IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 18, 2018, accepted June 25, 2018, date of publication July 6, 2018, date of current version July 30, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2853599

Localizing Access Point Through Simple Gesture

YONGLE CHEN, XIAOJIAN WANG, DAN YU, YULI YANG, AND JIAN CHEN, (Member, IEEE)
College of Information and Computer, Taiyuan University of Technology, Taiyuan 030024, China

Corresponding author: Yongle Chen (chenyongle@tyut.edu.cn)

This work was supported in part by the National Key Research and Development Program under Grant 2018YFB0803402 and in part by the Natural Science Foundation of Shanxi Province under Grants 201701D111002 and 201601D021074.

ABSTRACT It is important to obtain the location of an access point (AP), such as in the scenario of finding rogue AP in public places or designing indoor positioning system based on AP locations. Most of the existing AP localization methods depend on additional equipment with high cost or the path loss model suffering from indoor multipath. In this paper, an AP localization algorithm based on channel state information and Fresnel zone is proposed, which can just draw a semicircle with one hand to estimate the AP location. The algorithm is divided into two phases: preparations and positioning. Preparations' phase includes calibrating AP direction and identifying Fresnel zone cutting points which are obtained by combining the least squares fitting method in the time domain. Positioning phase consists of AP direction determination and AP position determination; the final AP position is confirmed according to the geometrical information. The experimental results show that the median error of our algorithm can achieve to 0.58 m, which significantly improve the AP positioning performance than other methods.

INDEX TERMS Channel state information, MIMO, position measurement, wireless LAN.

I. INTRODUCTION

With the widespread deployment of Wi-Fi access point, wireless networks have been perceived everywhere. It is necessary to find the location of an AP in some scenarios. For example, a rogue AP nearby is detected, but it is hard to find the accurate location of this AP in a wide range public area. Besides, a known AP location can be advantageous to optimize wireless coverage of access points within a service area and designing indoor accuracy positioning systems.

AP locations are usually known by default in most Wi-Fi-based indoor positioning systems [16], [19], [20], even for some applications that examine the effect on positioning performances when new AP is added [5]. Obtaining the location of these APs generally uses manual measurement methods, which are time-consuming and laborious. Therefore it is highly desirable to determine AP locations in an easy-to-use and accurate method.

The problem that we want to solve in this paper is how to determine the AP location easier and more accurate.

Some methods of locating AP are based on special hardware, such as deploying multiple directional antennas in suspicious areas, and estimating the AP location using signal contour maps based on signals received from multiple directional antennas [4]. But it is high-cost. Some other AP positioning methods utilize the path loss model based on the Received Signal Strength (RSS), which considers the area that is closer to the AP, where the Line-of-Sight (LoS) path is not blocked by obstacles, should have a higher signal strength. But RSS is significantly affected by multipath and shadow in the complex indoor environment. Experimental studies have shown that in the indoor environment of a stationary receiver, there is 5dB fluctuation of the received signal strength for a period of about one minute [7], this means that the RSS-based AP localization method hard to achieve an ideal accuracy.

There are also ways to use channel state information (CSI) for AP positioning. Zheng *et al.* [15] require people to stand at eight different positions, and then walk along a certain arc to compute the AP direction. SpinLoc can use the Energy of the Direct Path (EDP) of CSI to estimate the direction of the AP, where the user is expected to rotate once. But even assisted by multiple APs, the methods mentioned above are also hard to determine the accurate angle [16]. Our basic idea is to use a single receiver to collect CSI information to determine the AP direction, and further to obtain the location of AP by combining with the direction of three different locations. We have found that the CSI data collected at the Wi-Fi receiving device are affected by moving gesture, especially when a hand passes through the LoS path of the first Fresnel zone. Therefore, analyzing the CSI data collected by the moving as

a specific gesture, the AP direction can be determined more accurately.

The main contributions of this paper are as follows:

- We use only such a simple gesture as drawing a semicircle, analyzing the variation of corresponding CSI value, to determine the direction of AP more accurately without additional hardware cost and extensive labor.
- To our knowledge, Fresnel zone model is firstly applied to AP positioning, and the feasibility of using Fresnel zone model to detect specific gesture is verified by our experiments.
- We propose a LoS path identification method, using the delay distribution and outlier detection in the channel impulse response (CIR) to identify the existence of LoS path, and CIR can be obtained by applying inverse fast fourier transform (IFFT) on CSI.
- In order to minimize the influence of multipath, we use Discrete Wavelet Transform (DWT) to eliminate the background noise, and gained good effects of denoising.
- A linear fitting peak searching algorithm is proposed to identify Fresnel zone cutting point for improving the accuracy of AP direction, and the correlation characteristics of the CSI subcarriers found in the experiment were further used for AP direction correction.

The rest of this paper is organized as follows. In Section II, we present the related works. In Section III, we proposed the framework of our algorithm, introduce the knowledge of CSI and describe each part of the framework in detail. The experiment and evaluation are shown in Section IV. Finally, we summarize our work in Section V.

II. RELATED WORK

The existing AP positioning method can be divided into three categories: special hardware-based, RSS-based, and CSI-based.

A. SPECIAL HARDWARE-BASED

Most of the existing methods for positioning AP are based on the deployment of specialized hardware (e.g., multiple sniffers, directional antennas) [4], [8]–[10]. The rogue AP location can be estimated by using a signal contour map based on the distributed monitoring system which running wireless sniffing software [4]. The monitoring server will receive the received signal strength from wireless sniffers and determine AP position. Adelstein *et al.* [8] utilize a plurality of rotating directional antennas to collect the information of the signal strength, then to determine the AP position. Awad *et al.* [23] use a swarm of wireless connected mobile robots to detect the AP location by gathering a small amount of non-uniform distributed AP RSS samples collaboratively and autonomously. However, the cost is high in the above scenario of deploying multiple sniffers or directional antennas.

B. RSS-BASED

Most of RSS-based AP positioning methods assume the area closing to AP or getting the LoS path should have a higher signal strength. Some research works have used RSS data to achieve AP positioning [5], [10]–[13]. Han *et al.* [11] show a method using a gradient algorithm to locate AP position by combining the directional estimates from the RSS direction information of multiple advantageous points . The position of the unknown AP is obtained in [5] by managing the distance between the user at known locations and the unknown AP, which are calculated by using attenuation model based on the signal strength information. The arrival angle of the data frame transmitted from the AP is estimated by the signal strength of different directional beams which are collected from continuously rotated directional antenna [10]. Zhang *et al.* [6] show that the AP direction can be determined by estimating the greatest signal strength decline which is caused by the obstacle of the human body at the different directions of the wireless receiver. A point-to-point guidance system is implemented using a gradient method [13]. Wilson and Patwari [14] proposed a method of Radio Tomography Imaging (RTI) to track actions at the target area with sensor nodes deployed, and use the extra investment to mitigate the effects of multipath. Awad *et al.* [22] utilize received signal strength to estimate the distance between the AP transmitter and some known locations around, and proposed a Particle Swarm Optimization algorithm to search for the AP optimal location by matching the given sample set. The received signal strength sample set, along with their corresponding known locations will be the input of their algorithm. However, The RSS-based AP positioning method hard to achieve an ideal accuracy due to the complex indoor environments.

C. CSI-BASED

The fading characteristics of the human body in blocking AP are analyzed in [15]. People are required to stand in different positions and make a series of actions, then the AP direction is obtained by using the amplitude correlation and the amplitude orthogonal transformation in the time domain. Based on [15], Wang *et al.* [21] leverage the frequency domain CSI phase and the multiple antennas on the device to further improve the direction estimation accuracy. The determined direction of the rogue AP can facilitate the rogue AP localization by directly pinpointing the rogue AP using spatial diversity (with the directions determined at multiple locations). In SpinLoc [16], the power delay profile (PDP) is used to obtain EDP, and the user need to rotate for estimating the direction of the AP. The signal attenuates in different ways due to the human blocking, therefore the attenuate can reveal the direction of AP in the indoor environment.

Above methods either require high infrastructure cost and extensive labor or lack of precision, meanwhile these methods are also complicated. We proposed a new method that just uses a simple gesture (i.e. drajwing a semicircle with one hand) without any additional hardware to estimate the AP location.

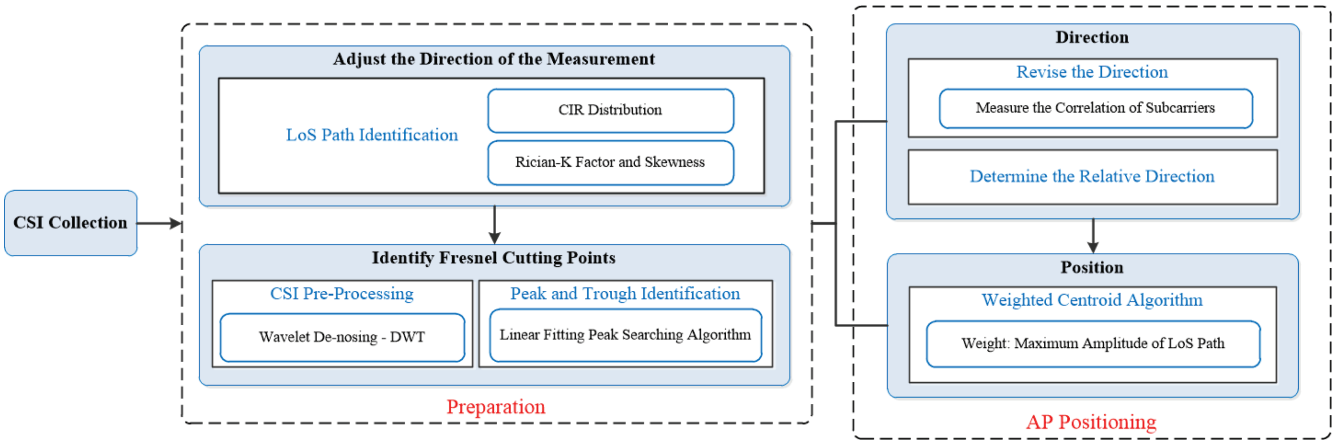


FIGURE 1. Framework overview.

III. ALGORITHM DESIGN

In this section, we introduce the basic conception of CSI and explain the workflow of our algorithm in detail.

A. ABOUT CSI

The majority of commercial off-the-shelf WiFi devices typically consist of multiple transmitter and receiver antennas due to support MIMO technology, and each MIMO channel includes multiple subcarriers. The channel state information (CSI) estimates the channel information by indicating the channel attribute of the communication link [17]. Channel state $H(f, t)$ at time t with carrier frequency f can be described by channel frequency response (CFR) or CIR. By modifying the firmware of the operating system's wireless network card [18], a sampling version of the CFR can be obtained from a commercial WiFi transmitter. In this paper, we use Intel 5300 wireless network card in 2.4GHz frequency, with 20MHz bandwidth, which can collect 30 subcarriers' CSI information. The CFR of CSI can be described as follows:

$$\mathrm{H(k)} = ||\mathrm{H(k)}||e^{\mathrm{j}\angle \mathrm{H(k)}} \tag{1}$$

where $H(\mathrm{k})$ is the CSI value of the k-th subcarrier, $||H(\mathrm{k})||$ and $\angle H(k)$ are the amplitude and phase of the k-th subcarrier. The CIR can be obtained by inversing Fourier transform of the CFR as follows:

$$\mathrm{h}(\tau) = \sum_{i=1}^{n} ai\, e^{-j\theta_i} \delta(\tau - \tau i) \tag{2}$$

For the i-th path, ai is the amplitude attenuation, θi is phase offset, τi is time delay, n is the total number of paths, and $\delta(\tau)$ is the Dirac pulse function.

B. FRAMEWORK OVERVIEW

Our experiments show that the CSI of the Wi-Fi receiving device will be affected by moving gestures, especially when the gesture moves through the first Fresnel zone. The Fresnel zone is a series of concentric elliptical regions, caused by multipath when a wave passes by an object in the propagation process. Due to the in phase and out of phase paths of different lengths, constructive and destructive interference are caused. We design a specific gesture which draws a 180-degree semicircle in front of the receiving end with one hand. The start and end point are shown in Fig. 2. When the moving hand cuts through the Fresnel zone between the AP and receiving end. The LoS path will be blocked and induce a greater impact on the CSI value. Therefore, by analyzing the CSI variation, the AP direction can be estimated more accurately. The main workflow of AP positioning algorithm is described in Fig.1. Firstly, we determine whether there is an available LoS path or not by analyzing the CSI in the time domain. If it exists, the waveform in the time domain is further analyzed to obtain the AP direction information. Otherwise, the AP position is re-determined by changing the measurement position. The final position of AP is obtained by using the geometrical information based on the AP direction and combining with the weighted centroid algorithm. The whole framework is divided into two phases as shown in Fig. 1.

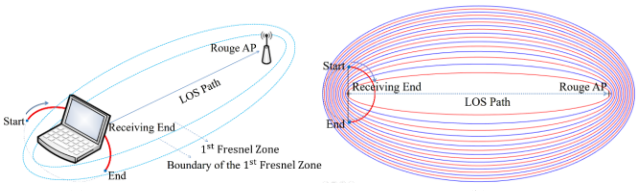


FIGURE 2. Methods expressed in sketch: (a) Side view of proposed method; (b) Top view of proposed method.

1) PREPARATION

This section consists of two steps, adjusting the direction of measurement and identifying the Fresnel zone cutting point. The reason why we need to adjust the direction of measurement is that we draw a semicircle in front of the human body with one hand rather than a complete circular

trajectory, which avoids the occlusion of the LoS path caused by the human body in the Fresnel zone. This means that we can only get information in front of the human body, and the information behind the body is unknown. If the LoS path does not exist in the range of front semicircle the user will be informed that turns back to measure the available data. In this paper, we use the CIR in the time domain to analyze the delay distribution to identify the existence of LoS path, which is important for the AP direction calculation. Identification of Fresnel zone cutting points mainly includes two steps: CSI preprocessing and peak and trough identification. In CSI preprocessing, the energy of the LoS path obtained from the CIR is further smoothed using discrete wavelet transforms (DWT). The peak and trough identification algorithm is used to determine the position of target valley, the start and end position of the target valley can be considered as the begin and end of the first Fresnel zone cutting point.

2) AP POSITIONING

This section also includes two steps: determining the direction and determining the position. First, through identifying the Fresnel cutting point, we judge whether the CSI characteristics generated during the gesture movement are in accordance with expectations, if it does match, export the percentage of the valley in the total data collected so as to derive the AP direction. If not match, it is necessary to make a second measurement and judge if there are some problems encountered in the LoS path identification. However, there is no guarantee that the data gathering process with start/end exactly simultaneous with gesture movement process begin/stop, data redundancy may occur under this circumstances. We find that the correlation of the 30 subcarriers in time domain show a strong continuous rising trend during the gesture moving processs, this phenomenon can help us correct the direction through finding the real start and end of the semicircle. Although the arc length between the two corresponding cutting points is determined, the waveform between two cutting points may not be perfect symmetry, which means the radius of the first Fresnel zone does not must be $R \sin\theta$, where R is the radius of the semicircle, 2θ is the central angle corresponding to the arc length between the two cutting points. Weigh the asymmetry and give an ideal corrected direction is needed. The final position of AP is obtained by using the geometrical information based on the AP direction and combining with the weighted centroid algorithm.

C. THE FOUND IN EXPERIMENT

In this section, we test the effect of gestures on CSI and verify the method of determining whether there is a LoS path.

1) THE EFFECT OF GESTURE ON CSI

The original amplitude information of 30 subcarriers generated from moving around the red arc in Fig. 2 is plotted in the time domain in Fig. 3. In Fig. 3(a), the abscissa axis is the number of samples, and the ordinate axis is the amplitude value.

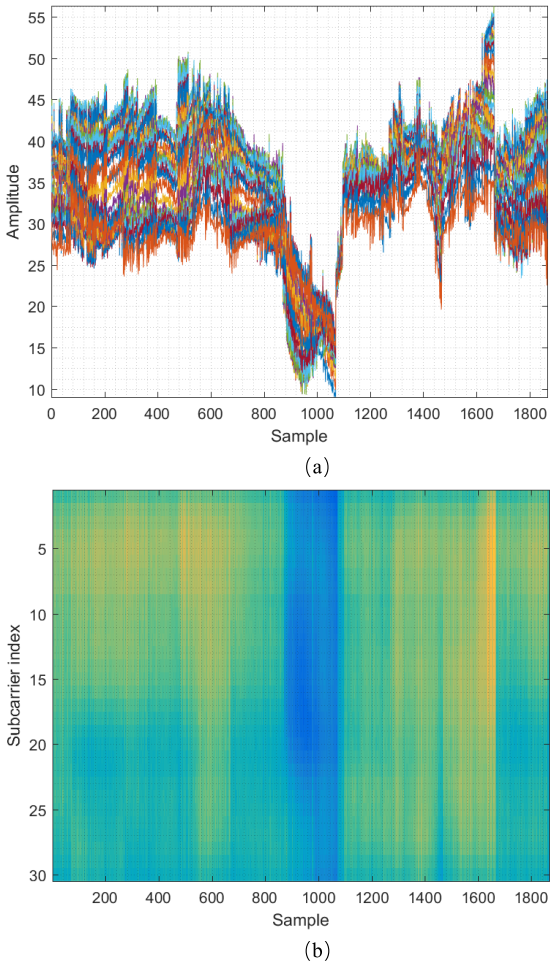


FIGURE 3. Illustration of the effect of gesture on CSI: (a) 30 subcarrier raw dat; (b) The data in (a) is converted to a different color by size.

We find that the amplitude of 30 subcarriers show a significant fall and rise trend (i.e. a valley)in the position of samples from 800 to 1200 in Fig. 3(a) when gesture passing through the first Fresnel zone. Meanwhile, the 30 subcarriers in Fig. 3(a) are strongly correlated during the gesture moving due to the synchronous amplitude variation. The data in Fig. 3(a) is converted to a different color by size in Fig. 3(b). The abscissa axis is also the number of samples, and the ordinate axis is 30 subcarriers. The intensity of the color indicates the magnitude of the subcarrier amplitude. Fig. 3(b) shows the blue ribbon appears due to the amplitude are fall and rise in the position of samples from 800 to 1200.

2) DETERMINE WHETHER THERE IS A LoS PATH

When AP behind the tester within 180 degrees range, due to the occlusion of the human body, the influence of gesture is not obvious. In other words, If the LoS path is blocked, the tester needs to turn back for obtaining the available data.

We find the CIR distribution between existence of LoS path and absence of LoS path is different. Due to the non-line of sight (NLoS) path has more delay than the LoS path, we can determine whether there is LoS path according to the delay distribution. We compare the CIR distribution between LoS path and NLoS path in Fig. 4. For each subgraph, the abscissa axis is the time delay and the ordinate axis is the amplitude corresponding to each delay in the time domain. The higher the amplitude value, the higher the energy carried by the signal arriving at that delay.

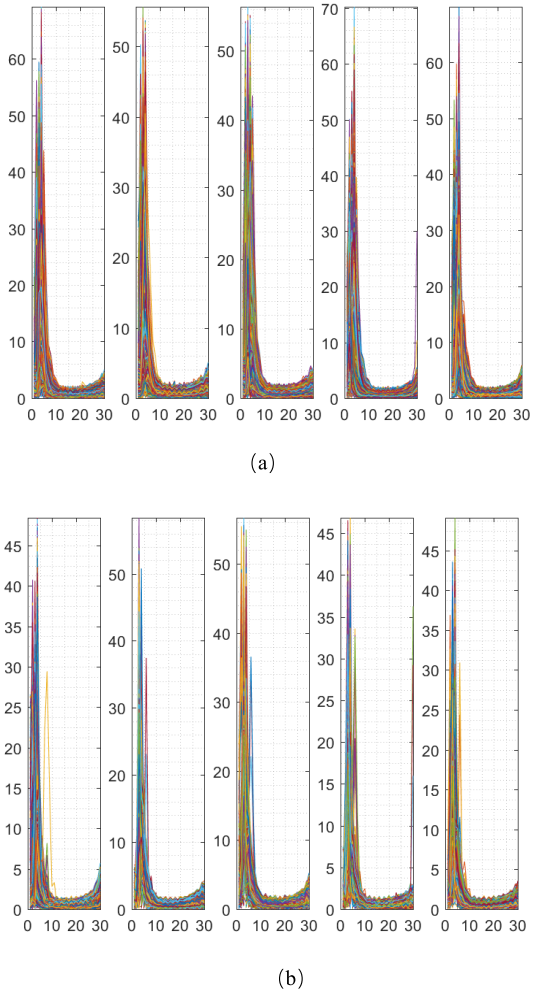


FIGURE 4. CIR comparison of LoS path and NLoS path for 5 times: (a) CIR distribution in the existence of LoS; (b) CIR distribution of the absence of LoS path (back to AP).

Comparing Fig. 4(a) with (b), we find that there will be at least one packet with higher energy outliers when absence of LoS path after about 4 × 50 ns. The occlusion of the human body during the radio propagation lead to this delay, we can identify such outliers through using the Local Outlier Factor (LOF) detection algorithm. The LOF algorithm can determine whether a data is an outlier by deriving the LOF value, which is suitable for data clusters based on different densities. The first 20 data of 5 × 50 ns and the subsequent delay in CIR are sorted in descending order as the input of the LOF algorithm. If the local outliers of the LOF algorithm are greater than 10, we consider this point to be an outlier, and we believe that the data collected is likely to be back to the AP when the number of outliers is greater than 5. The outlier points obtained by the outlier detection algorithm are shown in Fig. 5.

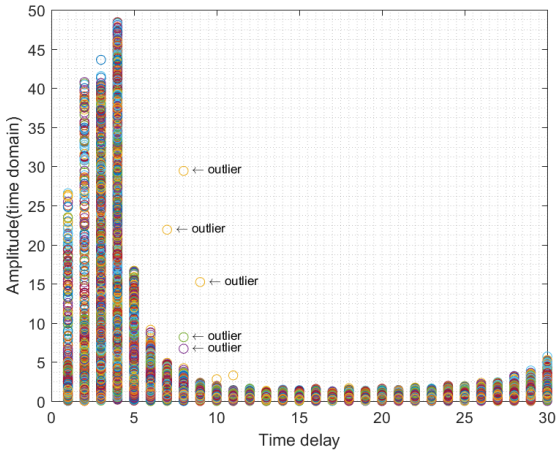


FIGURE 5. The outlier point which obtained by the outlier detection algorithm.

However, not all the NLoS paths appear outliers above mentioned, therefore we using the delay corresponding to the maximum amplitude of the three antennas to further address this problem as shown in Fig. 6. We find the maximum amplitude of LoS path in CIR is roughly concentrated at the delay of 4 × 50 ns as shown in Fig. 6(b), which can account for 98% of the total; the maximum amplitude of the NLoS path is still distributed at 5 × 50 ns and 6 × 50 ns after 4 × 50 ns, accounting for 41.67% of the total in Fig. 6(a). The delay of NLoS path is generally larger than the LoS path. We can take advantage of this character to further determine whether there is a LoS path.

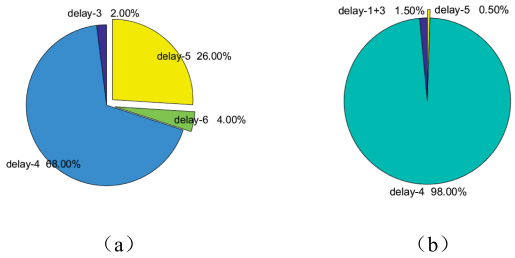


FIGURE 6. Distribution of CIR delay. 'delay-n' represents the position of the maximum amplitude of the three antennas in CIR at the delay n × 50ns. (a) The delay distribution of the maximum amplitude for NLoS path; (b) The delay distribution of the maximum amplitude for LoS path.

Further, we refer to the method in [24], which proposes that use Rician-K factor and skewness quantify the differences of the skewed envelope distribution under LoS and NLoS dominant conditions. The data flow gathering during the gesture movement is divided into slices so as to improve the precision and accuracy of LoS path identification.

D. IDENTIFY FRESNEL ZONE CUTTING POINTS

1) CSI PREPROCESSING

Raw CSI data from commercial WiFi device need to be denoised. We find that the DWT method is more efficient in eliminating noise than a simple discrete point removal filter or moving average filter in this scenario, which can extract totally the feature of CSI without losing important features in waveform.

The LoS path signal can be obtained by using CIR, which will mitigate the influence of channel environment such as multipath. However, the bandwidth of WiFi AP is set to 20MHz, then the time interval between neighbor subcarriers is $\frac{1}{20\text{MHz}} = 50\text{ns}$. Therefore, if the length of path is less than 15m, the multipath will be superimposed together to result in indistinguishable. The LoS path signal most likely travel directly to receiving end. In theory, the energy of LoS path signal that first arrived at the receiving end should be maximum, but the experiments show that it does not appear this feature. It may be due to the other electromagnetic interference or multipath in the real world. Therefore, we chose the path which has the maximum energy for further analysis. Since the CIR and CFR are the Fourier transform of each other, we use IFFT to transform the CFR in the frequency domain to the CIR in time domain. In this paper, we use the CFR data from one antenna pair for analysis.

Fig. 7 shows the CIR of a CSI stream when a single packet is converted to time domain using IFFT. The abscissa axis is time delay, and the ordinate axis is the amplitude value corresponding to each delay. The higher the amplitude value, the higher the energy carried by the signal arriving at the delay. The amplitude value in the time domain reaches the maximum at the delay of $4 \times 50\text{ns} = 200\text{ns}$ in Fig. 7, indicating that the signal energy arrives at this delay is the highest, most likely to be transmitted from the LoS path.

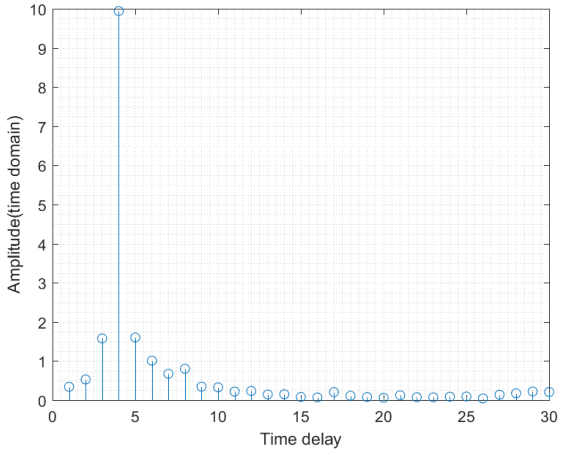


FIGURE 7. CIR image of a CSI stream when a single packet is converted to time domain.

The trend of the amplitude of the different paths over time are shown in Fig. 8. We find that the energy of the path first arrived at the receiving end is small and noisy in Fig. 8(a),

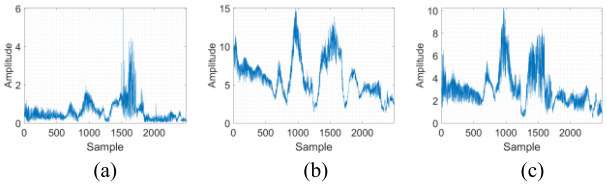


FIGURE 8. The trend of the amplitude of the different paths over time. (a) is the path arrived first at the receiver first; (b) is the path with the largest energy; (c) is the path has the second largest energy.

and the path with second maximum energy is also full of noise in Fig. 8(c), the maximum energy has the specific characteristic in Fig. 8(b).

To achieve a better denoising result, the DWT method is utilized to denoise the signal with maximum energy. We perform five-layer wavelet decomposition to get the coefficient of five layers of decomposed components (connected in a vector) and the length of each component. Then through reconstructing the five-layer approximation, the denoised data obtained. By using the DWT method for time-varying amplitude information, we can obtain the denoised waveform of amplitude information. The effect of denoising is shown in Fig. 9, where the blue line represents the original data and the red line represents the data after executing DWT method.

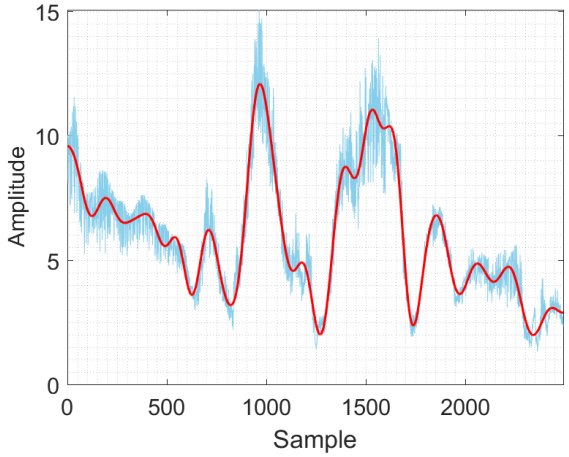


FIGURE 9. The effect of denoising using DWT.

2) PEAK AND TROUGH IDENTIFICATION

A linear fitting peak searching algorithm is proposed to extract the waveform information, where the sensitivity of the recognition is controlled by the critical value of the slope and the amplitude threshold. We can obtain the location, amplitude, peak width, duration, continuity and other parameters of the peaks and trough by combining the rising and falling of curves with the amplitude difference and the slope. We detect the valleys by looking for upward zero-crossings in the first derivative that exceed the critical value of the slope, and return a list containing valley number and position, depth, and width of each valley. The number points around the bottom

part of the valley are fitting to a parabola to determine the valley vertex and width. The position of peak is obtained using the similar method for finding valleys. We adopt the least squares linear fitting method, and use quadratic function and Gaussian function separately to derive a series of trough and peak points. Finally, we get the valley most likely to be cut in the first Fresnel zone, and get the Fresnel zone cutting point.

The effect of peak and trough identification method is shown in Fig.10. Fig. 11 further shows the accuracy of the peak and trough identification method. It can be found that the median accuracy of our method is 98.84%.

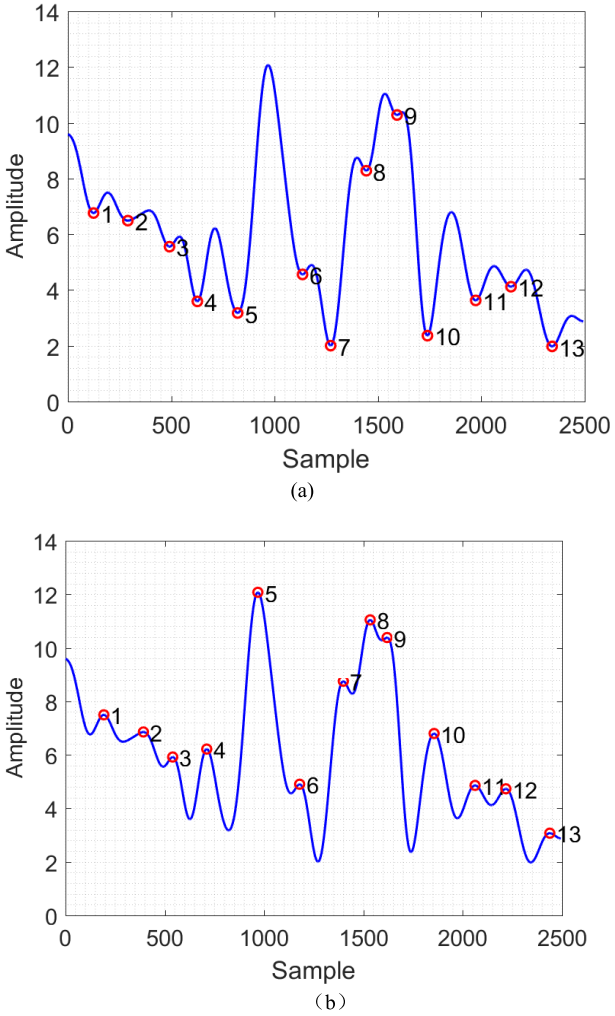


FIGURE 10. The effect of peak and trough Identification. The location and serial number of the peaks and troughs are marked with red circles and numerals. (a) is the trough we found; (b) is the peaks we found.

Many factors such as the amplitude of the peaks and troughs, the law of variation, etc. should be taken into account when we analyze the relationships between all the peaks and troughs, finally obtain a 'valley' and find the Fresnel cutting points as shown in Fig.12, the location of 'start' and 'stop' are the start and end point of the first Fresnel zone detected by our method.

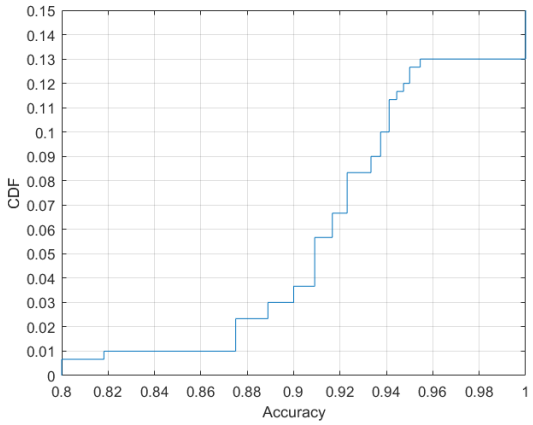


FIGURE 11. CDF of accuracy radio of the identification of peak and trough.

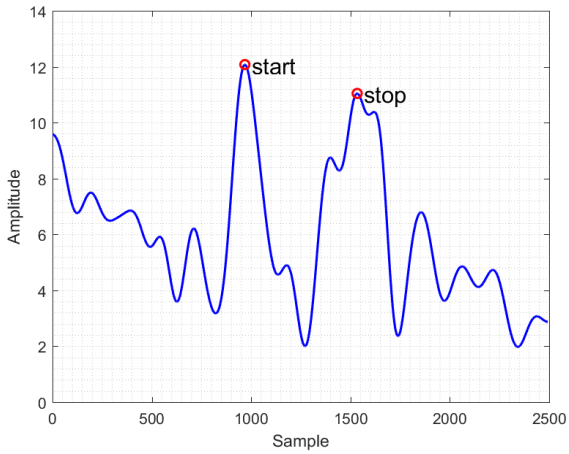


FIGURE 12. The Fresnel cutting points we found.

E. AP POSITIONING

1) DIRECTION DETERMINATION

We find the scope of the first Fresnel zone through the identification of the Fresnel zone cutting point, then determine whether the CSI characteristics generated during the gesture movement in the first Fresnel zone are in accordance with expectations, if it does match, we will export the percentage of the valley in the total data and derive the direction information.

However, there is no guarantee that the data gathering process with start/end exactly simultaneous with gesture movement process begin/stop. Therefore, there will be redundancy before and after the collected data and direct calculation will lead to an inaccurate result. Meanwhile, we find that the correlation of the 30 subcarriers in time domain shows a strong continuous rising trend during the moving of gesture in Fig. 13. We can determine the positions of the real start and end of the semicircle at the red dotted line in Fig. 13 by using this signal character.

We adopt sliding window to measure the correlation of subcarriers by using the sum of the standard deviations of the individual subcarriers in each window. The window with

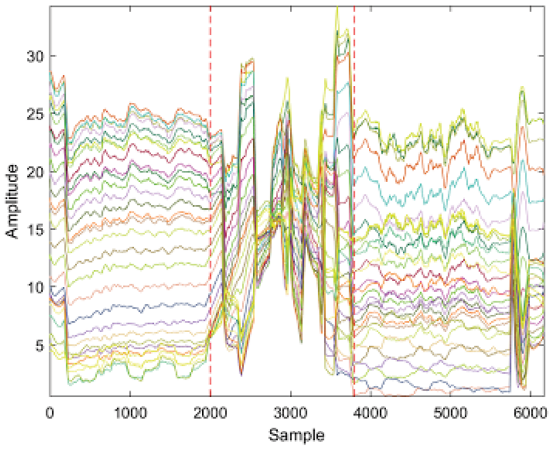


FIGURE 13. The correlation of the 30 subcarriers in the time domain show a strong continuous rising trend during the moving of gesture.

the gesture moving is the most relevant window which has maximum sum of standard deviation.

The correlation of the *j-th* window can be measured by the following formula:

$$\rho(\mathrm{j}) = \sum_{\mathrm{window\_init}}^{\mathrm{window\_end}} \sqrt{\frac{1}{\mathrm{S}-1}\sum_{\mathrm{k}=1}^{\mathrm{S}}(\mathrm{a(k)} - \frac{\sum_{\mathrm{i}=1}^{\mathrm{S}}|\mathrm{a(i)} - \frac{\sum_{\mathrm{t}=1}^{\mathrm{S}}\mathrm{a(t)}}{\mathrm{S}}|}{\mathrm{S}})^2} \tag{3}$$

Where both *window_init* and *window_end* are the start and end of the *j-th* window, and a(i) is the amplitude of the *i-th* subcarrier. S is the number of subcarriers, and in this case, S is 30.

2) POSITIONING

We can use the principle of Fresnel directly to calculate the distance from the AP, and then determine AP's position as shown in Fig. 14. The calculation formula is as following:

$$\sqrt{\mathrm{F_1^2}+\mathrm{d_1^2}}+\sqrt{\mathrm{F_1^2}+\mathrm{d_2^2}} = \mathrm{d_1}+\mathrm{d_2}+\lambda/2 = \mathrm{d}+\lambda/2 \tag{4}$$

Where F_1 is the radius of the first Fresnel zone, λ is the wavelength of subcarrier and d_1 and d_2 are the intermediate variables used to calculate d. If F_1, d_1 and λ are known, the distance d between the receiving end and the transmitting end can be obtained. The corresponding center angle θ is calculated from the percentage of the number of samples between the two Fresnel zone cutting points and the total number of samples in the process of drawing semicircle, combine with the radius of the semicircle R and trigonometric functions the F_1 can be calculated. However, in the case of fixing the transmitter, since the characteristics of the ellipse, the gap of θ between the different first Fresnel zone ellipse is small caused by the change of the focal length, result in the difference between the two Fresnel cutting points is very small. For an example, if the total number of samples is 2500,

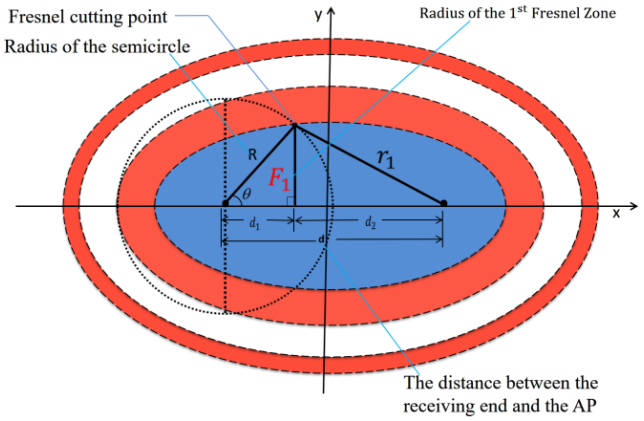


FIGURE 14. Calculate the distance using the Fresnel zone model.

the distance between transmitter and receiver are 100m and 10m corresponding the number of samples between Fresnel zone cutting point were 1292 and 1282 in theory, this 10 samples can cause a distance error of 90m.

In our method, the final position of AP is determined by using the coordinates of three positions combined with the direction of each position relative to the transmitter, and then using the weighted centroid algorithm. The final position (x_{final}, y_{final}) of the AP is calculated according to the following formula:

$$x_{\mathrm{final}} = \frac{\sum_{i=1}^{n}(x_i \times \sum_{j=i}^{m} d_j)}{m \times \sum_{i=1}^{n} d_i} \tag{5}$$

$$y_{\mathrm{final}} = \frac{\sum_{i=1}^{n}(y_i \times \sum_{j=i}^{m} d_j)}{m \times \sum_{i=1}^{n} d_i} \tag{6}$$

Whered_i is the maximum amplitude received from LoS path of each position. (x_i, y_i) is the intersection of the straight lines which determined by the coordinates of these positions and corresponding directions, three positions are used in this paper as shown in Fig. 15. The reason why the maximum amplitude of the LoS path is used as the weight is that it can be propagated through the LoS path without multipath affection, and fits to be the representative of the distance between the AP and receiver.

IV. PERFORMANCE EVALUATION

A. EXPERIMENTAL METHODOLOGY

1) EXPERIMENTAL SETUP

We use a laptop running the Ubuntu 12.04 operating system with the kernel version number 3.13.0 assembling an IWL 5300 wireless card with 802.11n Wi-Fi network, and a commercial wireless AP (TP-LINK TL-WR886N) to complete our experiment. The bandwidth is set to 20MHz. Each package includes 30 subcarriers. We use the ping

TABLE 1. The results of the LOS path identification method.

Evaluation Indicator	Formula	Percentage
True Positive Rate	$TPR = \frac{TP}{TP + FN}$	94%
True Negative Rate	$TNR = \frac{TN}{TN + FP}$	95%
False Positive Rate	$FPR = \frac{FP}{FP + TN}$	5%
False Negative Rate	$FNR = \frac{FN}{FN + TP}$	6%
Precision	$P = \frac{TP}{TP + FP}$	94.9%
Accuracy	$A = \frac{TP + TN}{TP + FN + FP + TN}$	94.5%

command to simulate the communication between the laptop and AP, where the data transfer rate is about 150 packets per second.

2) EXPERIMENTAL SCENARIOS

Our experiments are carried out in two classrooms, filling with desks and students who may sit there or walk around occasionally. This means that our experiments are surely affected by multipath interference. Since every classroom has its own wireless APs, The both adjacent classrooms will receive the interference of wireless signals from each other. The sizes of both classrooms are *16.3* m $\times$ *11.7* m and *11.6* m $\times$ *7.7* m respectively. In each classroom, we run multiple tests for our each experiment, taking into account the situation of the AP in all directions, including the AP in front, behind, right front, right rear, left rear, left front of the receiver.

B. LoS PATH IDENTIFICATION

Table 1 shows the statistic results of the LoS path identification method in 200 time tests.

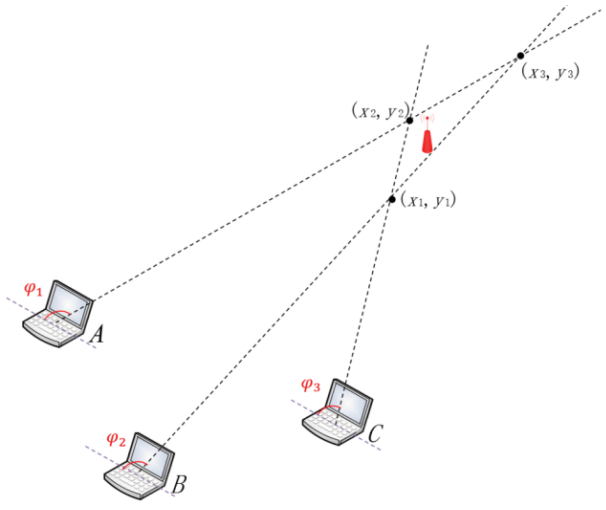


FIGURE 15. Position Estimation.

True Positive (TP) means that the NLoS sample is predicted as NLoS. True Negative (TN) means that the LoS sample is predicted as LoS. False Positive (FP) means that the LoS sample is predicted as NLoS. False Negative (FN) means that the NLoS sample is predicted as LoS. As we can find from Table 1, the accuracy and precision of this method on whether there is a LoS path are 94.5% and 94.9%. The performance was an improvement as compared to compare to an overall LoS identification rate of 90.4% with a false alarm rate of 9.3% achieved in [24].

C. DIRECTION ESTIMATION

Fig. 16 shows the angle value obtained after running 300 time tests. The reference angle is 90 degrees. We can find that the CSI-based deviation from the reference angle is quite small and stable comparing with RSS-based.

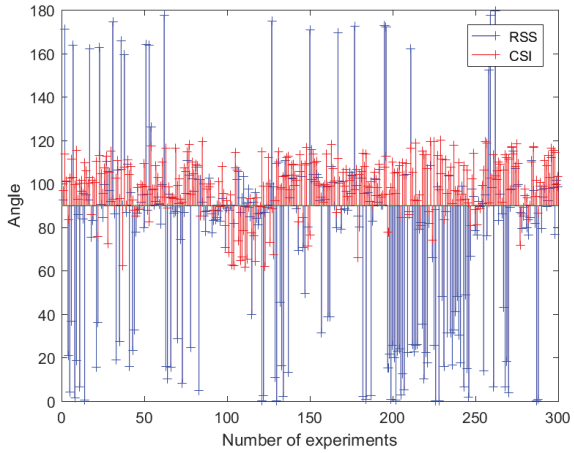


FIGURE 16. The distribution of angle.

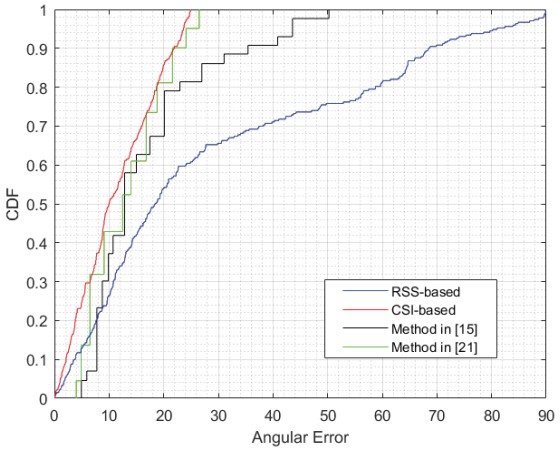


FIGURE 17. The CDF of angle errors.

Fig. 17 shows the CDF of the angular determination errors. For CSI-based method, the average error is about 11.29 degrees, the median error is about 9.98 degrees, the maximum error is 24.90 degrees, 90% errors are less than 23 degrees. Comparing with RSS-based method, the average error is about 29.05 degrees, the maximum error is

89.87 degrees, the median error is 29.05 degrees. The performance of CSI-based method has more improvement than CSI-based method. Besides, we compare our method with the method in [15] and [21] also shown in Fig. 17. It is obvious that our method can achieve a smaller angular error than the method in [15] and [21]. Importantly, our algorithm is more simpler, which does not require people to stand in a specific location and walk along a specific route.

D. POSITION ESTIMATION

As shown in Fig. 18, the maximum error of our CSI-based algorithm is 8.25m, the average error is 0.99m, the median error is 0.58 m,and over 90% of the errors are less than 2.5m. Comparing with the RSSI channel log attenuation model proposed in [5], the distance error is 617.17m, the average error is 17.30m, the mean of error is 4.08m. Our method has a much better positioning performance than RSS based method.

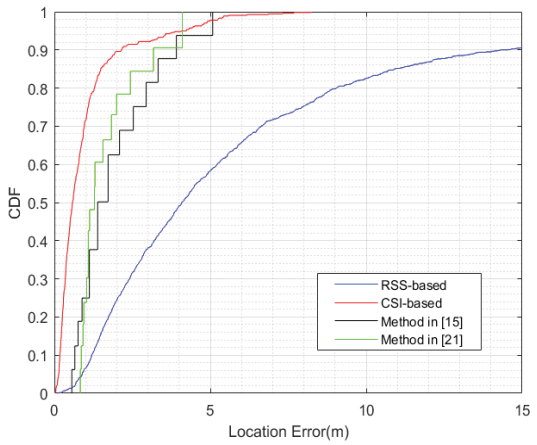


FIGURE 18. The CDF of distance errors.

Our algorithm comparing with the method in [15] and [21] is also shown in Fig. 18. Our method converges faster than the method in [15] and [21] and can achieve a lower positioning error, Such as our median error of 0.58m lower than 1.06m in [15] and 3.5 feet in [21]. Meanwhile, our method has a simpler implementationas mentioned above. Although Awad *et al.* [23] achieve a lower localization error, it depends on at least one robot and the execution time takes a minimum of 18 min. Besides, the Particle Swarm Optimization method in [22] is a RSS-based AP positioning depending on the sample set size and need a legitimate access point with a known location. the performance of their algorithm gets the best result when the sample set size is 60, the positioning error is 0.7m. Our positioning error is smaller, and our implementation does not need any prior knowledge of the environment.

V. CONCLUSION

In this paper, an AP positioning algorithm based on channel state information and Fresnel zone is proposed, which can just draw a semicircle with one hand to estimate the AP location. We use a single receiver to measure the CSI information without high infrastructure cost and extensive labor. Based on the CSI character of moving hand through Fresnel Zone, we can compute the AP direction firstly, and then determine the AP location combining with the AP directions computed in any three positions. Our algorithm includes two phase: preparations and AP positioning. Preparations include both calibrating AP direction and identifying Fresnel zone cutting points. AP positioning includes both AP direction determination and AP position determination. Our experiment results show that the accuracy and precision of our method on whether there is a LoS path are 94.5% and 94.9%, and the median error is about 9.98 degrees of the CSI-based angle determination method, meanwhile, the median positioning error is 0.58 m, and about 90% of the positioning errors are less than 2.5m. Our algorithm taking advantage of finer-grained CSI and Fresnel characteristic has a significant improvement than other methods.

REFERENCES

[1] K. Gopalakrishnan, M. Govindarasu, D. W. Jacobson, and B. M. Phares, "Cyber security for airports," *Int. J. Traffic Transport Eng.*, vol. 3, no. 4, pp. 365–376, 2013, doi: 10.7708/ijtte.2013.3(4).02.

[2] L. Ma, A. Y. Teymorian, and X. Cheng, "A hybrid rogue access point protection framework for commodity Wi-Fi networks," in *Proc. IEEE 27th Conf. Comput. Commun. (INFOCOM)*, Phoenix, AZ, USA, Apr. 2008, pp. 1220–1228.

[3] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, "A timing-based scheme for rogue AP detection," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 11, pp. 1912–1925, Nov. 2011, doi: 10.1109/TPDS.2011.125.

[4] D. Schweitzer, W. Brown, and J. Boleng, "Using visualization to locate rogue access points," *J. Comput. Sci. Colleges*, vol. 23, no. 1, pp. 134–140, 2007.

[5] J. Park, S. Kang, S. Kim, and W. Lee, "A study of estimation of ap position for improvement of indoor positioning performances," *Int. J. Control Automat.*, vol. 5, no. 2, pp. 73–80, Jun. 2012.

[6] Z. Zhang *et al.*, "I am the antenna: Accurate outdoor ap location using smartphones," in *Proc. 17th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, Las Vegas, NV, USA, 2011, pp. 109–120.

[7] K. Wu, J. Xiao, Y. Yi, M. Gao, and L. M. Ni, "FILA: Fine-grained indoor localization," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Mar. 2012, pp. 2210–2218.

[8] F. Adelstein, P. Alla, R. Joyce, and G. G. Richard, "Physically locating wireless intruders," in *Proc. Int. Conf. Inf. Technol., Coding Comput.*, Las Vegas, NV, USA, Apr. 2004, pp. 482–489.

[9] S. F. A. Shah, S. Srirangarajan, and A. H. Tewfik, "Implementation of a directional beacon-based position location algorithm in a signal processing framework," *IEEE Trans. Wireless Commun.*, vol. 9, no. 3, pp. 1044–1053, Mar. 2010, doi: 10.1109/TWC.2010.03.081204.

[10] A. P. Subramanian, P. Deshpande, J. Gao, and S. R. Das, "Drive-by localization of roadside WiFi networks," in *Proc. 7th Conf. Comput. Commun. (INFOCOM)*, Phoenix, AZ, USA, Apr. 2008, pp. 718–725.

[11] D. Han, D. G. Andersen, M. Kaminsky, K. Papagiannaki, and S. Seshan, "Access point localization using local signal strength gradient," in *Proc. 10th Int. Conf. Passive Act. Netw. Meas.*, Seoul, South Korea, 2009, pp. 99–108.

[12] T. M. Le, R. P. Liu, and M. Hedley, "Rogue access point detection and localization," in *Proc. IEEE 23rd Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Sydney, NSW, Australia, Sep. 2012, pp. 2489–2493.

[13] M. A. Gonzalez, J. Gomez, M. Lopez-Guerrero, V. Rangel, and M. M. de Oca, "GUIDE-gradient: A guiding algorithm for mobile nodes in WLAN and ad-hoc networks," *Wireless Pers. Commun.*, vol. 57, no. 4, pp. 629–653, Apr. 2011, doi: 10.1007/s11277-009-9865-2.

[14] J. Wilson and N. Patwari, "See-through walls: Motion tracking using variance-based radio tomography networks," *IEEE Trans. Mobile Comput.*, vol. 10, no. 5, pp. 612–621, May 2011, doi: 10.1109/TMC.2010.175.

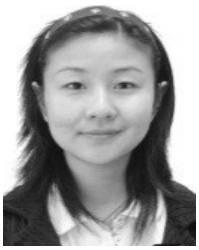
[15] X. Zheng, C. Wang, Y. Chen, and J. Yang, "Accurate rogue access point localization leveraging fine-grained channel information," in *Proc. Commun. Netw. Secur. (CNS)*, San Francisco, CA, USA, Oct. 2014, pp. 211–219.
[16] S. Sen, R. R. Choudhury, and S. Nelakuditi, "SpinLoc: Spin once to know your location," in *Proc. 12th Workshop Mobile Comput. Syst. Appl. (HotMobile)*, San Diego, CA, USA, Feb. 2012, pp. 1–6.
[17] K. Wu, J. Xiao, Y. Yi, D. Chen, X. Luo, and L. M. Ni, "CSI-based indoor localization," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 7, pp. 1300–1309, Jul. 2012, doi: 10.1109/TPDS.2012.214.
[18] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Predictable 802.11 packet delivery from wireless channel measurements," in *Proc. ACM SIGCOMM Conf.*, New Delhi, India, Aug./Sep. 2010, pp. 159–170.
[19] J. Wang *et al.*, "LiFS: Low human-effort, device-free localization with fine-grained subcarrier information," in *Proc. 22nd Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, New York, NY, USA, Oct. 2016, pp. 243–256.
[20] Z. Li, T. Braun, and D. C. Dimitrova, "A passive WiFi source localization system based on fine-grained power-based trilateration," in *Proc. IEEE 16th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Boston, MA, USA, Jun. 2015, pp. 1–9.
[21] C. Wang, X. Zheng, Y. Chen, and J. Yang, "Locating rogue access point using fine-grained channel information," *IEEE Trans. Mobile Comput.*, vol. 16, no. 9, pp. 2560–2573, Sep. 2017, doi: 10.1109/TMC.2016.2629473.
[22] F. Awad, M. Al-Refai, and A. Al-Qerem, "Rogue access point localization using particle swarm optimization," in *Proc. Inf. Commun. Syst. (ICICS)*, Irbid, Jordan, Apr. 2017, pp. 282–286.
[23] F. Awad, M. Naserllah, A. Omar, A. Abu-Hantash, and A. Al-Taj, "Collaborative indoor access point localization using autonomous mobile robot swarm," *Sensors*, vol. 18, no. 2, p. 407, Jan. 2018, doi: 10.3390/s18020407.
[24] Z. Zhou, Z. Yang, C. Wu, W. Sun, and Y. Liu, "LiFi: Line-of-sight identification with WiFi," in *Proc. 33rd IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Toronto, ON, Canada, Apr./May 2014, pp. 2688–2696.

YONGLE CHEN was born in Weifang, China, in 1983. He received the B.S. degree in computer science from Jilin University in 2007, the M.S. degree in computer science from the Institute of Software, Chinese Academy of Science, in 2009, and the Ph.D. degree in computer science from the University of Chinese Academy of Sciences in 2013.

From 2013 to 2015, he was an Assistant Professor with the College of Computer Science and Technology, Taiyuan University of Technology, Taiyuan, China, where he has been an Associate Professor since 2015. His research interests are wireless sensor networks, indoor positioning, and Internet of Things security.

XIAOJIAN WANG was born in Yuncheng, China, in 1995. She received the B.S. degree in Internet of Things (IoT) engineering from the Taiyuan University of Technology, Taiyuan, China, in 2017, where she is currently pursuing the M.S. degree.

Her research interests are indoor positioning and IoT security.



DAN YU was born in Taiyuan, China, in 1983. She received the B.S. degree in electronic engineering from the North University of China in 2007 and the M.S. degree in electronic engineering from the Beijing University of Posts and Telecommunications in 2013.

She is currently pursuing the Ph.D. degree with the College of Computer Science and Technology, Taiyuan University of Technology, Taiyuan. Her research interests are wireless sensor networks and Internet of Things.

YULI YANG was born in Yicheng, China, in 1979. She received the M.S. degree in computer science and technology from Guangxi Normal University, China, in 2007, and the Ph.D. degree in computer science and technology from the Taiyuan University of Technology, Taiyuan, China, in 2015.

She is currently a Lecturer with the College of Computer Science and Technology, Taiyuan University of Technology. Her research interests are related with computer network security, cloud computing, and trust management.

JIAN CHEN (M'08) received the B.S. degree from the North University of China, China, in 1990, the M.S. degree from The University of Aizu, Japan, in 2003, and the Ph.D. degree from Waseda University, Japan, in 2012. In 2013, he joined the Taiyuan University of Technology, where he involved extensively in research works in the fields of computer science and information systems involved social and human informatics and currently an Associate Professor with the College of Big Data. His recent research interests cover ubiquitous computing, behavior and cognitive informatics, user modeling, information retrieving and recommendation, and computing for pattern recognition. He is a member of IPSJ and CCF.