Chapter 2
A Measurement Study of Campus WiFi Networks Using WiFiTracer

Chengwei Zhang, Xiaojun Hei, and Brahim Bensaou

Abstract Highly dense and large-scale WiFi networks have been widely deployed in public areas to provide cost-effective high-speed wireless Internet access for mobile end users. This emerging practice has been leading to a severe spectrum usage overlap and channel interference between colocated WiFi networks. To understand the characteristics of highly dense WiFi networks, we conduct a measurement study of campus WiFi networks in this chapter. First, we instrument an Android App to sense WiFi access points (APs) to characterize WiFi networks in campus areas, including WiFi spectrum and channel usage, AP density, network distribution, and so on. Our measurement results demonstrate that a large number of WiFi APs have been widely deployed on campus, and about 80% of the total APs occupy the 2.4 GHz band, whereas the remainder part are the higher frequency 5 GHz APs, commonly used by public WiFi networks. The spectrum overlap and channel interference in the 2.4 GHz band is much more severe than that in the 5 GHz band. Then, extra WiFi connection measurements are conducted at selected areas with well-deployed campus WiFi networks, to understand WiFi connection characteristics while pedestrians are moving around in the coverage of the WiFi networks. By harvesting data from voluntary Android smart phone users, the connection setup time composed of Authentication–Association (AA) time, handshake time, and IP acquisition time is found to be generally affected by various factors, such as AP density, RSSI levels, etc. To achieve load balancing with reduced interference and higher WiFi network performance, this field measurement study may provide guidelines to design the next generation software-defined WiFi networks.

C. Zhang · X. Hei (✉)
Huazhong University of Science and Technology, Wuhan, China
e-mail: heixj@hust.edu.cn

B. Bensaou
The Hong Kong University of Science and Technology, Kowloon, Hong Kong, China

S. Guo, D. Zeng (eds.), *Cyber-Physical Systems: Architecture, Security and Application*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-92564-6_2

2.1 Introduction

WiFi networks have been providing a cost-effective high-speed wireless network access in the past decades. WiFi-based wireless local area networks are widely deployed on Edges of Internet for convenient user access due to the following three benefits: (1) simple technical implementation, (2) low-cost network construction, and (3) high-bandwidth wireless links [1]. Although only a limited number of user clients are supported by a single access point (AP) for the WiFi original design, WiFi network with multiple APs, such as a hotzone [2], has been increasing for supporting Internet access with a large number of clients in a relative large area [3, 4]. WiFi networks serving as the major network components have been envisioned for constructing smart city and even smart country [5].

The communication and entertainment paradigm in people's daily life has been gradually reshaped by the rapid penetration of smart phones. A variety of micro sensors have been integrated in modern smartphones, including accelerometers, gyroscopes, magnetometers, light sensors, global navigation satellite system (GNSS) as well as Bluetooth and WiFi transceiver modules [6, 7], which can cooperate with monitoring, positioning, and navigating applications. Due to the pervasive usage of smart phones, together with the cooperative sensing capability and users' mobility, smart phones have been evolving from ordinary mobile devices into measurement enablers [8, 9]. Users can carry smartphones around during their daily lives for measuring, collecting, and preprocessing data of user activities with powerful sensor and microprocessors embedded in smartphones. Recently, various research projects and applications deeply relying on smartphones and user mobilities have emerged for different purposes, such as smartphone-based indoor position system [10], recording physiological indexes of mobile users [11], monitoring user behavior [12], tracking the air quality of the urban environment [13], and so on. Mobile measurement applications running on smartphones carried by a large number of users, which can perform measurements individually and conduct analysis collaboratively, from the mobile crowd sensing (MCS) measurement [14, 15]. The MCS can fully exploit the limited resources of individual smart phones, and conveniently deploy real and randomized measurement experiments rather than well-planned experiments in a large scale [14, 15]. Lane et al. [16] and Xiao et al. [17] studied the data transmission efficiency and energy consumption problem of MCS. In particular, recent measurements [18, 19] have shown that significant energy has been consumed by wireless transceiver modules (WiFi and 3G/4G) of mobile devices during data transmission. These field measurement studies have greatly pushed forward the innovation of mobile cloud transmission systems [20, 21] to shift the heavy energy-hungry services for mobile Apps to the remote clouds, instead of local mobile devices.

In this chapter, we are motivated to conduct a measurement study to characterize the spectrum interference and the connection bottleneck on campus WiFi networks using a MCS approach. We developed a MCS platform for tracking the channel usage and connection bottleneck of campus WiFi APs. An augmented Android

measurement tool, named WiFiTracer, can automatically probe, maintain, and upload detected WiFi APs' information through smart phones from volunteers. For the large-scale WiFi measurement construction, student participants as anonymous users have been invited to perform random movement in various ways (driving, jogging, and walking) on the campus with the measurement APP running on smartphones for abundant measurement data collection. During this crowd sensing measurement process, we conducted various experiments to quantify the connection time for a public campus WLAN. The major results from these experiments are summarized as follows:

1. We first summerized the WiFi dataset on our campus area. Our results show that there are considerable and high-density WiFi APs maintained on the campus area. Over 10,000 WiFi APs and more than 7000 distinct WiFi networks have been detected.
2. We characterized a public campus WiFi network quantitatively. Our results show that more than 70% measurement areas have been covered by this public campus WiFi WLAN. We quantified the interference of this public campus WLAN with its nearby private WiFi networks. Extra experiments were conducted to compare campus WiFi networks deployed indoors and outdoors. Measurement results also show that the dynamic frequency selection (DFS) feature of WiFi APs is not enabled in the general circumstance.
3. We conducted the WiFi connection setup time on the public campus WiFi networks during the MCS measurement process. The connection setup time deviates significantly on the different mobile devices, ranging from the tens of milliseconds to tens of seconds.

In this chapter, we first introduce the concept of MCS and recent research progress. Then, we propose and implement a crowd sensing measurement platform. Next, we dissect the WiFi connection setup process for public WiFi networks. Afterwards, we report our measurement results mainly on two aspects: channel interference and connection time. Finally, we conclude this chapter. The measurement results demonstrate the necessity of a configurable and manageable software-defined WiFi network that can dynamically adjust WiFi channels based on the current network states to achieve load balancing with reduced interference and improved WiFi network performance.

2.2 WiFi Measurement Platform

Public campus WiFi networks are widely deployed at public locations through the campus; for understanding the characteristics of WiFi networks, like channel usage, AP density, connection time, etc., we are motivated to propose a general WiFi sensing measurement framework using the MCS way as shown in Fig. 2.1 to provision the data transmission and sharing of measurement results. The measurement platform can conveniently cooperate with particular WiFi measurement modules to inspect various metrics of WiFi networks.

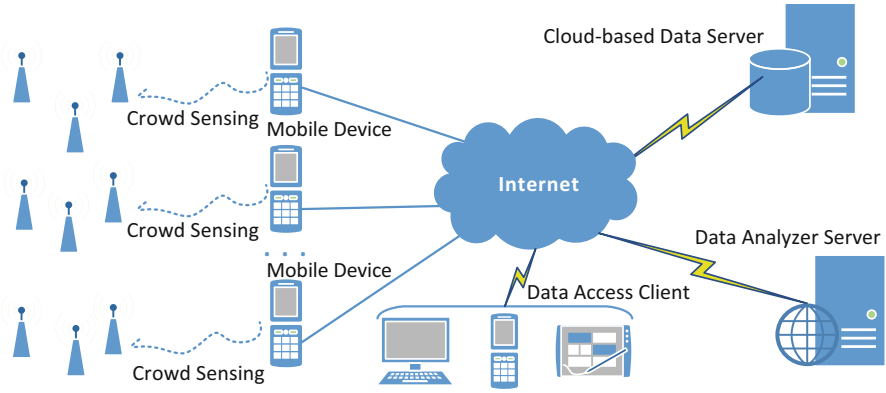


Fig. 2.1 WiFi measurement architecture using mobile crowd sensing (MCS)

2.2.1 Measurement Framework Overview

The proposed MCS platform, consisting of three major modules including data acquisition, collection, and analysis, is constructed in Fig. 2.1. Smartphones equipped with WiFiTracer can successfully turn these typical mobile devices into WiFi measurement tools for the nearby WiFi information harvest and preprocessing. WiFi measurement data has been collected and formatted locally on mobile devices by data acquisition module. Preprocessed data from varied mobile devices will be collected and analyzed as a repository hosted on a cloud platform by the data collection module. When the volunteers complete the measurements, Android app or service running on the framework will automatically upload the local results to the server with timestamps and user tags. The reward module is used to share the available WiFi information as an incentive for participants. The server provides information about available WiFi networks close to the end users and the possible WiFi network access at the current location, which can be displayed to users through web pages or the client app. Increasing individual users are willing to contribute the measured data and acquire better network connection performance potentially based on the incentive crowd sensing way.

2.2.2 WiFiTracer Architecture

WiFiTracer is an Android mobile app which can run on different Android smartphones to explore and aggregate the WiFi network information from the WiFi client side. Its software architecture is constructed with four major layers as shown in Fig. 2.2, including application interface, task module, system libraries, and Android system control. Each layer implements the individual function and works collaboratively to transform a normal mobile phone into a general portable measurement device.

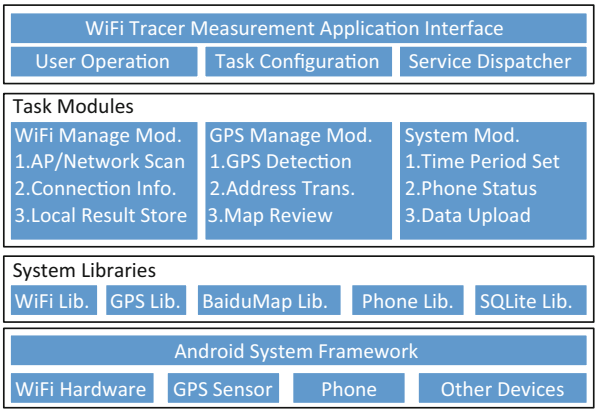


Fig. 2.2 The software architecture of WiFiTracer

- **Android system control layer:** It provides the necessary physical device drivers and interfaces for the Android applications and services. Through this layer, the high-level applications can apply a general unified way to access and manage various sensors, such as WiFi transceiver, GPS sensor, and so on.
- **System library layer:** The system dependence libraries, including WiFi Lib., GPS Lib. et al., extend the management for the Android resources. Those third-party libraries can provide additional functions and data sources than those generic ones. The BaiduMap library, as an extra map provider library, offers more accurate GPS location service and various data visualization methods on the map.
- **Task module layer:** This layer, designed as the main module of WiFiTracer, consists of three individual components: (1) WiFi management module, (2) GPS management module, and (3) application configuration module. The WiFi and GPS management components are used to access the corresponding drivers and obtain the raw measurement results from the low-level Android devices, such as WiFi basic information and GPS raw data. The configuration component offers a flexible interface for higher layers and supports multidimensional measurement tasks of WiFiTracer.
- **User interface layer:** This layer provides a friendly operation graphic interface for end users. A user can configure parameters of the tool, schedule tasks, and manage low-level sensors of the tool.

2.2.2.1 Measurement Sample

WiFi APs may be sensed repeatedly for multiple times during the measurement process; therefore, the same WiFi APs may be tagged with different timestamps and locations during measurement. For the purpose of describing the measurement

results conveniently, a measurement sample by a single smartphone can be summarized as follows:

$$o^i_{bssid} = \{timestamp(ts), round, bssid, ssid, channel, rssi, capabilities, gps\}. \tag{2.1}$$

o^i_{bssid} represents the measurement data of WiFi AP which appears for the i-th time. During each sensing round, ts, $round$ and gps represent the general round information of WiFi measurement, where ts represents the accurate sensing time on the smartphone, $round$ records the time number of measurement, and gps stores the current measurement location. Each WiFi AP's basic information, including BSSID (as $bssid$), SSID (as $ssid$), the channel frequency (as $channel$), the signal strength RSSI (as $rssi$), and the security mechanism (as $capabilities$), once sensed during the measurement process, will be obtained and merged with the general round information to formulate a unique and complete measurement sample set o^i_{bssid}. Therefore, the whole dataset of WiFi APs' bssid is detected on MCS measurement process as S; the results of the same WiFi APs (using $bssid$ as the identifier) compose independent result set O_{bssid}:

$$O_{bssid} = \{o^i_{bssid}, i \in [1, +\infty], bssid \subseteq S\}. \tag{2.2}$$

MCS allows using different devices to harvest WiFi network information. The measurement result sets of different devices can be expressed in Eq. (2.3). The results of each device can be formed as an independent measurement result set which can be identified by the unique device ID. The measurement data collected by WiFiTracer are uploaded to the remote server through the Internet and then are analyzed afterwards.

$$OD_{device} = \{\{id, deviceid, O_{bssid_i}\}, i \in [1, +\infty], bssid_i \subseteq S\}. \tag{2.3}$$

2.2.3 Measurement Sampling Procedure

With the supplement of the MCS mechanism, WiFiTracer can cooperate with various Android mobile devices for WiFi measurement. The tool implements an optimized scanning procedure as shown in Algorithm 1, which can significantly improve the efficiency and accuracy of measurements and avoid unnecessary multiple sensing rounds on the same locations.

WiFiTracer tracks the dynamics of WiFi APs periodically (such as 10 s) while the user is in moving states. During the WiFi measurement process, WiFiTracer obtains and computes the distances between the current measurement location and the previous measurement location. Once the computed distance is larger than a threshold (10 m as default), the tool will activate the scanning process to detect the nearby WiFi APs tagged with timestamps and GPS coordinates to form the measurement metadata. Results are then stored locally in the Android SQLite database, and will be uploaded in the cloud repository for further analysis.

Initialization: Smartphone, WiFi transceiver, and GPS sensor initialized ;
Data: $deviceinfo \leftarrow$ deviceinformation, $origpos \leftarrow$ currentGPSposition,
Data: $period \leftarrow$ userconfiguration, default : 10s,
Data: $mindistance \leftarrow$ userconfiguration, default : 10m ;
Result: WiFi measurement dataset on variant mobile devices: $O_{deviceid}$;
while *scanning service is not stopped* **do**
  if $scanperoid = peroid$ **then**
    $currentpos \leftarrow$ currentGPSposition ;
    if $distance(origpos, currentpos) > mindistance$ **then**
      activate the WiFi scanning process; scan the WiFi APs nearby ;
      $scantime \leftarrow$ currenttimestamp, $scancount \leftarrow$ currentscancounter ;
      record $scanresult : (bssid, ssid, frequency, rssi, capabilities)$;
      build entity: $o^i_{bssid} : (scantime, scancount, deviceinfo, scanresult, currpos)$;
      store the dataset O and upload to the remote server ;
      terminate the current service ;
    else
      exit the current service, start a new round timer for scanning ;
      continue ;

    $origpos \leftarrow currpos, scancount = scancount + 1$;
    start a new round timer for scanning ;
    continue ;
  end
end
User terminates the application, and stop all the functions.

Algorithm 1: Sketch of the WiFiTracer sensing procedure

2.3 Sensing Result Analysis

MCS supports various mobile devices in collaborative measurement and each mobile device becomes a distinct end-point measurement tool. The measurement device cooperating with user's mobility translates the whole experiment to a randomized distributive measurement process, and the data storage and computation on the cloud offers convenient data sharing and analysis among all measurement clients. The main campus of our university has been chosen as the main experiment area to launch the WiFi measurement. Well-performed Android smartphones, such as HUAWEI Honor7, ZTE Nubia Z7, etc., have been carefully selected as measurement devices to operate WiFiTracer tool, and all devices can perform smoothly on WiFi standard frequencies in both 2.4 and 5 GHz bands for WiFi standard protocols such as 802.11 a/b/g/n. Participants as anonymous users have been invited to perform random movement in various ways (driving, jogging and walking) on the campus with the measurement APP running on smartphones for abundant measurement data collection.

Participants were requested to perform randomized movement on the main roads with a relative low speed ($\leq$20 km/h) during each measurement process and almost took 1.5–2 h to traverse the whole campus measurement areas. In order to cover the whole measurement areas with sufficient and accurate WiFi metadata, the entire measurement experiments have been lasted for around 30 days and the total measurement time is up to almost 100 h. Due to different WiFi networks have variant radiation coverages, the proposed experiments assumed that most of indoor WiFi APs and networks were visible on the main roads and could be obtained by the WiFiTracer.

Table 2.1 Measurement dataset

Metric	Amount
Scan times	20,210
Data samples	534,210
Independent areas by GPS	13,065
Number of distinct WiFi APs	11,380
Number of distinct WiFi networks	7483
Number of 2.4 GHz APs	10,390
Number of 5 GHz APs	1988
Number of public WiFi APs	2893

2.3.1 Basic WiFi Dataset

By Eq. (2.2), each WiFi AP detected by smartphone applications can be presented as an independent measuring result set which records the location information and current signal strength (RSSI). The values of WiFi's RSSI have a variance relation to the distance from the measurement node to the AP [22], which implies that a smaller distance leads to a stronger signal. It is possible that we can choose the APs' results with the maximized RSSI value and utilize the GPS information to estimate the real AP locations.

The distribution of WiFi APs is primarily on roads or near roads because the measurements were conducted along the main roads of the campus covered by WiFi APs with intensive quantities. Table 2.1 shows the WiFi sensing measurement dataset that over 10,000 independent WiFi APs have been successfully sensed and most of them are private. Private WiFi networks constructed by independent APs can provide small range network access with passwords or other authentications. With dense deployment of WiFi networks, it has become an emerging problem for WiFi networks to reduce the spectrum interference from other WiFi APs.

2.3.2 General Analysis of WiFi Networks

2.3.2.1 Heatmap of WiFi APs' Distribution

Figure 2.3 shows the heatmap of the WiFi APs distribution, where red areas suggest high density of WiFi APs deployed. Demonstrate that there is a strong correlation between the high-density WiFi networks. The circled areas $1 \sim 6$ are official areas, teaching areas, and living areas where people spend most of daily time. Covered with orange colors are focused on crossroads or intersections of roads. One reason is that the intersections are the connections of different roads which potentially have more chances to measure than normal areas during the random movement under crowd sensing measurements; the other one is that WiFi APs usually are deployed with buildings. Hence, Fig. 2.3 indicates the WiFi density near intersections heavier than normal areas.

Fig. 2.3 WiFi AP heatmap

2.3.2.2 WiFi Channel Usage

Densely deployed WiFi APs would potentially result in severe spectrum interferences in WiFi channels. Figure 2.4 depicts channel usages of WiFi networks for both 2.4 GHz band and 5 GHz band. Results demonstrate that 2.4 GHz band is the main working band occupied almost 80% in the sensing dataset while 5 GHz band only accounts for 20%. Private WiFi networks seldom work on 5 GHz band, and over 95% 5 GHz APs are used for public WiFi networks. IEEE WiFi standard organization encourages more than 15 channels in 5 GHz band for high-speed WiFi networks, whereas part of them are allowed to use in different countries, such as only channels 149–151, 161, and 165 are permitted as legitimate channels in China.

Figure 2.4 shows various channel usages in percentages. Results demonstrate that channels 1, 6, and 11 in 2.4 GHz are the most popularly used channels among all channels. The reasonable explanation is that WiFi manufactures usually set the 2.4 GHz WiFi appliances default in these independent channels to avoid the adjacent channel interference in practical applications. However, even these three channels are completely independent of each other in the spectrum, and due to the fact that WiFi users rarely change these default channel settings, the overuse of these channels would greatly increase the co-channel overlaps and interferences. On the contrary, channels in 5 GHz are completed isolated from each other and result none of adjacent channel interferences.

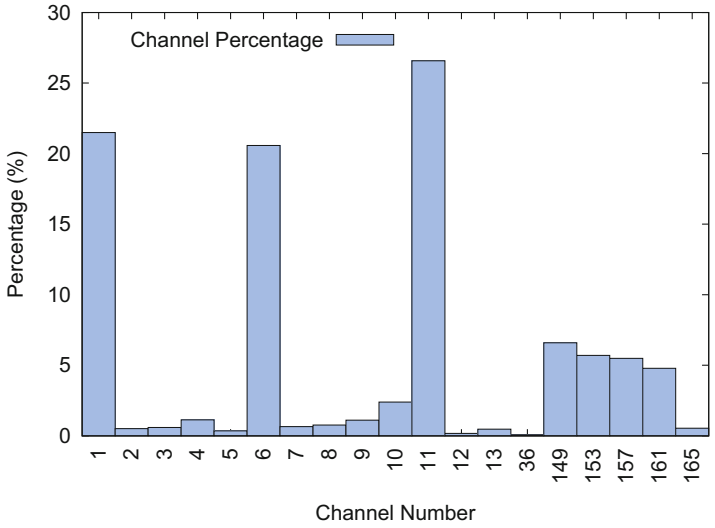


Fig. 2.4 WiFi channel utilization

2.3.2.3 WiFi AP Hardware Legality

Variant WiFi devices have been widely put into commercial use for the simplicity and convenience of WiFi network. Figure 2.5 presents top 10 WiFi manufacturers used in measurement areas. Wireless devices made by TP-Link dominates over 20%, for their high price–quality ratio of small home routers. Over 35% WiFi devices marked with "Unknown" cannot find the corresponding manufactures through the registered manufacturer information provided by IEEE Standard Association (ISA) [23]. Two reasons can explain why there are so many "Unknown" devices. One is that the manufacturer list is not updated in time by ISA; the other is that some factories do not register in ISA at all and produce WiFi devices illegally and privately.

Table 2.2 shows channel usages of "Unknown" WiFi devices, where the percentage of channel 11 is nearly double of channels 1 and 6. Therefore, it can be inferred that these anonymous manufactures choose the highest channel 11 in 2.4 GHz to avoid the interferences with other commercial products' channels. However, joint consideration with Fig. 2.4, channel 11 has the highest utilization among all the channels for its overuse by a large quantity of "Unknown" WiFi devices, which could potentially result much severer co-channel interference than others.

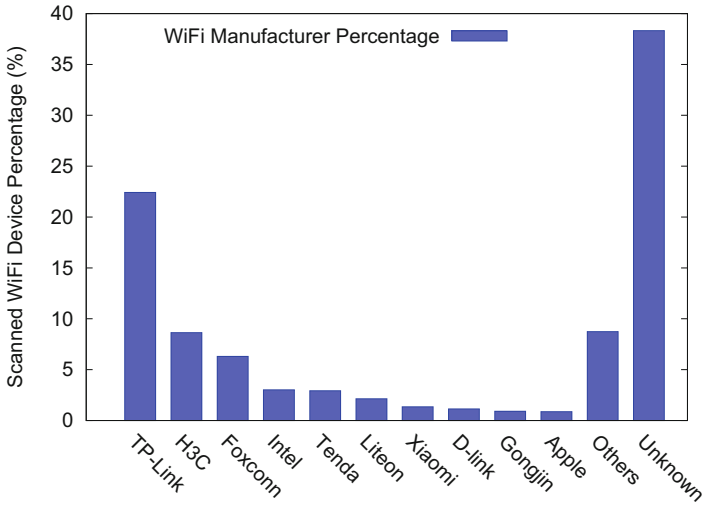


Fig. 2.5 WiFi device usage of different manufacturers

Table 2.2 Channel usage of "Unknown" WiFi devices

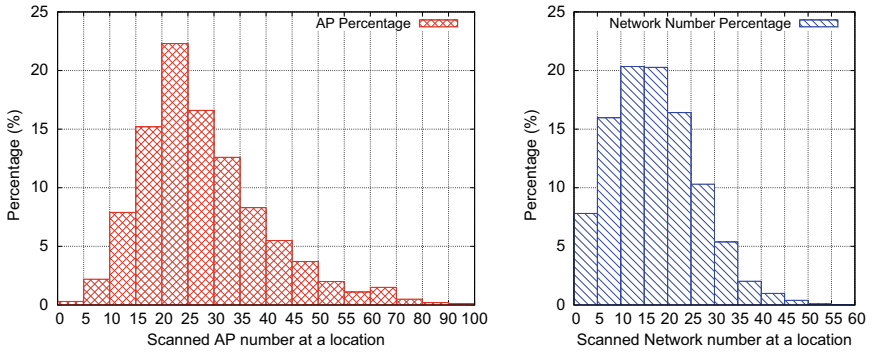
Channel	Number	PCT.(%)
1	958	24.0
6	983	24.7
11	1912	48.0
Others	130	3.3

2.3.2.4 Density of WiFi APs and Networks

AP densities at distinct measurement locations are shown in Fig. 2.6. Results in Fig. 2.6a indicate that over 15 individual WiFi APs have been detected in almost 90% measurement areas and over 100 independent APs have been scanned in some extremely high-density areas. Under the Extended Service Set(ESS) model, independent APs may construct a wide-range WiFi network with the same identified network name. Therefore, densities of WiFi networks would exhibit different characteristics from densities of WiFi APs in the same areas. Figure 2.6b demonstrates independent WiFi networks at various measurement locations with percentages. Over 10 independent WiFi networks have been detected in about 80% measurement areas. Results from densities of WiFi APs and networks illustrate the approximation to the normal distributions.

2.3.2.5 Utilization in 5 GHz Band

Figure 2.4 illustrates that WiFi channel utilization meets the 80/20 rule, 80% for 2.4 GHz band and 20% for 5 GHz band. Table 2.3 shows that only 5% of 5 GHz



(a) (b)

Fig. 2.6 Density of WiFi APs and distinct networks. (**a**) Density statistics of WiFi APs. (**b**) Density statistics of WiFi networks

Table 2.3 Usage of 5 GHz WiFi APs

Type	Private APs	Public APs	Total
Number	100	1888	1988
PCT.(%)	5	95	100

APs are used to construct private WiFi networks, even they have better performance and less interferences than 2.4 GHz APs; whereas 95% ones are used by public WiFi networks for high quality access.

2.3.3 Characterizing Public Campus WiFi Networks

Through the enhanced scanning measurements for public WiFi networks, more than 7000 distinct public campus WiFi APs have been successfully scanned and recorded. Considering the maximum signal strength (RSSI) received at GPS locations, distributions and coexistent characteristics between public and private WiFi networks can be merged on the real areas by heatmaps, measurement results depicted in Fig. 2.7 show that public networks and private networks appear to be complementary.

2.3.3.1 Indoor vs. Outdoor Channel Usage

Figure 2.8 shows the usage of channels in campus (outdoor/indoor) WiFi networks differentiate distinctly from private networks. The numbers of the occupied 2.4 GHz and 5 GHz bands are similar and the channel bands are distributed evenly except that channel 165 has fewer WiFi APs. We infer that public WiFi networks adopted the balanced AP deployment strategy to make frequency bands evenly distributed

Fig. 2.7 Spatial spread density statistics of WiFi networks. (**a**) Density of public WiFi. (**b**) Density of private WiFi

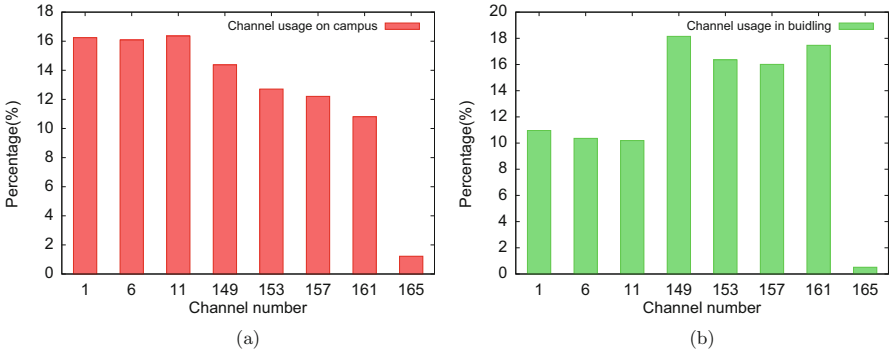


Fig. 2.8 Channel spatial distribution of campus WiFi channels. (**a**) Channel usage (outdoors). (**b**) Channel usage (indoors)

and reduce co-channel interference in the same network. In the 2.4 GHz band, public WiFi APs commonly select channels 1, 6, and 11 which are completely independent from each other and the other channels are not occupied to avoid the adjacent channel interferences within WiFi networks. However, in the 5 GHz band, the uniform deployment appears to be enabled without considering the adjacent channel interference. Considering the coverage and penetrability of 5 GHz WiFi networks, the proportion of 5 GHz WiFi APs is lower than the outdoor 2.4 GHz WiFi APs while the proportion of 5 GHz WiFi APs is higher than the indoor 2.4 GHz APs for providing higher access rate and better access quality.

Figure 2.9 shows RSSI CDFs of public campus WLAN under the indoor and outdoor environments. Figure 2.9a shows the RSSI CDF from every measurement record and results have obviously shown that the indoor signal strength is stronger than outdoors. Due to certain coverage of WiFi APs, a WiFi AP RSSI information can be measured frequently in the coverage areas. To make a deeper comparison, we refined the maximal RSSI from the observation set OD; results shown in Fig. 2.9b

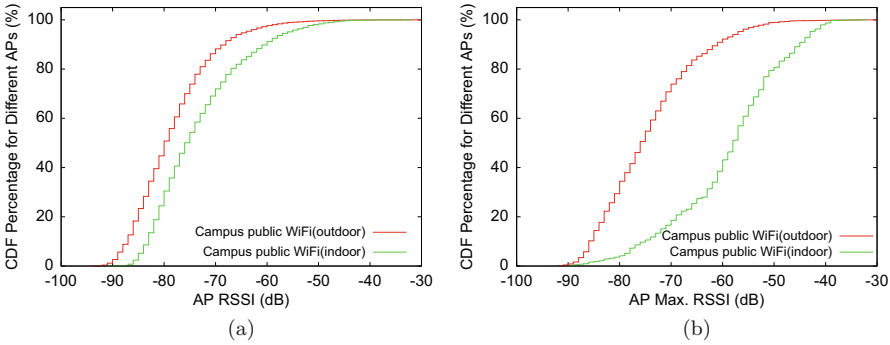


Fig. 2.9 RSSI comparison of indoor and outdoor APs. (**a**) All RSSI. (**b**) Max. RSSI

also present that the indoor AP RSSI is much greater than outdoors. Hence, results prove that deployments of most WLAN APs are dependent on the buildings. Current mobile devices choose WiFi APs mainly relied on the current AP RSSI, so we can infer from the measurement that it is much easier to obtain access to available WiFi APs indoors rather than outdoors, and we also can infer that interferences indoors are more serious than outdoors.

2.3.3.2 Indoor vs. Outdoor Interference of Public WiFi Networks

For more insights of WiFi networks, extra measurement experiments were also conducted indoors. Figure 2.10 presents the comparison of WiFi AP density results between the outdoors and the indoors. As shown in Fig. 2.10a, over 60% outdoor areas are covered with public WiFi APs ranged from 20 to 60, and nearly 20% areas are covered with over 60 ones. The adjacent channel interference among WiFi networks is shown in Fig. 2.10a by public WiFi network density with the green curve. As the previous analysis in Sect. 2.3.2.2, the default frequencies of most WiFi APs usually are configured on three independent channels (1, 6, and 11) in 2.4 GHz instead of other channels. Therefore, further public WiFi APs in the same areas would potentially generate additional co-channel interferences as shown in Fig. 2.10a with the red curve.

Figure 2.10b shows that 60% indoor areas are covered with public WiFi APs ranging from 40 to 100, which is doubled with the outdoor result. The extreme AP density at several indoor locations is over 200. Therefore, more serious co-channel interference has been discovered indoors through the comparison of Fig. 2.10. Figure 2.10 shows that public campus WiFi networks suffer the co-channel interferences from themselves rather than external private WiFi networks.

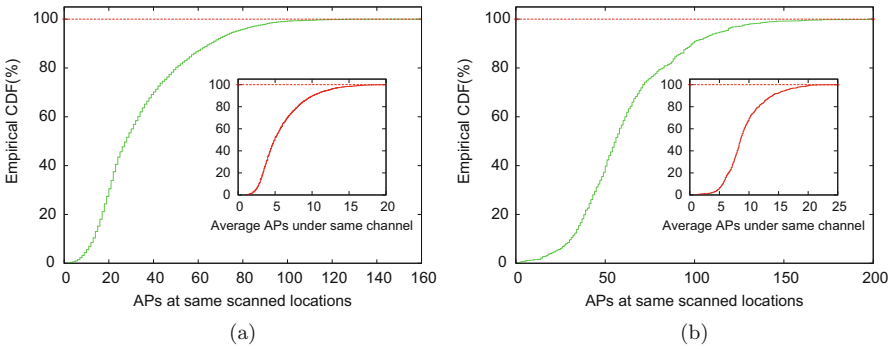


Fig. 2.10 CDF of public campus WLAN density. (**a**) WiFi AP density CDF (outdoors). (**b**) WiFi AP density CDF (indoors)

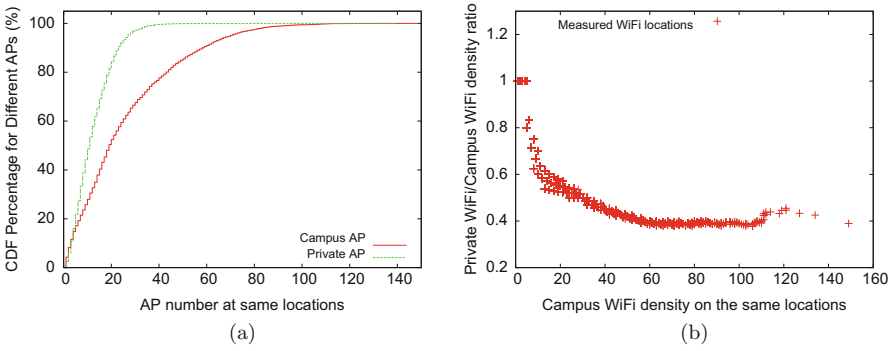


Fig. 2.11 Public campus WLAN vs private WLAN. (**a**) CDF of private and public APs. (**b**) Density ratio of private/public APs

2.3.3.3 Interference of Hybrid WiFi Networks

Figure 2.11 presents a comparison of densities between public networks and private networks in measurement areas, where public and private networks construct hybrid WiFi networks. Figure 2.11a shows that public campus WiFi density is higher than private WiFi density on the average and 80% measurement areas are covered with less than 20 private APs. Compared between the private and public WiFi APs, densities of the public WiFi networks are almost doubled in the same locations. It can be inferred from results that public WiFi networks are not only affected from external private networks but also from the internal networks themselves.

To differentiate the network interference of hybrid network in various areas, we defined the **Relative Density Ratio** as private AP's density divided by public AP's density at a measurement location for further analysis. The defined ratios with public WiFi APs in the hybrid network areas is shown in Fig. 2.11b. Results indicate

that about 90% measurement areas obtain the ratio value smaller than 1, which implies that the density of public APs is higher than the number of private APs at the same locations. Results demonstrate that public campus WiFi networks suffer from the potential interferences not only from those private networks but also from themselves due to their high-density deployments.

2.3.3.4 Dynamic Frequency Selection Detection

To reduce the impact of spectrum interference, WiFi APs may adopt the DFS feature which can dynamically adjust the WiFi transmitting frequency based on the channel utilization of the WiFi APs in the neighborhood to avoid the busy channels and select the appropriate working channel. As shown in Fig. 2.12, we tracked the number of channels utilized by the same AP in our dataset. The results show that WiFi APs enabling DFS account for only 20% over all the measured dataset and about 80% percentage of WiFi APs do not change channel numbers at all. There might be two reasons for this observation: one is that these devices may not support DFS; the other one is that many users enable the DFS without configuring the WiFi devices appropriately so that AP devices stay with the default factory settings.

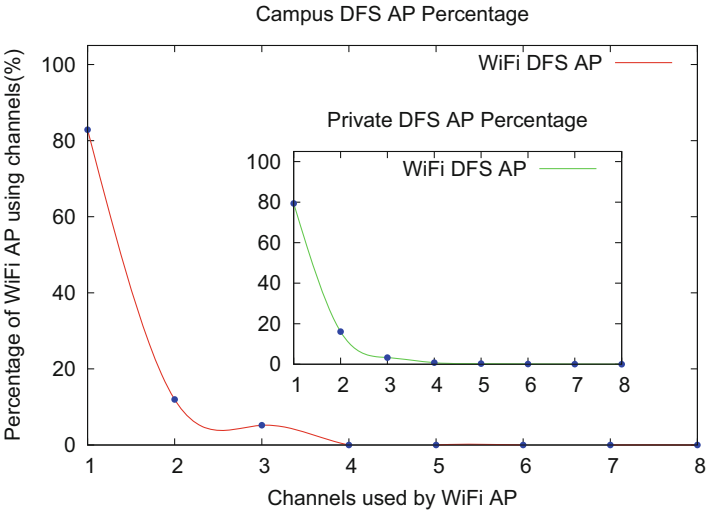


Fig. 2.12 Dynamic frequency selection (DFS) technology used in WiFi APs

2.4 Characterization of WiFi Connection Time

During the WiFi sensing measurement process, the WiFi connection monitor module will cooperate with WiFiTracer to record the overall connection process when the public campus WiFi networks are available to use. Sensing results in Fig. 2.7 strongly recommend us that the connection measurement experiments should be conducted in the following distinct areas, such as 1–3 areas on the map shown in Fig. 2.7a, where public campus WiFi networks have been densely deployed.

2.4.1 WiFi Connection Dataset

Based on results analyzed from the WiFi sensing dataset, the measurement areas can be determined for conducting the connection measurement experiments. Students invited as participants are required to load the connection monitor module in WiFiTracer and to move around in measurement areas during their daily lives. By over 2 months' measurement, a WiFi connection dataset has been successfully collected for various data of connection procedures, discussed previously in Sect. 2.2.

Table 2.4 presents a data summary of connection experiments conducted in chosen areas covered with well-deployed public campus WiFi networks. Over 70,000 times of connection attempts have been successfully observed from the measurement dataset, and only about 10% attempts have achieved the complete connection procedure and smoothly set up the data communication link between WiFi APs and clients. The dataset not only records the connection measurement results of public campus WiFi networks but also contains private WiFi networks' connection information for daily usages of participants.

From statistics in Table 2.4, the number of WiFi BSSIDs is much larger than WiFi SSIDs, which can be inferred that actual public WiFi networks extend the network coverage with multiple APs under the same SSID (recognizable network name) by WiFi ESS (extended service set) technique. Once successfully connected to a WiFi

Table 2.4 Connection measurement dataset

Metric	Amounts
Measure duration	Over 2 months
Phone models	10
Platforms	Android
Total connected WiFi SSIDs	69
Total connected WiFi BSSIDs	2255
Campus WiFi SSIDs	3
Campus WiFi BSSIDs	1643
Observed successful connections	7289
Observed connection attempts	70,516

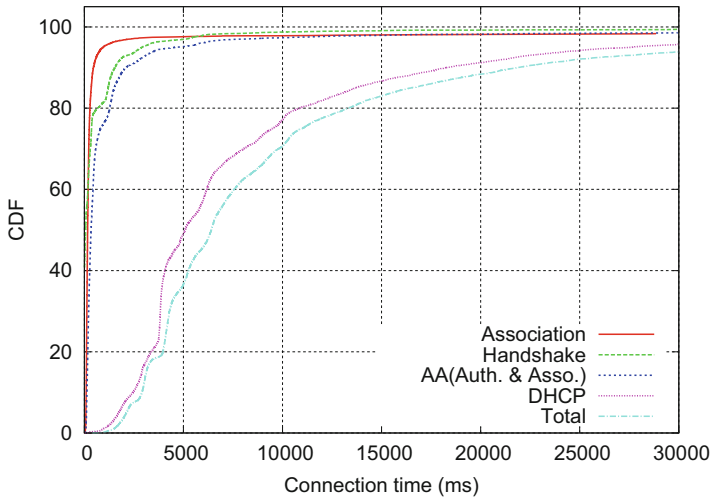


Fig. 2.13 CDF of the total connection setup time

network, the basic network information, like SSID, username, and password, will be automatically recorded and stored locally at WiFi client side in Android system. Due to WiFi networks normally recognized by SSIDs, this feature will engage the WiFi client to trigger the connection procedure automatically once the previous connected networks with the same SSIDs becoming available, which is quite applicable for connection measurements.

2.4.2 Characterizing Successful WiFi Connections

2.4.2.1 Overall of WiFi Connection Time

Figure 2.13 shows the CDFs of successful connection setup times for chosen WiFi networks, composed of AA times, handshake times, and IP acquisition (DHCP) times. Results demonstrate that the DHCP time is much larger than the other phases in the connection setup procedure, and occupies most of the connection time among all connection aspects. Furthermore, the AA time and handshake time only dominate a very small portion of the complete connection setup time, normally under 10%, and present a quite different trend from the connection time. About 80% successful connections can be completed within 10 s, which is considerably acceptable for mobile end users, and the main factor to influence the total connection time is the DHCP phase, which exhibits the similar variation tendency with the curve of connection setup time.

Figure 2.14 presents a close observation on the small portions of the connection setup procedure, which consists of the association phase, AA phase, and handshake

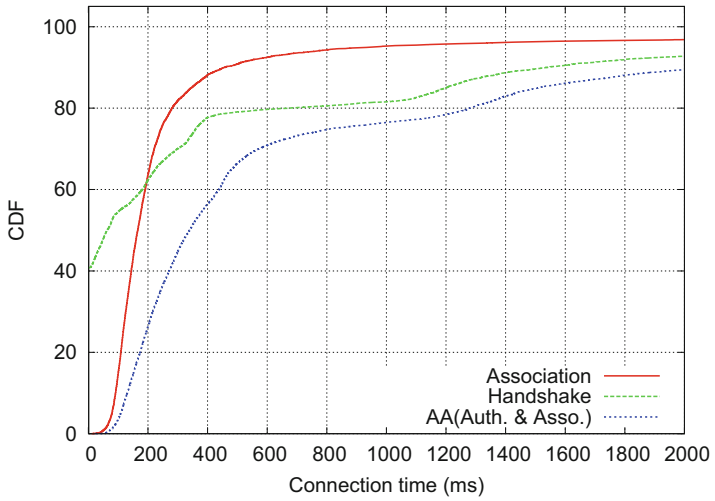


Fig. 2.14 CDF of association, AA, and handshake times

phase, to demonstrate the detailed interactions during WiFi connections. Results reveal that these minor time phases are quite short, but vital for the connection setup, and some can be completed instantly without user's awareness.

Nearly 90% of association times are under 400 ms and about 80% of AA times are completed in 1000 ms. Note that the WiFi handshake mechanism, utilized by WiFi APs and clients to identify each other based on some security specifications (WPA or WPA2), is optional for the connection setup. If the WiFi network is open and free accessible for WiFi clients without any security and authentication, the handshake time will always be 0 ms. About 40% of handshake times remain 0 in the dataset, due to some WiFi networks configured as "[ESS]" for totally free access without any security mechanism. Currently, some public WiFi networks utilize extra authentication portals, such as web access control servers or popular Android tools like WeChat [24], to verify the clients' intentions of WiFi connection, which does not encrypt the wireless communication lines and totally does not need any handshake procedure. It seems that the omitted handshake phase would shorten the overall connection process; however, in real environments, this connection approach needs the manual operations of WiFi clients and substantially lengthens the connection time than the normal ones.

2.4.2.2 Differentiate WiFi Connection Time by Various Devices

Figures 2.15 and 2.16 show the dissections of the connection time under the variant mobile devices. Figure 2.15 shows that the connection time range varies from several milliseconds to several seconds, and all the measured devices have a median

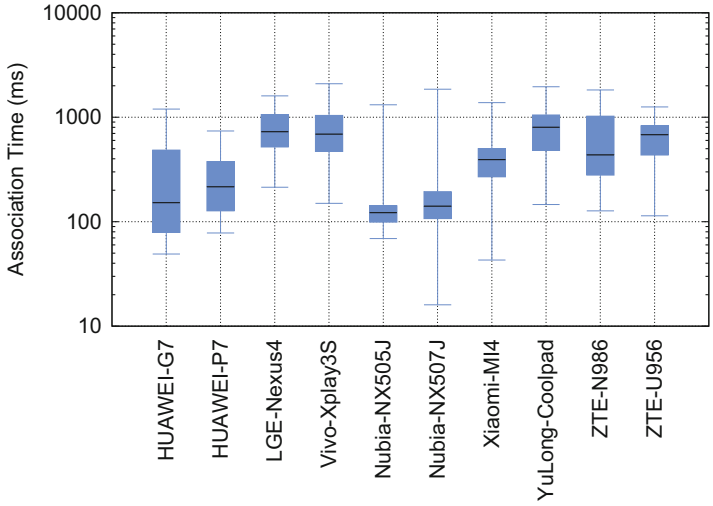


Fig. 2.15 Minimum, 25th, 50th, 75th percentiles, and maximum of AA time

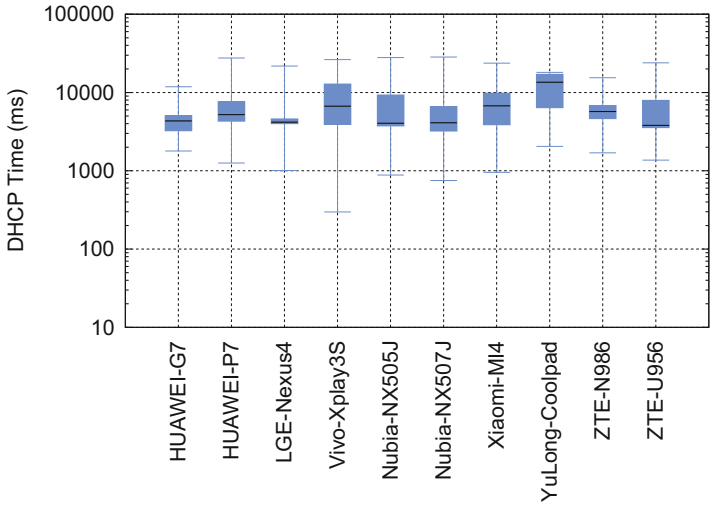


Fig. 2.16 Minimum, 25th, 50th, 75th percentiles, and maximum of DHCP time

association time smaller than 1 s. 6 phone models have a 75th percentile of less than 500 ms and it is less than 2 s among all the measured phone models.

Figure 2.16 shows that 6 phone models have a median percentile of IP acquisition time ranging from 3 to 5 s, and for 2 phone models, the time is greater than 6 s. And, for one model it was greater than 10 s. Measurement results show that the IP acquisition time is mainly distributed in the range of [2, 10] s. From these two figures, the IP acquisition time is the dominated part and greatly affects the overall connection time.

2.5 Related Work

In this section, we review the measurement studies on WiFi networks. Spectrum interference of WiFi networks have been examined in passive sniffing in a few studies. In [25], Rose and Welsh designed the Argos system which deployed 26 stationary devices around a city to sense wireless devices using passive sniffing. Argos is the first city-level wireless network inspection system that can detect, measure, and analyze the performance of wireless devices and networks, including network type, data traffic, and application type, etc. However, due to the specialized devices and fixed deployment in Argos, it is quite expensive and has low flexibility in the large deployment and measurement. Applying a similar carrier sensing mechanism, in [26] Paul et al. studied the interference of WiFi networks for detecting misbehaving WiFi nodes. Van Bloem et al. studied the effect of different interference sources on WiFi network, such as audio and video transmitter, microwave, and Bluetooth [27]. The results showed that the audio and video transmission have a serious impact on WiFi networks and lead to poor network performance.

Active measurement has also been applied in WiFi measurement. Sommer and Barford utilized an Internet measurement web site to the clients and collected more than 300 million user measurement results in 15 different areas [2]. They compared various performance issues between WiFi networks and cellular networks in distinct areas. Their results show that there exists notable room for improving and optimizing the deployment for these two kinds of networks. In [28], Seneviratne et al. investigated the WiFi connection setup time in a lab environment. They examined the whole WiFi connection procedure between smart phones and WiFi APs. They found that the WiFi connection time is strongly impacted by the DHCP message transmission and proposed a scheme to accelerate the DHCP process for reducing the WiFi connection time. Farshad et al. utilized an Android App, RF Signal Tracker, to measure WiFi APs and networks in a typical European city (Edinburgh) in [29]. Participants took buses as the carriers on the main roads in the city and run the measurement tool in smartphones to characterize the urban WiFi distributions and features using the MCS. WiGLE [30] aggregated the WiFi measurement data collected by the war-driving measurement tool and constructed the wireless network mappings on the Google map which was also visualized on a web site. The results showed that WiFi networks have been hugely increased and densely deployed in recent years, and WiFi devices have been experiencing potential channel and spectrum interference in high-density deployment areas.

In this chapter, we designed and implemented a MCS platform to conduct a comprehensive WiFi measurement study with the focus on two aspects in both spectrum interference and connection establishment during mobility in a real campus network environment. We classified the interferences between the private and public WiFi network. In particular, we inspected the overall WiFi connection procedure by dissecting the detailed steps in the connection process with tracking connection state transitions. We also analyzed the reasons for unsuccessful connections based on our measurement data. Similar to [29], our results confirm that WiFi network deployments have been increasingly dense and causing consequences.

2.6 Conclusion

In this chapter, we conducted a measurement study of increasingly densely deployed WiFi networks in a campus area based on the MCS mechanism. Due to no planning, large-scale, and high-density deployment of WiFi networks, our measurement results show that current WiFi networks have various problems in frequency interferences. The campus WiFi networks suffer from the potential interferences not only from private networks but also from themselves for the high-density deployment in the main channels. With the growth of the public WiFi networks' deployment density, the intra-network interference is becoming dominating, and the aggregate interference becomes more severe. By supporting the measurement tools using the MCS way on Android systems, we chose measurement areas with well-deployed public campus WiFi networks to investigate the characteristics of the connection setup time of WiFi networks. The WiFi connection setup is the prerequisite condition for the WiFi connection and data transmission. Our measurement results showed that the connection time deviates significantly on different mobile devices.

Our overall measurement results showed that the current WiFi network deployments are largely unplanned and disordered and lead to the significant performance degradation due to inter-/intra-interference, the competition, and sharing of channels. It may not be sufficient to solve these emerging problems in densely deployed WiFi networks with the standard 802.11 protocols. Motivated by the findings in this chapter, we will design and develop software-defined WiFi network infrastructure and protocols to mitigate the interference and mobility to enhance the performance and manageability of WiFi networks [31–33]. Our preliminary study have demonstrated the feasibility of constructing a software-defined WiFi network testbed and there exists the trade-off between performance and programmability of software-defined APs [34].

Acknowledgements This work was supported in part by the National Natural Science Foundation of China (no. 61370231), in part by the Fundamental Research Funds for the Central Universities (nos. 2016YXMS303 and 2017KFYXJJ190).

References

1. Zhang C, Qiu D, Mao S, Hei X, Cheng W (2015) Characterizing interference in a campus WiFi network via mobile crowd sensing. In: 11th international conference on collaborative computing (CollaborateCom), pp 173–182
2. Sommers J, Barford P (2012) Cell vs. WiFi: on the performance of metro area mobile connections. In: ACM SIGCOMM IMC, pp 301–314
3. Suiy K, Zhou M, Liu D, Ma M, Pei D, Zhao Y, Li Z, Moscibroda T (2016) Characterizing and improving WiFi latency in large-scale operational networks. In: 14th annual international conference on mobile systems, applications, and services (MobiSys), pp 347–360

4. Shi J, Meng L, Striegel A, Qiao C, Koutsonikolas D, Challen G (2016) A walk on the client side: monitoring enterprise WiFi networks using smartphone channel scans. In: IEEE INFOCOM
5. Gao Y, Dai L, Hei X (2017) Throughput optimization of multi-BSS IEEE 802.11 networks with universal frequency reuse. IEEE Trans Commun 65(8):3399–3414
6. Goel U, Wittie M, Claffy K, Le A (2016) Survey of end-to-end mobile network measurement testbeds, tools, and services. IEEE Commun Surv Tutorials 18(1):105–123
7. Guo B, Wang Z, Yu Z, Wang Y, Yen N, Huang R, Zhou X (2015) Mobile crowd sensing and computing: the review of an emerging human-powered sensing paradigm. ACM Comput Surv 48(1):7:1–7:31
8. Khan WZ, Xiang Y, Aalsalem MY, Arshad Q (2013) Mobile phone sensing systems: a survey. IEEE Commun Surv Tutorials 15(1):402–427
9. Lane N, Miluzzo E, Lu H, Peebles D, Choudhury T, Campbell A (2010) A survey of mobile phone sensing. IEEE Commun Mag 48(9):140–150
10. Zhuang Y, Syed Z, Georgy J, El-Sheimy N (2015) Autonomous smartphone-based WiFi positioning system by using access points localization and crowdsourcing. Pervasive Mob Comput 18:118–136
11. Gao C, Kong F, Tan J (2009) HealthAware: tackling obesity with health aware smart phone systems. In: IEEE ROBIO, pp 1549–1554
12. Vu L, Nguyen P, Nahrstedt K, Richerzhagen B (2015) Characterizing and modeling people movement from mobile phone sensing traces. Pervasive Mob Comput 17:220–235
13. Mun M et al (2009) PEIR, the personal environmental impact report, as a platform for participatory sensing systems research. In: ACM MobiSys
14. Ganti R, Ye F, Lei H (2011) Mobile crowdsensing: current state and future challenges. IEEE Commun Mag 49(11):32–39
15. Lane ND, Eisenman SB, Musolesi M, Miluzzo E, Campbell AT (2008) Urban sensing systems: opportunistic or participatory? In: ACM HotMobile
16. Lane ND et al (2013) Piggyback crowdsensing (PCS): energy efficient crowdsourcing of mobile sensor data by exploiting smartphone app opportunities. In: ACM conference on embedded networked sensor systems (SenSys)
17. Xiao Y, Simoens P, Pillai P, Ha K, Satyanarayanan, M (2013) Lowering the barriers to large-scale mobile crowdsensing. In: ACM HotMobile
18. Shu P, Liu F, Jin H, Chen M, Wen F, Qu Y (2013) eTime: energy-efficient transmission between cloud and mobile devices. In: IEEE INFOCOM
19. Zhang T et al (2015) eTrain: making wasted energy useful by utilizing heartbeats for mobile data transmissions. In: IEEE ICDCS
20. Liu F et al (2013) Gearing resource-poor mobile devices with powerful clouds: architectures, challenges, and applications. IEEE Wirel Commun 20(3):14–22
21. Liu F, Shu P, Lui JC (2015) AppATP: an energy conserving adaptive mobile-cloud transmission protocol. IEEE Trans Comput 64(11):1
22. Gualda D, Urena J, Garcia J, Garcia E, Ruiz D (2013) RSSI distance estimation based on genetic programming. In: International conference on indoor positioning and indoor navigation (IPIN), pp 1–8
23. IEEE standards, WiFi MAC producer query. http://standards.ieee.org/develop/regauth/oui/public.html/
24. Tencent Inc. Wechat: connecting people with chat, calls and more. http://www.wechat.com/
25. Rose I, Welsh M (2010) Mapping the urban wireless landscape with Argos. In: ACM SenSys, pp 323–336
26. Paul U, Kashyap A, Maheshwari R, Das S (2013) Passive measurement of interference in WiFi networks with application in misbehavior detection. IEEE Trans Mobile Comput 12(3):434–446
27. van Bloem JW, Schiphorst R, Kluwer T, Slump C (2012) Interference measurements in IEEE 802.11 communication links due to different types of interference sources. In: 2012 8th international conference on wireless communications, networking and mobile computing (WiCOM), pp 1–6

28. Seneviratne S, Seneviratne A, Mohapatra P, Tournoux PU (2013) Characterizing WiFi connection and its impact on mobile users: practical insights. In: ACM MOBICOM, pp 81–87
29. Farshad A, Marina M, Garcia F (2014) Urban WiFi characterization via mobile crowdsensing. In: IEEE network operations and management symposium (NOMS)
30. Wigle: Wireless geographic logging engine. http://wigle.net/
31. Nsunza WW, Hei X (2017) Design and implementation of a smart home router based on Intel Galileo gen 2. In: 12th EAI international conference on testbeds and research infrastructures for the development of networks & communities (TRIDENTCOM)
32. Chen Z, Fu D, Gao Y, Hei X (2017) Performance evaluation for WiFi DCF networks from theory to testbed. In: The 16th IEEE international conference on ubiquitous computing and communications (IUCC)
33. Kang J, Hei X, Song J (2017) A comparative study of Zynq-based OpenFlow switches in a software/hardware co-design. In: International workshop on network optimization and performance evaluation (NOPE)
34. Zahid T, Hei X, Cheng W, Ahmad A, Pasha M (2018) On the tradeoff between performance and programmability for software defined WiFi networks. Wirel Commu Mobile Comput 2018:12 pp