 2nd quarter 2018, by Operating System. Statista.com (2019). https://www.statista.com/statistics/266219/global-smartphone-sales-since-1st-quarter-2009-by-operating-system/. Accessed 01 July 2019
9. Wi-Fi Alliance: Wi-Fi Peer-to-Peer (P2P) Technical Specification Version 1.7, Wi-Fi Alliance, P2P Technical Group (2016)
10. Tumusok, J.P., Newth, J.D.: Wi-Fi signal strength: what is a good signal and how do you measure it. EyeSaaS.com (2018). https://eyesaas.com/wi-fi-signal-strength/. Accessed 01 July 2019