Journal of Computers Vol. 30 No. 1, 2019, pp. 64-74
doi:10.3966/199115992019023001007

Dissecting Campus WiFi Connections in an Empirical View

Chengwei Zhang[1], Xiaojun Hei[1*], Yexian Fan[2], Liang Xiao[3]

[1] Huazhong University of Science and Technology, Wuhan, China

[2] Normal University, Ningde, China

[3] Xiamen University, Xiamen, China
{zhangcw, heixj}@hust.edu.cn, yfan@ndnu.edu.cn, lxiao@xmu.edu.cn

Received 9 January 2018; Revised 22 January 2018; Accepted 22 January 2018

Abstract. High-density WiFi networks have been deployed in large-scale public areas to provide cost-effective Internet access for mobile end-users in recent years. While pedestrians are wandering around in WiFi coverage areas, the most essential issue is to establish and maintain connections between WiFi end-hosts and access points (AP) to deliver data effectively. As the resident time restricted by the end-user's mobility and the limited WiFi coverage, the connection establishment and re-connection may significantly impact user's experience and transmission efficiency of WiFi networks. We conducted a measurement study of dissecting WiFi connections on the real-world densely-deployed campus WiFi networks using an instrumented WiFi measurement framework. The whole connection setup procedure, consisting of Authentication-Association (AA), handshake and IP acquisition, is generally affected by AP densities, RSSI levels, pedestrians' moving characteristics, etc. Mobile devices frequently attempt to establish wireless connections with available WiFi APs; nevertheless, the ratio of successful attempts is only about 10% in the observed measurements, which is quite low while pedestrians moving around in WiFi hot spots. Our field measurement may provide insights into designing the next generation software-defined WiFi networks for optimizing connection setup time, improving success connection ratio and achieving high effective data delivery.

Keywords: active probing, connection time, mobile crowd sensing, WiFi measurement

1 Introduction

WiFi networks and mobile devices have become pervasive in the recent decade. Mobile devices equipped with WiFi modules can often utilize widely-deployed WiFi networks for mobile data traffic offloading for throughput enhancement or security measures [1]. Originally designed for single access point with a limited number of user devices, WiFi networks have now been deployed in public areas for supporting a large number of WiFi connections due to simple technical implementations, low-cost network construction and high-performance wireless links [2]. However, these co-located private and public WiFi networks are commonly deployed without any coordination and compete for unlicensed bandwidth, which may lead to significant performance degradation due to severe interference [3].

To make highly effective utilization of WiFi offloading, most traffic-intensive applications and services can schedule and postpone data transmission when mobile devices are moving through areas covered by available WiFi networks at public locations such as railway stations, airports and shopping malls [4]. It is necessary for a mobile device to be able to quickly establish wireless connections with available WiFi APs, then applications and services can download vital messages and data during the period that the user is within the coverage of the connected AP in a short-lived connection [5-6].

A short-lived connection is composed of three main phases: (1) connection establishment; (2) effective

* Corresponding Author

data transmission; (3) connection termination, which not only depends on the WiFi protocol standard [7], the pseudo error rate (PER) and interference [8], but also on the WiFi coverage, the speeds and directions of pedestrians [9].

Smart phones can measure, collect, and pre-process necessary data through powerful sensors and microprocessors while users carry them around during their daily activities [10]. Mobile measurement applications running on smart phones carried by a large number of users, can perform measurements individually and conduct data analysis collaboratively, to achieve mobile crowd sensing measurements.

In this paper, we are motivated to conduct a measurement study to characterize the connection procedure and its impacts of public campus WiFi networks in an empirical view. We first instrumented an Android App, namely WiFi Tracer [11], which can sense the neighboring WiFi APs through Android mobile devices, to obtain the distribution characteristics of neighboring WiFi APs. Then, we design a small Android App running at the background of smart phones, namely WiFi Status Monitor [12], to collect the complete connection events and status from mobile devices. This tool allows different mobile devices to track their own WiFi connection status and upload the results to the remote data server. Volunteers are required to install this app on smart phones and walk round in the public campus WiFi areas in their daily lives. Our major measurement results are summarized as follows:

(1) Characterize the connection establishment time for well-deployed public WiFi networks. A connection establishment consists of Authentication-Association (AA), handshake and IP acquisition. Nearly 80% observed connections can be established within 10s, and the IP acquisition occupies most of the connection setup time.

(2) Analyze various factors which can influence the connection setup time including WiFi AP densities, RSSI levels and pedestrians' moving characteristics. Within areas covered with denser WiFi APs and stronger RSSI levels, the connection setup consumes shorter time in establishing the connection.

(3) Infer the reasons for unsuccessful WiFi connection setups. Our results demonstrate that the AA phase, as a small portion of the connection process, is the main factor to hinder the successful connection establishment while mobile clients are in the moving states.

The remainder of this paper is organized as follows. Section 2 presents the background of a WiFi connection process during a short lived connection, and dissects the connection setup phases. The WiFi measurement framework and tools are described in Section 3, for conducting WiFi experiments and collecting data. In Section 4, we report the measurement results and data analysis. Finally, we conclude the paper and present the future work in Section 5.

2 Background

In general circumstances, while a mobile device is moving through the coverage of a WiFi hot spot, the mobile device will setup a short lived connection with the AP to transmit data needed by the mobile applications and services. Note that the short lived connection duration covers 3 different phases: (1) connection establishment; (2) effective data transmission; (3) connection termination. Fig. 1 illustrates the complete process of this short lived connection from the initialization to the termination when a user with a mobile device, normally a smart phone, walks through the coverage of a WiFi hot spot.

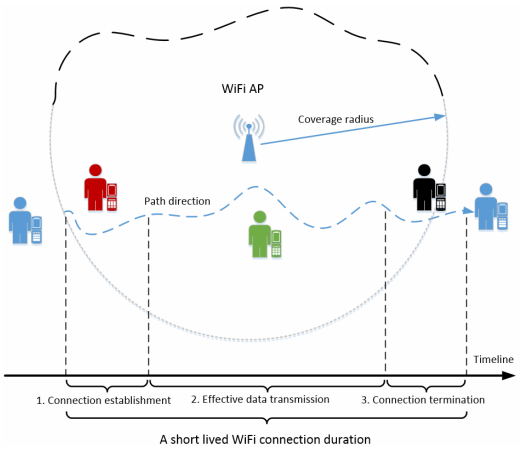

Fig. 1. WiFi connection duration illustration of mobile user

The above three phases in the connection duration are straightly step by step. Once a user with a smart phone walks into the coverage of a WiFi hot spot, the mobile device will actively or passively obtain the available WiFi APs and choose one suitable AP to initiate phase 1, namely the connection establishment, in which the client and the chosen AP will negotiate with each other on the association of the encryption method, protocol type and link speed. More details in the connection setup process will be discussed in Section 2.1. After that, the mobile client can transmit the data through the connected WiFi in phase 2. When the user moves towards the edge of the WiFi hot spot, where the signal strength becomes weaker, the data transmission will gradually experience lower link quality. Until the loss rate and speed of the link are not well enough to support wireless connections and meet the disconnection condition, the disconnection message will be sent between the AP and the client to terminate the wireless connection in phase 3. User icons with various colors in Fig. 1 reveal different phases during the short lived connections, and only the icon man in green has the probability to enjoy wireless data transmission.

2.1 Dissecting Connection Process

Before effective data transmission, the mobile device must succeed in initializing the connection setup process as phase 1. Fig. 2 shows the detailed initialization procedure of a WiFi connection setup. The complete connection setup process consists of three main phases: network discovery (scanning), network Authentication-Association (AA) and IP acquisition.

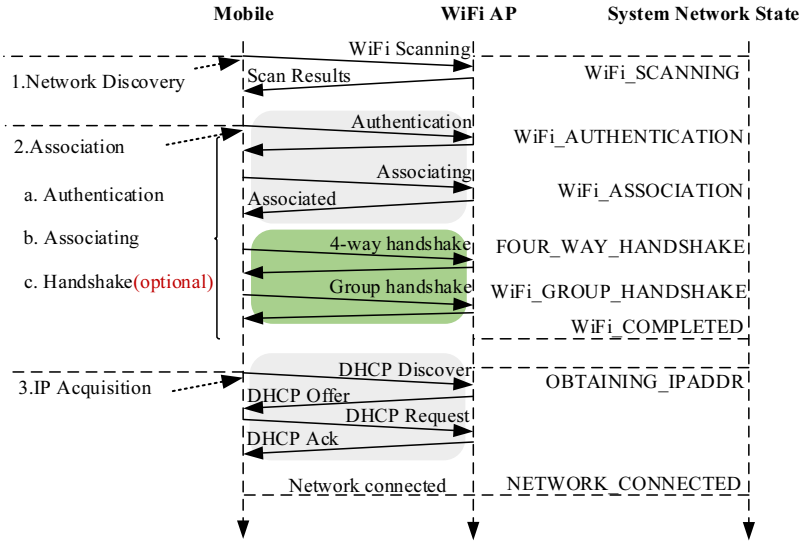

Fig. 2. Initialization of WiFi connection setup

Although a WLAN extends the whole WiFi network coverage and make it possible to support the WiFi clients moving around in a relative large areas, due to the limited coverage of each single WiFi AP in the WLAN, the WiFi client will still frequently change the WiFi APs to initiate the WiFi connection during the moving state. If the connection setup process failed, the client cannot build a successful WiFi connection with the chosen WiFi AP and will automatically reconnect to some WiFi APs using WiFi AP chosen algorithms (the default is the best RSSI chosen algorithm). Therefore, the WiFi connection time is a key metric to evaluate the performance of WiFi networks.

As there are three phases existing in the connection procedure, they must be achieved one by one in turn. A mobile client can discovery available WiFi APs either passively or actively. Passive discovery uses the beacon frames broadcasted by the WiFi AP at intervals of 100ms or some multiple of 100ms [13]. Active discovery is that the WiFi devices transmit a probe request for the WiFi APs nearby and the request received APs will response their own basic WiFi information to the WiFi clients, the discovery frequency depends on the WiFi module configuration of the mobile devices. For the scenarios considered in this paper, the discovery procedure is treated as an independent phase distinctly from the other two phases, because it does not trigger the initial connection procedure and only provides available WiFi networks' information which would be ready for WiFi connections.

Once a suitable WiFi network is identified, the mobile device will enter the next phase: Authentication-Association (AA) phase, where the mobile device transmits an Authentication frame to authenticate itself with the chosen AP. Once authenticated, it sends an Association Request to the authenticated AP to associate with the AP. Besides the AA time, due to the different security mechanisms in WiFi networks, the four-way handshake and group handshake would be admitted through this phase followed by the Association Response.

After the AA phase has been confirmed, the device begins to obtain the IP address within the DHCP phase. The WiFi device will broadcast a DHCP Discovery message. This notifies the DHCP server in the WiFi network to send a DHCP Offer as the response message. When the DHCP Offer message is received, the client will broadcast a DHCP Request message for requesting the IP address. The DHCP server confirms the client DHCP request by returning a DHCP acknowledgement message. If no response is received from the DHCP Request or DHCP Discovery messages, the sender waits for a period time determined using an exponential back-off algorithm. Once the IP acquisition is successful, the overall connection setup is complete and the mobile client can transmit data on the connected WiFi network.

2.2 Tracking Connection States at the Client Side

The investigation in differentiating various stages of the connection can motivate us to discover the factors and bottlenecks influencing the connection setup process. Due to messages and data transmitted between WiFi APs and mobile devices, there have two ways to obtain the significant information, which is at the side of the WiFi AP or the WiFi client. It is a big challenge to install some applications or services on WiFi APs, because WiFi APs are commercially black boxes and not open for end users. On the contrary, it is applicable to deploy the measurement applications or services on the Android WiFi client side, which is an open platform widely used by end users [14-15].

As the Android system utilizes "wpa_supplicant" [16], an open-source IEEE 802.11X/WPA component for variant systems, to manage the overall WiFi connection, transmission and disconnection states from the kernel level, which offers a set of key messages to represent the whole WiFi connection at the mobile client side. Thus, it is possible to provide applications or services to inspect the entire connection duration, including the establishment, data transfer and termination, for distinguishing distinct stages at the Android WiFi client side.

Fig. 3 presents a complete WiFi state machine in the Android system, which is executed at the lower layer of "wpa_supplicant" and controlled at the higher layer of WiFi management. Then the coarse states of the connection duration shown in Fig. 1 can be conveniently extracted by corresponding WiFi states, represented with the predefined broadcast messages in the Android system. To distinguish subtler states in the connection setup, more fine-grained states are defined and matched with the illustration as shown in Fig. 1 and Fig. 2. Therefore, by utilization of WiFi and other sensor modules in Android mobile devices, we can not only observe the coarse and fine-grained states of WiFi connection process, but also analyze the characteristics of WiFi connection and its impact factors at the WiFi client's side.

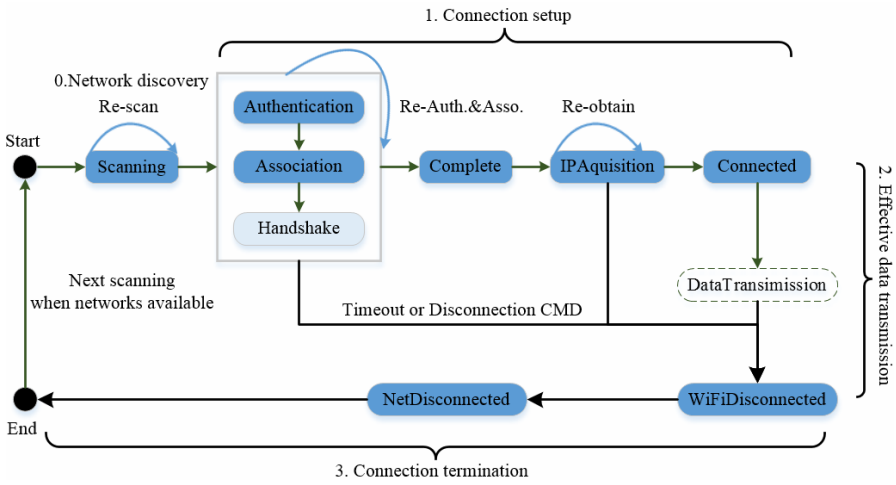

Fig. 3. Connection state machine on WiFi client side

3 Methodology

The public campus WiFi networks are widely deployed at public locations through the campus, and we are motivated to conduct a measurement study to characterize the connection process and the impacts of WiFi networks from an empirical view. Before conducting the connection experiments at these public locations, we need to understand the general deployment characteristics of campus WiFi networks for making experiment decisions. We first proposed a general WiFi sensing measurement framework using the mobile crowd sensing method to provision the transmission and sharing of measurement results, which can be collected and shared among various end devices like computers and smartphones.

3.1 Measurement Framework

Our proposed mobile crowd sensing platform is an integrated framework which consists of three major parts including data acquisition, collection and analysis. The first part, the data acquisition of measurement, can be formatted and stored locally to match the data transmission format defined by the framework, which is controlled by Android applications and services. The second part is responsible for collecting and analyzing the data as a repository server hosted on a cloud platform. When the volunteers finish the measurements, the Android app running on the framework will automatically upload the formatted results to the cloud server and the server will mark the time tags and user tags to distinguish each data source. The third part is used to share the available collected information as an incentive for participants. The server provides information about available WiFi APs near 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 application.

3.2 Android Measurement Tools

We designed two different Android apps under the proposed measurement framework, which are the WiFi Tracer [11] and WiFi Status Monitor [12] respectively. WiFi Tracer can sense the neighboring WiFi APs through Android mobile devices and tag the measurement results with time stamps and GPS coordinates so that different users can cooperate together to sample the WiFi basic characters efficiently at specified locations. While understanding the blueprint of WiFi networks deployed on the campus, we can easily choose well-deployed WiFi locations as the connection measurement locations to conduct the connection measurement of public campus WiFi networks. To extract the accurate WiFi connection states during the connection duration, we designed a small Android app, named WiFi Status Monitor, which is running background and monitor the complete connection events and status, discussed in Section 2, from Android devices. Due to these two apps designed based on the crowd sensing measurement framework, volunteers' smart phones installed with them can be utilized to take the measurement experiment in daily lives without much disturbance, which can maintain the diversity of various results and improve the measurement efficiency.

4 Results

By deep inspecting basic information of WiFi networks in a university campus, we have successfully collected two measurement datasets. One is for distinguishing the characteristics and difference between public WiFi networks and private networks at measurement locations through the whole campus, which can be used to identify the classic areas covered by public campus WiFi networks. The other one is the connection measurement dataset collected by different mobile devices at the chosen areas through the daily lives.

4.1 Basic WiFi Dataset

The basic WiFi information dataset was obtained by installing an application we developed, WiFi Tracer on volunteers' smartphones. Participants carrying different smartphones moved around on the main roads with relatively stable speeds to traverse the campus measurement areas. The basic WiFi sensing results, as shown in Table 1, summarize 18741 independent WiFi APs in measurement areas.

Table 1. WiFi sensing measurement dataset

Metric	Amounts
Scan times	50447
Measurement result sets	2412569
Independent areas by GPS	16076
Number of distinct WiFi APs	18741
Number of distinct WiFi Networks	13959
Number of 2.4GHz APs	11761
Number of 5GHz APs	4315
Number of public WiFi APs	7618

The basic WiFi dataset shows that more than 7000 distinct public campus WiFi APs have been successfully scanned and recorded during the WiFi scanning measurement process. Considering the maximum signal strength (RSSI) received at GPS locations, we can figure out the distribution and coexistence characteristics of the public and private WiFi APs. Based on the analysis of basic WiFi dataset, the areas covered with well-deployed public campus WiFi networks have been chosen to conduct the connection measurement experiments.

4.2 WiFi Connection Dataset

We invited volunteers as participants to install WiFi Status Monitor developed for Android systems and to move around the measurement areas during their daily lives. Through almost two months' measurement, we finally collected a WiFi connection dataset containing various data of connection procedure, discussed in Section 2. Table 2 presents data summary of connection experiments conducted on the chosen areas covered with well-deployed public campus WiFi networks. Based on the dataset, we have successfully observed more than 70000 times of connection attempts, and only about 10% attempts have finished the complete connection procedure and smoothly set up data communication links between WiFi APs and clients.

Table 2. WiFi connection measurement dataset

Metric	Amounts
Measure duration	nearly 2 months
Phone models	10
Platforms	Android
Total WiFi SSIDs	69
Campus WiFi SSIDs	3
Campus WiFi BSSIDs	1579
Observed succeeded connections	7289
Observed connection attempts	70516

4.3 Characterization of WiFi Connection Setup Time

Fig. 4 shows the CDF of the WiFi total connection setup, consisting of AA times, handshake times and IP acquisition (DHCP) times. Among all the aspects of the connection setup time, the IP acquisition time is relative larger than the other phases and dominates most of the time in the overall connection process. Nearly 80% connection process can be completed within 10s, which is considerably acceptable for mobile end users, and the DHCP time is main factor to influence the total connection setup time.

Fig. 5 presents a close observation at small portions of the connection setup procedure, which consists of association phase, AA phase and handshake phase, to demonstrate the detailed interaction of WiFi networks. The results reveal that these minor time phases are quite short, which can be completed instantly without user's awareness, but vital for the connection procedures. Over 90% association time is in 0.6 second and 80% AA time is finished within 1 second.

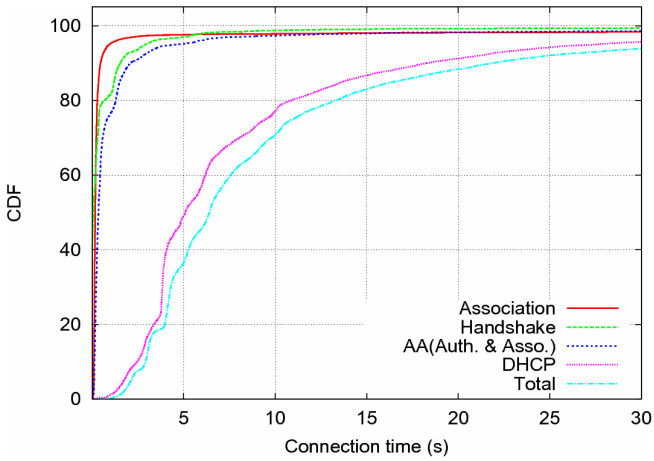

Fig. 4. CDF of total connection setup time

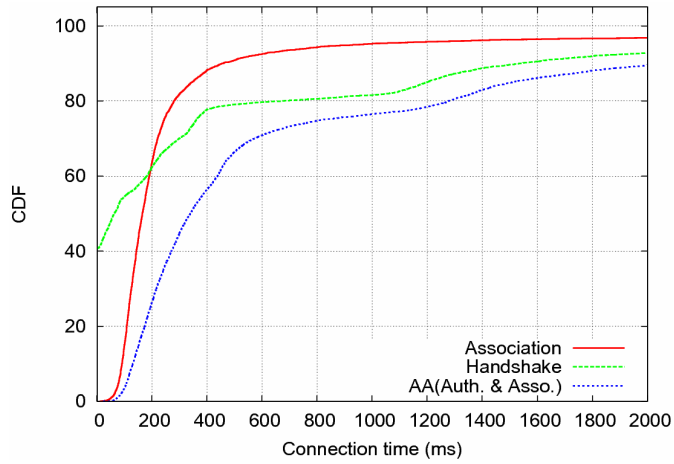

Fig. 5. CDF of association, AA and handshake times

Note that the WiFi handshake mechanism, which is utilized by the WiFi AP and the client to identify each other based on the security specifications (WPA or WPA2), nearly 40% of its consumed time is approaching 0ms. The reason is that some public WiFi networks instructed the additional web portal to authenticate the username and password from the client side, which do not need the handshake process at all.

4.4 Factors Affecting the Connection Setup Time

The connection setup process of WiFi networks is constrained potentially by the signal coverage, AP density and the pedestrian's moving behavior. To investigate these factors, which could influence the connection setup time substantially, can help us to deeply understand interactive characteristics of WiFi networks and limitations of WiFi protocols.

AP density of WiFi networks. Two reasons for high-densely deployed WiFi networks, one is for supporting a large number of clients to access the Internet simultaneously and reducing the conflictions during WiFi connection; the other is for extending the single AP's coverage and forming a relative large coverage with the support of multiple APs.

Consider the coexistence between public campus WiFi networks and private WiFi networks, the Public Ratio is defined to represent the number of public campus APs as the total APs. With more public campus APs deployed on measurement areas, the ratio is larger. Fig. 6 presents the connection setup time associated with different public WiFi ratios. The results imply that the number of WiFi APs deployed on measurement areas influences the overall connection time greatly. With more public APs deployed, the connection times are shorter because there are more candidate APs for association.

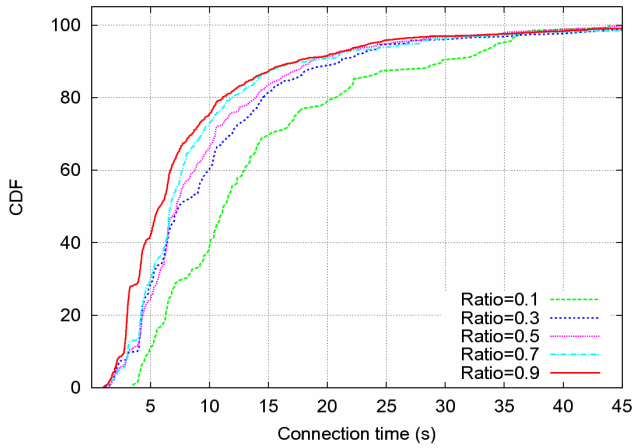

Fig. 6. Connection time CDF with different public ratios

Signal strength of connecting WiFi networks. When a WiFi client enters the coverage of available WiFi network, it will choose the AP with the strongest signal strength (RSSI) to setup a connection by the scanning in the AP discovery process. Due to the RSSI is in a relative value range to indicate the power level transmitted from the AP, we first mapped the RSSI values in an integer level range [0, 4]. A higher level indicates a stronger signal. Fig. 7 demonstrates that the better RSSI will help in decreasing the total connection time. Over 80% connection times at the strongest level's locations are completed in an acceptable time 10s, whereas only 20% connection times at the weakest level's locations meet the time level.

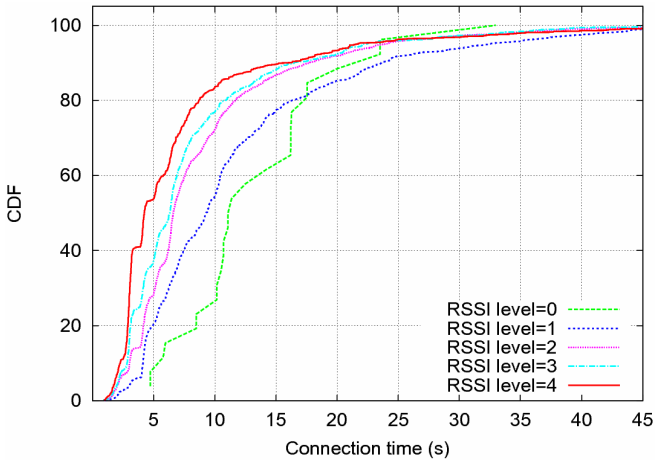

Fig. 7. Connection time CDF by RSSI levels

Moving directions while connecting WiFi networks. Measurement participants are suggested to move around in the coverage of available WiFi networks, who may cross the areas where RSSIs are in different levels. By comparing RSSI levels in moving states, we can roughly determine the moving direction as the direction level. When a user moves from a strong RSSI level area to a weak RSSI level area, which means the user is approaching to the connected AP, the direction level is greater than 0, whereas the direction level is less than 0. Fig. 8 shows that if the user does not cross a relative large area through the coverage area and just wanders in a small area, the connection time will result better performance than the other two scenarios.

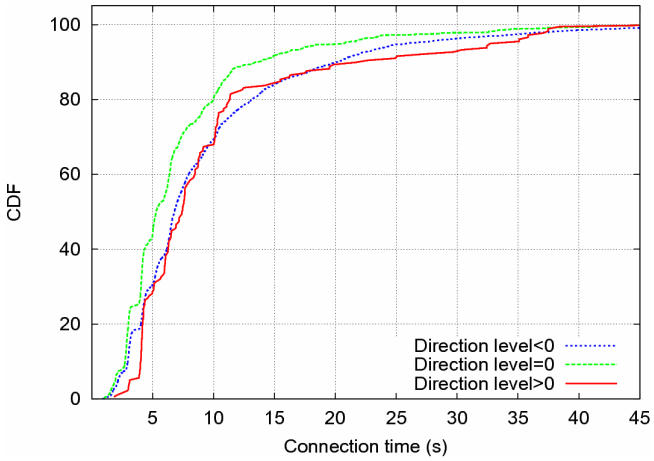

Fig. 8. Connection time CDF by direction levels

4.5 Failure Analysis for WiFi Connections

As a normal WiFi client, once it enters some areas covered by available WiFi networks, it will frequently attempt to setup the connections with different WiFi APs until it successfully connects some AP through the connection setup process. The connection measurement experiments have succeeded in collecting the complete dataset of variant WiFi connection procedures, which can be classified into 2 types: (1) success connections; (2) failure connections. The failure connections, dominating the total connection dataset, demonstrate the low success efficiency of WiFi connections and would provide more insights into maintaining continuous WiFi connections.

Table 3 summarizes the reason classifications in the failed connection dataset observed at the WiFi client side. The results demonstrate that the failure of the Association phase, a small portion in the connection setup procedure, as the major reason for resulting in the failed WiFi connections, dominates over 90% of the total failed connections; whereas the failure of the DHCP phase, occupying most of the connection time, accounts for only about 8% of the failed ones. The primary analysis for the failed WiFi connections is different from [6], which stated that the DHCP phase is the main factor to hinder the connection setup instead of the AA phase.

Table 3. Reason classification for failure connections

Item	Category	Results	PCT. (%)	Total
Total connections	Success	7289	10.3	70516
	Failure	63227	89.7	
Failure reasons	Authentication	1201	1.9	63227
	Association	57365	90.7	
	IP Acquisition	4653	7.4	
Disconnection reasons for failure connections	Regular	9209	13.1	70516
	Timeout	61307	86.9	

5 Conclusion

In this paper, we analyzed the connection setup process and its impacts of WiFi networks. The WiFi connection setup is prerequisite for WiFi data transmission. Our results show that the connection setup mainly consists of the AA time, the handshake time and the DHCP time, which is generally affected by WiFi AP densities, RSSI levels and pedestrians' moving characteristics. The success ratio of connection attempts is quite low while users move around between WiFi APs. The AA phase is the dominating factor to prevent the connection establishment between mobile devices and WiFi APs. We are now motivated to utilize a software-defined approach to design a general SDN-based WiFi platform to meet these challenging issues for provision of fast connection setup, high efficient connection ratio and low-energy WiFi systems. The connection setup phase can even be eliminated based on the coordination

between APs in a software defined WiFi network architecture [17]. We plan to design and implement a light-weighted virtual access point on Zynq-based programmable WiFi systems in a software/hardware co-design approach [18].

Acknowledgements

This work was supported in part by the national Natural Science Foundation of China (No. 61370231, No. 61671396), in part by the Fundamental Research Funds for the Central Universities (No. 2016YXMS303 and 2017KFYXJJ190).

References

[1] L. Xiao, Y. Li, X. Huang, X. Du, Cloud-based malware detection game for mobile devices with offloading, IEEE Transactions on Mobile Computing 16(10)(2017) 2742-2750.

[2] C. Zhang, D. Qiu, S. Mao, X. Hei, W. Cheng, Characterizing interference in a campus WiFi network via mobile crowd sensing, in: Proc. 2015 11th International Conference on Collaborative Computing (CollaborateCom), 2015.

[3] Y. Gao, L. Dai, X. Hei, Throughput optimization of multi-BSS IEEE 802.11 networks with universal frequency reuse, IEEE Transactions on Communications 65(8)(2017) 3399-3414.

[4] H. Yao, D. Zeng, H. Huang, S. Guo, A. Barnawi, I. Stojmenovic, Opportunistic offloading of deadline-constrained bulk cellular traffic in vehicular DTNs, IEEE Transactions on Computers 64(12)(2015) 3515-27.

[5] C. Pei, Z. Wang, Y. Zhao, Z. Wang, Y. Meng, D. Pei, Y. Peng, W. Tang, X. Qu, Why it takes so long to connect to a WiFi access point? in: Proc. INFOCOM, 2017.

[6] S. Seneviratne, A. Seneviratne, P. Mohapatra, P.-U. Tournoux, Characterizing WiFi connection and its impact on mobile users: practical insights, in: Proc. International Conference on Mobile Computing and Networking (MOBICOM), 2013.

[7] B.P. Kraemer, An incentive framework for cellular traffic offloading, in: Proc. IEEE Computer Society LAN MAN Standards Committee, 2009.

[8] J.-R. Lin, T. Talty, O. Tonguz, An empirical performance study of intra-vehicular wireless sensor networks under WiFi and blue tooth interference, in: Proc. 2013 IEEE Global Communications Conference (GLOBECOM), 2013.

[9] M. Simsek, M. Bennis, M. Debbah, A. Czylwik, Rethinking offload: how to intelligently combine WiFi and small cells? in: Proc. 2013 IEEE International Conference on Communications (ICC), 2013.

[10] U. Goel, M. Wittie, K. Claffy, A. Le, Survey of end-to-end mobile network measurement testbeds, tools, and services, IEEE Communications Surveys and Tutorials 18(1)(2016) 105-123.

[11] C. Zhang, D. Qiu, X. Hei, WiFi Tracer. <http://www.wandoujia.com/apps/com.wifitracer>.

[12] C. Zhang, D. Qiu, X. Hei, WiFi Status Monitor. <http://itec.hust.edu.cn/_zhangcw/WiFiTracer>.

[13] V. Iyer, F. Hermans, T. Voigt, Detecting and avoiding multiple sources of interference in the 2.4 GHz spectrum, in: Proc. European Conference on Wireless Sensor Networks (EWSN), 2015.

[14] K. Fukuda, K. Nagami, A measurement of mobile traffic offloading, in: Proc. the ACM SIGCOMM Internet Measurement Conference (IMC), 2013.

[15] J. Sommers, P. Barford, Cell vs. WiFi: on the performance of metro area mobile connections, in: Proc. ACM SIGCOMM Internet Measurement Conference (IMC), 2012.

[16] J. Malinen, WPA supplicant. <http://w1.fi/wpa supplicant/>.

[17] T. Zahid, X. Hei, W. Cheng, A. Ahmad, M. Pasha, On the tradeoff between performance and programmability for software defined WiFi networks, in: Wireless Communications and Mobile Computing (WCMC), 2018.

[18] J. Kang, X. Hei, J. Song, A comparative study of Zynq-based OpenFlow switches in a software/hardware co-design, in: Proc. the 5th International Workshop on Network Optimization and Performance Evaluation (NOPE), 2017.