Accurate Rogue Access Point Localization Leveraging Fine-grained Channel Information

Xiuyuan Zheng[1], Chen Wang[1], Yingying Chen[1], Jie Yang[2]
[1]Department of ECE, Stevens Institute of Technology, Hoboken, NJ 07030
{xzheng1, cwang42, yingying.chen}@stevens.edu
[2]Department of Computer Science, Florida State University, Tallahassee, FL 32306
jie.yang@cs.fsu.edu

***Abstract*—Rogue access point (AP) has emerged as an important security problem in WLANs. However, it is a challenge task to localize the rogue AP with both high accuracy and minimal infrastructure cost. Either expensive professional infrastructure (e.g., multiple wireless sniffers) or additional hardware (e.g., directional antenna) need to be pre-deployed for rogue AP localization with high cost. Moreover, existing methods using Received Signal Strength (RSS) result in large error as RSS is suffered from the multipath and shadowing effects in complex wireless environment. In this work, we exploit the channel state information (CSI), which is readily available from commercial Wi-Fi devices, to locate the rogue AP with high accuracy. We use only a single off-the-shelf Wi-Fi device for rogue AP localization which involves minimal infrastructure requirement. Our proposed rogue AP localization framework consists of two components: direction determination and position estimation. By characterizing time domain CSI amplitude, we develop direction determination approach to estimate the direction of the rogue AP at the Wi-Fi device. We further propose two schemes to estimate position of the rogue AP: directions determined at multiple locations grounded on triangulation, or walking towards the rogue AP with direction adjustment. Results from extensive experiments in both indoor and outdoor environments show that our framework can achieve more practical and accurate rogue AP localization when comparing with existing RSS-based approach.**

I. Introduction

With the rapid advancement of wireless technologies, wireless networks play an increasingly important role in our daily lives. For example, the wide deployment of Wi-Fi Access Points (APs) enables any-time any-where Internet access in public places, offices and homes. While the mobile device users (e.g., smartphone, tablet and laptop) enjoy the convenience of accessing the Internet through the increasingly pervasive Wi-Fi APs, the security and privacy issues can become a barrier for the successful deployment of Wi-Fi networks. In particular, the emergence of rogue Access Points (i.e., rouge APs) brings significant security and privacy threats in wireless local area network (WLAN) [1], [2]. A rogue AP is an unauthorized access point not deployed by the WLAN administrator but created by an adversary to conduct a man-in-the-middle attack [3]. The rogue AP is usually equipped with two wireless cards, one is connected to an authorized legitimate AP and the other is configured as an AP for users to connect to [4]. The rogue AP can thus eavesdrop the wireless communication and make the users to believe that they are connected to the legitimate AP. It has been estimated that almost 20% of corporations have rogue APs in their networks, which opens up the network to a number of targeted cyber-attacks [5], [6].

A rogue AP is easy to setup, for example, an attacker can simply configure a laptop as a rogue AP to mimic the legitimate AP in public places, such as fast food restaurants (e.g., MacDonald's), cafes (e.g., Starbucks), airport lounges and hotels. The rogue AP can passively wait for users to connect to, or actively send out a disassociation frame to force user to switch the connection from a legitimate AP to a rogue AP. And the rogue AP usually performs further configurations to reduce the chance to be detected including spoofing MAC address and SSID and setting up a DHCP server to assign valid IP addresses to the connected users [4]. Once the users connect to a rogue AP, the attacker can intercept and manipulate the wireless communications and in the meanwhile providing Internet access for the connected users. By intercepting and manipulating the wireless communication, the attacker can further conduct a variety of malicious attacks [3] including launching phishing attacks by redirecting an user's webpage to a fake one so that to steal the user's private information (bank account and password for example).

There have been active work in detecting rogue AP by either using the fingerings of legitimate APs [1], [7], or by analyzing the network traffic at the gateway [8], or by measuring the connection time at wireless users [9]. In this paper, we take the view point on how to locate the rogue AP's position after detecting its presence. Knowing the location of the rogue AP allows the network administrator to further exploit a wide range of defense strategies. For example, we can physically visit the rogue AP and eliminate it from the network. Existing work in locating a rogue AP are usually based on the measured signal strength of the wireless signal emitted from the rogue AP. For example, by deploying multiple sniffers or specialized hardware (e.g., directional antenna) in the area of interest, the location of the rogue AP can be estimated based on the received signal at multiple sniffers [10]. Or the administrators can hold a wireless sniffer and walk towards the direction with decreasing signal power to reach the rogue AP [11]. However, deploying multiple sniffers and dedicated hardware involves high infrastructural cost and extensive labor, especially in a large organization. Furthermore, it is well-known that the RSS is significantly affected by the multipath and shadowing effects in a complicated indoor environment. As a result, the places received stronger signal strengths do not necessarily mean they are closer to the rogue AP. Thus, the RSS based rogue AP localization methods suffer from poor accuracy, involve more time and effort, or even fail to pinpoint the rogue AP.

In this work, we use only a single wireless device and exploit the Channel State Information (CSI) available from commercial Wi-Fi devices to locate the rogue AP. CSI can be obtained from the subcarriers on Orthogonal Frequency Division Multiplexing (OFDM), which is commonly used in wireless communication systems (such as IEEE 802.11 a/g/n, WiMAX). The detailed channel response from multiple OFDM subcarriers is a suitable candidate to achieve accurate location estimation of rogue AP. Different from having only one RSS value per packet, we can obtain multiple channel responses from each wireless packet including amplitude and phase at each OFDM subcarrier. CSI thus provides fine-grained information when comparing to RSS and allows to obtain more accurate localization results.

Our basic idea is to determine the direction of the rogue AP leveraging CSI by using a single Wi-Fi device. Specifically, we find that the CSI received by the wireless device (e.g., laptop or smart phone) will be significantly affected by a blocking object (e.g., the user) when the user stands in-between the wireless device and the rogue AP. Toward this end, we capture this phenomenon to facilitate estimating the direction of the rogue AP utilizing CSI amplitude in time domain. Grounded on the CSI-based direction determination technique, we derive two position estimation methods: *geometric relationship based* and *obstacle avoidance direction adjustment*. The *geometric relationship based* approach is to directly pinpoint the rogue AP's position using triangulation based on the directions determined from a few locations using a Wi-Fi device. And the *obstracle avoidance direction adjustment* is to walk towards the rogue AP via continuous direction adjustment while the user encounters an obstacle. Our framework can be used by either the network administrator or WiFi users for locating the rouge AP. The involvement of the users could prevent a variety of adversarial activities (e.g., private information leakage). Certain rewards (e.g., points, virtual currency) can be used to compensate the users who actively participate in locating the rouge AP [12]. Note that our framework can be easily extended to facilitate the localization of legitimate APs or wireless emitters.

We summarize the main contributions of our work as following:

- We utilize CSI, which is a fine-grained physical layer information provided by commercial Wi-Fi cards, to locate the rogue APs. Different from existing received signal strength (RSS) based methods, CSI provides richer information to characterize the wireless channel, and makes it possible for more accurate and practical rogue AP localization.
- We capture the "blocking" effect on CSI amplitude when an object standing between a wireless device and the rogue AP and utilize this important phenomenon to derive the direction of the rogue AP. New techniques are developed to examine the CSI amplitude in time domain by conducting amplitude correlation and orthogonal transformation to determine the direction of the rogue AP.
- We develop a user-centric framework to localize the rogue AP in two ways. One is to utilize the spatial diversity by performing direction determination at multiple locations to enable the Wi-Fi user to pinpoint the rogue AP's position, and the other is to let the user walk towards the direction of the AP to finally reach it, in which we perform direction adjustment to deal with obstacles encountered along the way.
- We conduct comprehensive experiments in both indoor and outdoor environments to validate the proposed framework. Comparing with existing RSS-based direction determination, we show that our approach is highly effective to determine the rogue AP's direction by achieving over 40% reduction in maximum error and 60% in median error in both environments. This facilitates higher accuracy of the location estimation of the rogue AP.

The rest of the paper is organized as follows. In Section II, we present the related studies. We then describe our framework in Section III. In Section IV, we present the blocking effect on CSI. We detail our direction determination scheme in Section IV and further develop two position estimation methods in Section VI. We conduct experiments and evaluate our proposed framework in Section VII. Finally, we conclude our work in Section VIII.

II. Related Work

Existing work on rogue AP detection can be classified into three categories. The first category of the work utilizes wireless sniffers to capture the fingerprint of an AP (such as SSID, MAC address [1], and RSS values [7]) for rogue AP detection. And the radio frequency variations [13], and clock skews [14] have been proposed as well for building the fingerprint of an AP. The second category of the work is to analyze network traffic at the gateway to detect if the associated AP is a rogue one [8], [9]. For instance, the temporal characteristics, such as inter-packet arrival time [8] is first proposed to detect rogue APs. The last category of the work utilizes the basic information that the rogue APs are in the middle of users and the real AP for attack detection. The connection time or wireless hop is utilized to detect the presence of rogue APs since the wireless hops for a user to access Internet increase under rogue AP attack [3], [4]. These rogue AP detection techniques can be utilized by our framework to detect the rogue APs prior to localize them.

There has been active work on localizing APs. They either utilize RSS [10], [11], [15]–[18], or leverage additional hardware [19], [20], i.e., directional antenna, for AP localization. The RSS-based approaches assume that a location closer to the AP will have a higher RSS value. One commonly used method for localizing rogue AP is to hold a wireless sniffer and walking along the direction with decreasing signal power to reach the rogue AP [11]. Or with multiple wireless sniffers in an area of interest, a signal contour map can be built in order to locate the rogue AP [10]. For localizing legitimate APs, existing RSS-based approaches compute the gradient of the RSS value across different locations either with a small set of local measurements online [16], or by integrating the results of a large number of measurements offline [17]. However, all of these RSS based approaches either result in relatively large localization errors due to the complicated indoor signal propagation environments or involve intensive labor due to signal map construction.

One recent work proposes to use human body as an obstacle to block the wireless receiver at different directions, and the direction of the AP can be determined when the signal strength has the largest degradation [18]. However, it cannot work

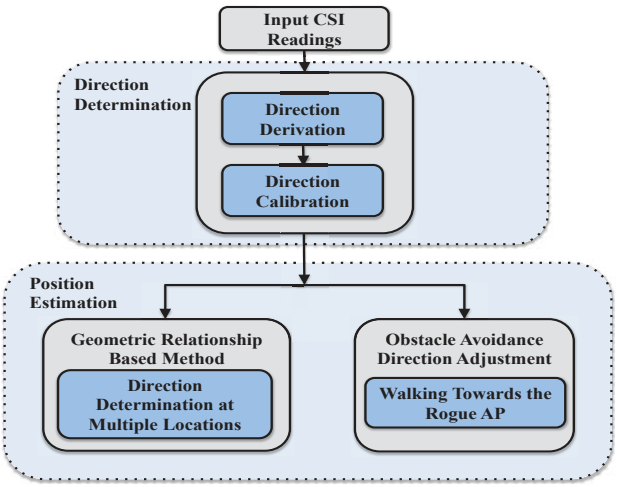


Fig. 1. Framework overview.

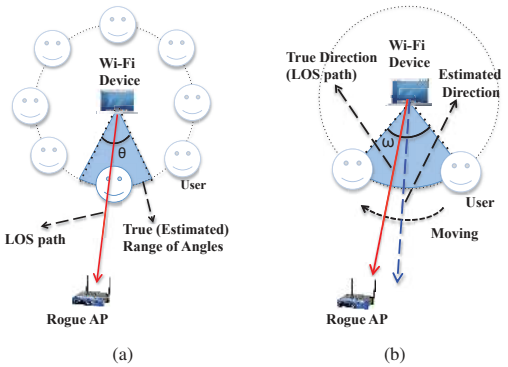


Fig. 2. Illustration of direction determination: (a) Direction Derivation: user stands at eight different positions around the laptop; (b) Direction Calibration: user moves across an arc which covers an angle range obtained by direction derivation.

in complicated indoor environments and the performance in outdoor environments still have large room for improvement. Further, the work that uses additional hardware, i.e., directional antenna, either at the receiver or transmitter, to locate the APs [19], [20] involves higher infrastructural cost and is neither scalable nor portable. Different from the above work, we perform rogue AP localization with high accuracy in both indoor and outdoor environments by exploiting CSI which provides richer channel information than that of RSS. Our method is cost saving as it uses only one off-the-shelf Wi-Fi device without requiring additional hardware.

III. Framework of CSI-based Rogue AP Localization

In this section, we first provide the motivation of using CSI for rogue AP localization. We then present the overview of our proposed CSI-based rogue AP localization framework.

A. Motivation

We exploit CSI, the fine-grained description of the wireless channel, measured from OFDM subcarriers to perform rogue AP localization. OFDM techniques have been extensively used in wireless systems, such as IEEE 802.11a/g/n, WiMAX and 3G LTE, to improve the communication performance. CSI thus becomes available at commercial wireless devices. For example, the firmware of IWL 5300 wireless card exports the frequency response as complex vectors over 30 subcarriers [21]. Different from the traditional RSS, which is an averaged signal power over all the subcarriers with only one value per packet, CSI provides multiple channel responses from each packet including amplitude and phase at each of the 56 (128) OFDM subcarriers on standard 20 (40) MHz channel. It describes how the signal propagates from the transmitter to the receiver and reveals the impact of multipath effect on each of the subcarriers instead of the coarse-grained impact on the whole channel bandwidth as the RSS does. We thus expect CSI to better describe the wireless channel than RSS, especially in complex indoor environments when the multipath dominates the signal propagation.

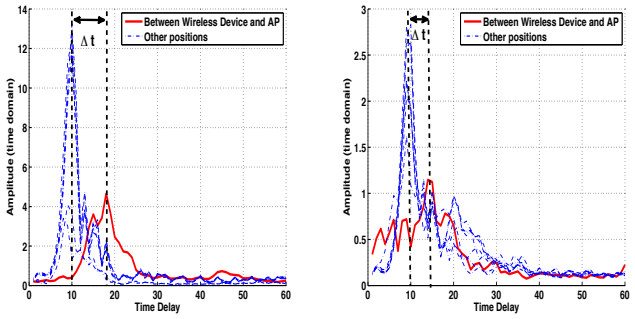
B. Framework Overview

Our basic idea is to determine the direction of the rogue AP via CSI measured at a single Wi-Fi device as knowing the direction of the AP can be the first step toward estimating the AP's position. Specifically, we find that the CSI measured at the Wi-Fi device (e.g., laptop or smart phone) will be significantly affected by a blocking object (e.g., the user) in-between the Wi-Fi device and the rogue AP. By standing at multiple positions around the Wi-Fi device, the different blocking effects captured by CSI can be used to estimate the direction of the rogue AP in both indoor and outdoor environments. We derive techniques utilizing CSI amplitude in time domain to capture such effects for direction estimation. Determination of the direction of the rogue AP can facilitate our system to localize the rogue AP in two ways. We can either directly pinpoint the rogue AP based on the direction determination at multiple locations using triangulation. Or we can walk towards the rogue AP by adjusting walking direction when the user encounters permanent obstacles such as walls or furnitures. Note that our framework can also localize legitimate APs or wireless emitters.

Our rogue AP localization framework consists of two main components as shown in Figure 1: *direction determination* and *position estimation*.

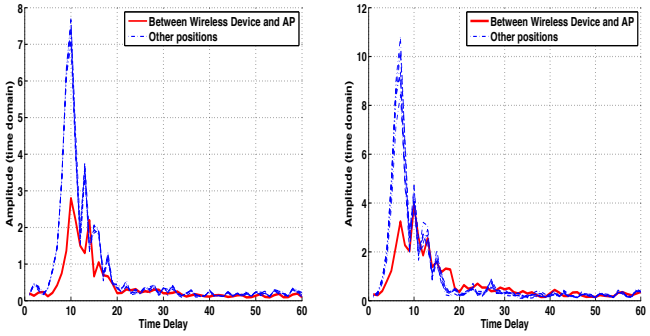
Direction Determination. We propose a two-step approach to determine the direction of the rogue AP: (1) *direction derivation* and (2) *direction calibration*. At the first step, the user stands at multiple positions around the wireless device as shown in Figure 2 (a). By analyzing the CSI obtained from different standing positions, we can derive one standing position that has the most significant impact to the wireless channel. The angle range derived by this standing position indicates the rough direction of the rogue AP. In order to further obtain the accurate direction of the rouge AP, in the second step the user moves across the arc of the angle range slowly as shown in Figure 2 (b) based on the rough direction determined by the first step. We expand the angle range obtained from the first step to its left and right side to tolerant possible estimation error from the first step. By analyzing the continuously collected CSI data when the user moves slowly across the arc, we are able to narrow down the range of angles, and derive an accurate angle pointing towards the rogue AP.

Position Estimation. Based on the results of direction determination, we develop two methods to estimate the rogue AP's postion to meet user's different requirements. The first method, *geometric relationship-based*, is to perform direction determination at multiple locations to enable the user to directly



(a) Indoor (b) Outdoor

Fig. 3. CSI amplitude in time domain at eight different positions around the wireless device: time delay phenomenon in *simple* wireless environments.



(a) Indoor (b) Outdoor

Fig. 4. CSI amplitude in time domain at eight different positions around the wireless device: time delay phenomenon in *complex* wireless environments.

obtain the position of rogue AP. At each position, the user with the Wi-Fi device can obtain an estimated direction towards the rogue AP based on the direction determination approach. One straight line can be uniquely determined by the direction starting from the device's physical location. Thus, we can find the rogue AP's position by averaging the intersections of these straight lines using triangulation. The second method, *obstacle avoidance direction adjustment*, is to let the user walk towards the rogue AP following the direction determination result of a single Wi-Fi device. We design direction adjustment scheme to guide the user's walking direction when the user encounters permanent obstacles (e.g., doors, buildings, etc.), since the permanent obstacles cause signal reflections and degradations, and may deviate the true direction of the rogue AP.

IV. Blocking Effect on CSI

In this section, we discuss how the CSI measured at the Wi-Fi device is affected by the user standing at different positions around the Wi-Fi device.

Time Delay When Blocking the Line of Sight (LOS). Given the CSI measured at each subcarrier in frequency domain, we can obtain the time domain CSI by applying the n-point Inverse Fast Fourier Transform (IFFT). In this work, we apply a 60-point IFFT, which provides an appropriate time resolution for our investigation. The commonly used CSI in time domain is described as:

$$h(\tau) = \sum_{i=1}^{N} a_i e^{-j\theta_i} \delta(\tau - \tau_i), \quad (1)$$

where N is the number of multipath channel components, a_i, θ_i and τ_i are the amplitude, phase and the propagation time delay of the ith path, and $\delta(\tau)$ is the Dirac delta function.

The curves in Figure 3 describe the CSI amplitude with different time delays when the user stands at different positions as shown in Figure 2 (a) with LOS existing between the rogue AP and the Wi-Fi device. In particular, the red solid curve shows the case when the user stands at the position blocking the LOS, whereas the dash curves indicate the cases when the user stands at other positions. We observe in Figure 3 that the CSI amplitude in time domain have multiple amplitude peaks with different time delays. The strongest peak represents the signal arrived through the LOS path since the signal propagating through the LOS path carries most of the power in the received signal. And the smaller amplitude peaks at later times indicate that the reflected signals transmit through longer reflection paths.

More importantly, we observe from Figure 3 in both indoor and outdoor environments that the strongest peak of the received signal is significantly delayed when the user stands in-between the wireless device and the rogue AP (curve in red) compared to other user positions (curves in blue). This is because the user standing in-between the wireless device and the rogue AP blocks the direct path of the signal transmission. Thus a larger portion of signals transmit through the indirect and longer propagation paths. In other words, the reflected signal transmitted through multipath takes more time to arrive at the wireless device. This phenomenon is presented in both indoor and outdoor environments when the LOS path is blocked. We utilize this important observation as the basis to derive the direction of the rogue AP.

Capturing Time Delay Using Amplitude Correlation. We find however the time delay phenomenon may not be obvious in complex indoor environments when no LOS exists and the multipath dominates the signal propagation. Figure 4 shows a scenario that there is no obvious time delay at the strongest peak. We find that this happens mostly in complex wireless environments, i.e., indoors with many permanent infrastructures, or outdoor environments with people blocking the LOS path. Due to the complex wireless environment, the time delay phenomenon may be shifted and observed at the smaller amplitude peaks.

In order to capture the time delay phenomenon in both simple and complex environments, we explore to use amplitude correlation instead of directly examining the time delay of the strongest CSI amplitude for direction determination. This is because the CSI amplitude obtained from different standing positions tend to be more correlated with each other as long as the user is not blocking the direct path between the wireless device and the rogue AP. In particular, as shown in Figure 3 and 4, the correlation between the blue curves is over 90%. On the other hand, the CSI amplitude when the user stands in-between the wireless device and AP (curve in red) tends to be less correlated to other user positions (curves in blue). The correlation is less than 60% as shown in Figure 3 and 4. These observations enable us to derive the direction of the rogue AP by utilizing amplitude correlation at different user positions.

V. Direction Determination

In this section, we present the proposed two-step approach for determining the direction of the rogue AP: (1) *direction*

derivation and (2) *direction calibration*.

A. Direction Derivation

As the first step, the user identifies the standing position that has the most significant impact on CSI, by analyzing the CSI measured at the Wi-Fi device when the user stands at multiple different positions around the Wi-Fi device. The angle range derived by such standing position shows the angle area the rogue AP roughly locates. We next derive two statistical methods, *Amplitude Correlation Method* and *Amplitude Orthogonal Transformation Method*, to perform direction derivation under different scenarios. We then take advantage of these two statistical methods to improve the direction derivation accuracy through *Amplitude Combined Method*.

1) Amplitude Correlation Method: We find in our experiments that the CSI amplitude is highly correlated with each other when the user stands at the positions out of the direct path between the Wi-Fi device and rouge AP. However, the CSI amplitude obtained when the user stands in-between the wireless device and rogue AP is less correlated with that of the positions out of the direct path. This indicates that the standing position in between the Wi-Fi device and rogue AP has the most significant impact on the wireless channel. This is caused by the user's blocking effect to the wireless channel as described in Section IV. To capture such blocking effect and estimate the standing position for deriving the direction of the rogue AP, we study amplitude correlation.

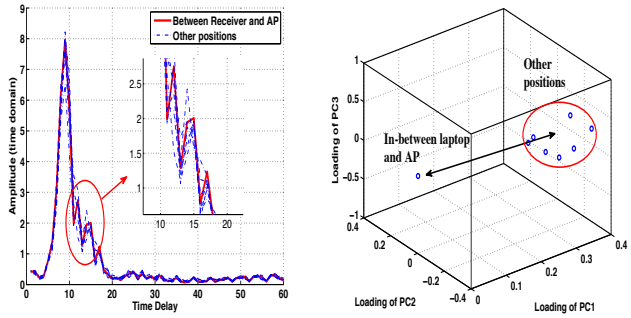
At each standing position, we obtain the time domain CSI amplitude $a(t)$, which denotes the arrival signal with different time delays due to multipath effect. We define the *amplitude correlation* between two standing positions i and j as,

$$\rho_{i,j} = \frac{\sum_{t=1}^{T}(a_i(t)-\bar{a}_i)(a_j(t)-\bar{a}_j)}{\sqrt{\sum_{t=1}^{T}(a_i(t)-\bar{a}_i)^2}\sqrt{\sum_{t=1}^{N}(a_j(t)-\bar{a}_j)^2}}, \quad (2)$$

where T is the number of time delays, a_i and a_j are the time domain CSI amplitude vectors of size $1 \times T$ at position i and j. $\bar{a}_i$ and $\bar{a}_j$ are the mean value of the CSI amplitude at position i and j respectively.

We calculate the amplitude correlation between position i and the rest positions, and then average the sum of the correlation as $\rho_i = \frac{\sum_{j=1,j\neq i}^{l}\rho_{i,j}}{l}$, $0 < i,j \leq l$. Therefore, the angle range that captures the rogue AP's direction can be derived as the angle range of the position i with the smallest amplitude correlation value ρ_i.

2) Amplitude Orthogonal Transformation Method: During the course of our project, we find that under some scenarios the received CSI amplitude at different positions tends to be highly correlated no matter where the blocking object locates (e.g., on the direct path between the rogue AP and the Wi-Fi device) as shown in Figure 5 (a) (amplitude correlation between positions is over 94%). This happens for example when the wireless device is in a spacious open space with less reflections and far away from the rogue AP, or when the device is in a complex indoor environment with permanent obstacles which incur many reflections and refractions. Since the amplitude correlation method only captures the coarse-grained information on how two sequences are different, it is thus difficult to capture more detailed differences.



(a) (b)

Fig. 5. Illustration of using amplitude orthogonal transformation method: (a) Time domain CSI amplitude at eight different positions around the wireless device: the correlation between the positions is over 94%; (b) after using amplitude orthogonal transformation method while three principal components are considered.

We find that multiple distortions exist at the smaller amplitude peaks when comparing the solid curve to those of dash curves as shown in the zoom-in part of Figure 5 (a). This inspires us to investigate the method that can capture such detailed differences exhibited in CSI when the user stands at different positions. We thus transform the raw data to orthogonal spaces and convert the correlated data into uncorrelated ones for capturing the detailed differences.

In particular, we utilize principal component analysis (PCA) in our second method to derive the direction of the rogue AP. PCA is an orthogonal linear transformation method that converts a set of observations of possibly correlated variables into orthogonal spaces of linearly uncorrelated variables called principal components. We then study the impact of the blocking object on the orthogonal spaces. The detailed procedure of PCA can be found in literature [22].

Scheme Description. The CSI amplitude in time domain at multiple positions can be represented as a $t \times l$ matrix a, where t denotes the number of time points and l denotes the number of standing positions around the wireless device. In order to capture the blocking effect when the user stands in the direct path, we perform PCA on the matrix a, and obtain the loading matrix b [22]. The $l \times l$ loading matrix b indicates the correlation between l original variables (CSI at l positions) and l variables in orthogonal spaces (principle components). Each element $b_{i,j}$ in this matrix is a weight, which measures how important the variable j (CSI at position j) is associated with variable i in orthogonal spaces (principle component i). Higher value of $b_{i,j}$ indicates that the position j is associated with larger amount of variation on principal component i in the orthogonal spaces.

Therefore, the column vector b_j of matrix b measures the relationship between the position j and all l principal components, which suggests the contribution of position j to the variation of the data in the orthogonal spaces. In order to measure the user's impact to the wireless channel at different positions, we calculate the vector distance among column vector $b_j, j = 1 \ldots l$. We thus define the *distance in orthogonal spaces* between position j and k,

$$D_L\{b_j, b_k\}_{j\neq k} = \sqrt{\sum_{i=1}^{L}(b_{i,j}-b_{i,k})^2}, \{j,k\} \in 1...l, L \leq l. \quad (3)$$

The distance in orthogonal spaces measures the 'similarity' between two positions in the orthogonal spaces. Then, we sum the distance in orthogonal spaces between position j and all other positions: $D_L(b_j) = \sum_{k=1,k\neq j}^{L} D_L\{b_j, b_k\}$. Thus the angle range derived by the position j, which has maximum sum of orthogonal space distance $D_L(b_j)$, is determined as the angle range towards the rogue AP. Note that the number of principal components L is decided as follows.

Number of Principal Components L. In order to calculate the distance in orthogonal spaces for each position, it is important to determine an appropriate value L, which is the number of principal components for distance calculation. For each position $j = 1...l$, we calculate the $D_L(b_j)$ from $L = 1$ to l, and choose L that produces the maximum value of $D_L(b_j)$, because it better represents the discrepancy of this position in terms of L principal components. Note that the value of L for different positions could be different.

An illustration of the amplitude orthogonal transformation method with three principal components is presented in Figure 5. Figure 5 (a) shows that the CSI amplitude from all positions are highly correlated to each other (over 94% average amplitude correlation). However, we can observe distortions for different positions at smaller amplitude peaks from the zoom-in figure. By measuring the distance in orthogonal spaces as shown in Figure 5 (b), we can capture the user's blocking effect to the wireless channel, and distinguish the position where the user is on the LOS path from other positions.

Confidence Level. We provide a confidence level associated with each estimation via amplitude orthogonal transformation method. The confidence level gives the user additional useful information of how confident the estimation is. While performing PCA, we also obtain eigenvalues [22] for each principle component, which indicates the variation in the orthogonal spaces corresponding to each principle component. While the angle range corresponding to one standing position is derived as the direction of the rogue AP, we have L principal components involved in calculating the distance in orthogonal spaces at that position. We thus define the *confidence level* as the percentage of eigenvalues of the L principle components used for the distance calculation to the eigenvalues of all principle components. The percentage of the eigenvalue corresponding to number of principle components can be used as an indication of how much variations of the data we have measured in our method. It thus indicates how confident our estimation is.

3) Amplitude Combined Method: We further combine amplitude correlation and amplitude orthogonal transformation to benefit from both time domain CSI amplitude and its orthogonal spaces.

When the amplitude correlation between user positions exceeds certain threshold ζ indicating the difficulty for amplitude correlation method to provide accurate estimation, we turn to use the amplitude orthogonal transformation method. Furthermore, if the amplitude orthogonal transformation method produces a low confidence level γ indicating that both correlation and orthogonal transformation method have uncertainties of the estimation, we merge the results obtained from both methods. We modify the two approaches by outputting m (starts from 1) estimated directions. We choose the overlapped estimates of the two approaches as the direction of the rogue AP. If we do not have an overlap on the estimates from these two methods, we increase m by one and re-perform the above step until an overlapped estimate is obtained. By combining the results from the two methods, we characterize the blocking effect from both the time domain CSI amplitude and its orthogonal spaces, and thus reduce the large error and enhance the robustness of the direction derivation of the rogue AP.

B. Direction Calibration

With an angle range towards the rogue AP derived from the previous step, we then perform direction calibration to narrow down the angle range to a direction pointing to the rogue AP. As shown in Figure 2 (b), we can obtain the continuous collected data with M packets when the user moves slowly across the arc of the angle range ω.

We then compute ω averaged CSI from these collected M packets to get the degree resolution as 1 degree. Specifically, we average the data over a sliding window of size N with a step size $n = \lfloor \frac{M}{\omega} \rfloor$, where $N = M - n \times (\omega - 1)$ (i.e., $M = 300$, $\omega = 90$, $N = 33$, and $n = 3$ are used our experiments). We use these ω averaged CSI to simulate the CSI collected at ω evenly distributed positions along the ω degree arc. Therefore, the degree difference between two simulated neighbor positions is one degree. We then compute the orthogonal space distance based on these ω averaged CSI and further determine the direction of the rogue AP by choosing the direction with the largest distance in orthogonal spaces to others. Note that we also consider utilizing amplitude correlation to calibrate the direction. However, the computational cost of calculating correlation between any two positions can be extremely high (e.g., $O(\omega^2)$ operations of correlation calculation). Therefore, we apply the amplitude orthogonal transformation method in direction calibration leveraging time domain CSI amplitude.

VI. Position Estimation Methods

In this section, we develop two methods to estimate the position of the rogue AP based on direction determination: *geometric relationship based* and *obstacle avoidance direction adjustment*.

A. Geometric Relationship-based Method

This method directly pinpoints the location of the rogue AP using spatial diversity. It performs direction determination at multiple locations and applies triangulation to obtain the position of the rogue AP. In particular, the user can derive the direction of the rouge AP at multiple locations by placing the Wi-Fi device at different locations with spacial diversity. Then the location of the rouge AP can be estimated by using the derived directions together with the locations where the Wi-Fi device has been placed.

Our proposed scheme takes two inputs: the physical locations where the Wi-Fi device was placed, (x_i, y_i) for ith position, and the angle ϕ_i derived at position i towards the rogue AP. Then, a straight line $l_i : y = a_i x + b_i$ can be uniquely determined by the two inputs, where $a_i = -tan(\phi_i)$ and $b_i = y_i + x_i tan(\phi_i)$. Given different number of locations the Wi-Fi device was placed, there are two scenarios: 1) If the user repeats direction determination at two different locations, we can pinpoint the rogue AP as the intersection point $(\hat{x_1}, \hat{y_1})$ of the two directional lines determined independently at two positions; 2) If the user repeats direction determination at more than two locations, we can obtain multiple intersections $(\hat{x}_i, \hat{y}_i), i = 1, 2, ..., m$, where m is the total number of intersections. We then derive

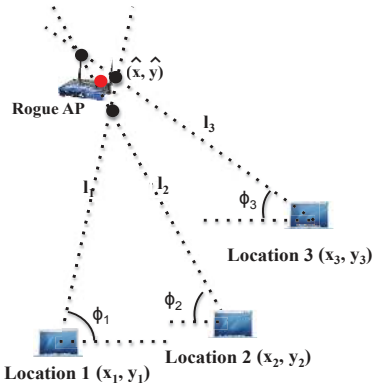


Fig. 6. Illustration of position estimation of the rogue AP through geometric relationship based method while conducting direction determination at three different locations.

the location of the rogue AP by calculating the centroid of these intersections $(\hat{x}, \hat{y}) = (\frac{1}{m}\sum_{i=1}^{m} \hat{x_i}, \frac{1}{m}\sum_{i=1}^{m} \hat{y_i})$. An illustration of the geometric relationship based method is shown in Figure 6. We show the example of locating the rogue AP by performing direction determination at three different locations. The red dot represents the estimated location of the rogue AP, which is the centroid of the three intersection points of the three directional lines.

B. Obstacle Avoidance Direction Adjustment

In this method, the user walks towards the rogue AP along the determined direction with a single Wi-Fi device to reach the AP. However, the user's path may be blocked by doors, walls, buildings, etc. The user needs to bypass the obstacles and then continue approaching the rogue AP. Under such situations, we develop a direction adjustment scheme to re-calculate the direction of the AP after passing the obstacle, since the obstacles may affect the accuracy of the previous direction determination.

The user makes the direction adjustment in two scenarios. First, the user encounters a permanent obstacle such as a building or room, and bypasses it along the previous estimated direction by entering the building or room. We conduct the direction adjustment after passing the obstacle. If the obstacle is a dead end, such as corner or the border of a building, we re-conduct our direction determination scheme at the current location. Second, the user performs the direction determination again after walking over a long distance, i.e., 300 feet, since the coverage of normal wireless AP is around 300 feet [23]. Under such a scenario, the result of the previous direction determination maybe inaccurate, we thus need to perform direction adjustment.

VII. Performance Evaluation

A. Experimental Methodology

1) Experimental Setup: We conduct experiments in a 802.11n Wi-Fi network using a laptop equipped with IWL 5300 wireless cards [24]. We associate the laptop with a commercial wireless AP, Linksys E2500, which serves as the rogue AP. The laptop runs Ubuntu 10.04 LTS with the 2.6.36 kernel. The Intel wireless cards' driver we installed are able to collect CSI information from frames transmitted in HT rate [23]. We use *ping* command to simulate the communication packets transmitted between the laptop and the AP. The packet rate is 20 packets per second. For each packet, we extract the CSI measured at 30 subcarriers which are distributed evenly in the 56 subcarriers of a 20MHz channel [21]. The laptop is placed on a high stool with 4 feet high. The user stands at 8 evenly distributed positions with 1 foot away around the wireless device as shown in Figure 2 (a). The user slowly moves across the arc at a speed of $\nu = 6^\circ/sec$ as shown in Figure 2 (b). We note that the range that the user moves across in direction calibration is $\omega = 90$ degree. The granularity of the direction calibration is 1 degree. For our amplitude combined method, we set the correlation threshold $\zeta = 0.85$, and confidence level threshold $\gamma = 0.75$.

2) Experimental Scenarios: We conduct experiments in both indoor and outdoor environments. The indoor environments include a *research lab* and *classrooms*, and the outdoor environments include a *soccer field* and the area *outside of the research building*. For each site, we put the laptop at more than 50 locations with the AP placed at several different positions. During the experiments, there are people moving in the environments, e.g. students playing in the soccer field or walking in the research lab.

The details of the experimental environments are described as follows: 1) The *research Lab* with a size of 50×60 feet is located on the 5th floor of Burchard building at Stevens Institute of Technology. The research lab includes two rooms, where the outer room has desks, chairs and shelves with electronic instruments on it, and the inner room is an empty space without furnitures. We experiment in both the inner empty space and the outer room with few students in the lab. 2) The *classrooms* are located on the first floor of Babbio Center of Stevens Institute of Technology. One large classroom with 100×80 feet, and two small classrooms with around 40×50 feet are full of desks and chairs. 3) The *soccer field* on campus is a large open area around 500×350 feet. We collect data at various positions from 30 feet to 400 feet away from the AP. During our experiments, several students are playing soccer or base ball in the field. 4) We examine the scenario where the AP is placed inside the first floor of the Burchard building, and the user and the laptop are *outside of the research building*. We collect the data at various locations from 50 feet to 200 feet away from the AP.

B. Metrics

We use the following metrics for experimental evaluation.

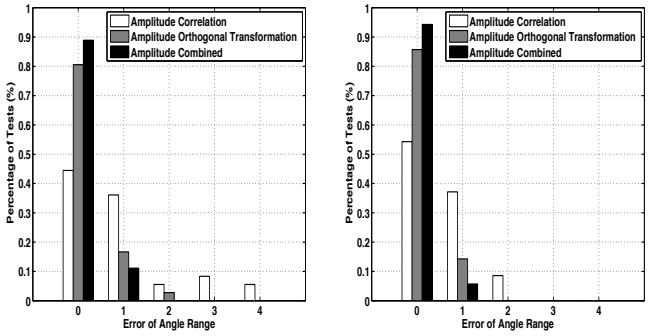
Error of Angle Range. It is defined as the error between the estimated angle range and the true angle range where the rogue AP locates. As there are 8 positions to test around the Wi-Fi device, each position represents the angle range of 45 degrees. If the estimated range has n range differences from the true range, the error of angle range is n.

Angular Error. It is defined as the error between the true direction of the rogue AP and the estimated direction with granularity to be 1 degree.

Location Error. It is the distance between the estimated location and the true location of the rogue AP.

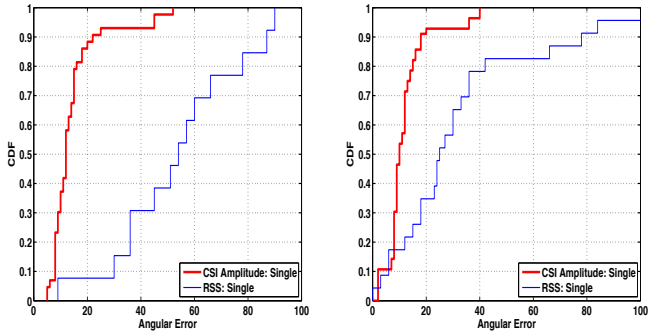
C. Performance Evaluation of Direction Determination

1) Direction derivation: Figure 7 (a) and (b) present the performance of direction derivation with single antenna for indoor and outdoor environments respectively. We observe that the proposed amplitude combined method is very effective in capturing correct angle range of the rogue AP in both indoors



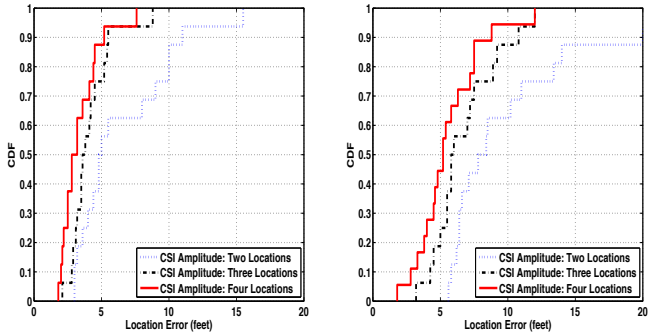
(a) Indoor (b) Outdoor

Fig. 7. Direction derivation with single antenna for indoor and outdoor.



(a) Indoor (b) Outdoor

Fig. 8. Direction calibration with single antenna using CSI-based method (amplitude combined method for direction derivation), and RSS-based method respectively.



(a) Indoor (b) Outdoor

Fig. 9. Position estimation performance via geometric relationship based method while using amplitude combined method for direction derivation.

and outdoors. Specifically, the amplitude combined method produces the correct angle range at around 90% of the cases for both environments. Furthermore, the performance in outdoors is slightly better than that of indoors due to the signal propagation is less complicated in outdoors. Moreover, although the performance of the amplitude correlation and amplitude orthogonal transformation methods varies, the two amplitude methods can be combined to improve the performance.

The results are encouraging and show that the amplitude combined method takes advantages of both the correlation and orthogonal transformation methods and achieves high accuracy in estimating the angle range of the rogue AP in both environments. We note that multiple antennas are widely available on current commercial Wi-Fi devices (e.g., laptops). The additional antenna pairs can provide spatial diversity to combat the multipath effects and may further enhance the performance of direction deprivation. We will study the performance of using multiple antennas in our future work.

2) Direction Calibration: In Figure 8, we present the performance of direction calibration (i.e., red curves) in both indoor and outdoor environments based on the angle range provided by the amplitude combined direction derivation method. We find that the proposed direction calibration achieves high accuracy in identifying the direction of the rogue AP in both indoors and outdoors. In particular, the median error is about 10 degrees and the 90% error is at around 20 degrees in both indoors and outdoors. We do observe that the CDF curves have tails in both environments with about 40 degrees maximum error. This is mainly because we have a very small percent of cases which bring in errors from the direction derivation step. That is, the true direction of the rogue AP does not fall into the range which is used for calibration. Moreover, we observe that the performance of indoors is comparable to that of the outdoors, although it is more challenging in indoors. The results demonstrate that our method is highly effective in outdoors as well as in complicated indoor environments with heavy multipath and shadowing effects.

3) Comparison with RSS-based Method: We further compare our CSI-based direction determination methods with the existing RSS-based method. Specifically, we compare our CSI-based method with the RSS-based method proposed in [18]. By using human body as an obstacle to block the wireless receiver at different directions, RSS-based method determines the direction of the AP when the signal strength has the largest degradation. Figure 8 shows the comparison of the direction determination accuracy when using CSI-based method (i.e., red curves) and RSS-based method (i.e., blue curves) under our experimental setup in both indoors and outdoors.

We observe that the proposed CSI-based method significantly outperforms the RSS-based methods in both environments. In particular, we can achieve around 10 degree median error for both environments, while the maximum error is around 25 degree in outdoors and 50 degree in complex indoor environments for RSS-based method. Overall, our approach can achieve over 40% error reduction in maximum error for both indoors and outdoors, 80% error reduction in median error for indoors, and 60% error reduction for outdoors. This is because CSI provides fine-grained channel information and can characterize the user's blocking effect better, whereas the RSS is coarse-grained information and suffers from the multipath and shadowing effects in complex wireless environments.

D. Performance Evaluation of Position Estimation

1) Position Estimation through Geometric Relationship-based Method: We present the position estimation results of geometric relationship based method in Figure 9 by using the directions determined at two, three or four locations. The position estimation performance is related to the direction estimation accuracy at each location and the number of locations used. Specifically, the maximum error is reduced from 15 feet to around 8 feet in indoors, and from over 20 feet to 12 feet in outdoors by increasing the number of locations used from 2 to 4. And we achieve 3.5 feet median error in indoors, and 6.5 feet median error in outdoors when using four different locations.

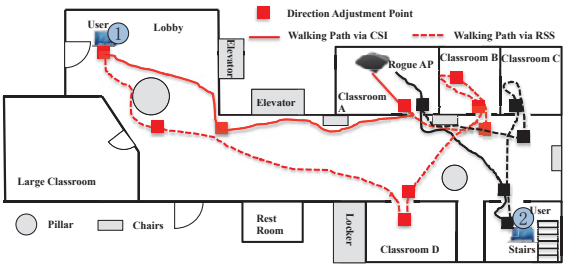


Fig. 10. Position estimation through obstacle avoidance direction adjustment: the 1st floor of Babbio Center of Stevens Institute of Technology.

2) Position Estimation through Obstacle Avoidance Direction Adjustment: Finally, we present the path comparison of the user walking towards the rogue AP utilizing CSI and RSS respectively in an indoor environment. Figure 10 shows two walking paths (starts from the lobby and the stairs respectively) towards the rogue AP on the 1st floor of Babbio Center of Stevens Institute of Technology. The solid line represents the walking path using CSI (amplitude combined method), and it takes 3 times of direction determination to arrive at the rogue AP. Whereas the dash line represents the walking path via RSS, which takes more than 5 direction adjustments to capture the rogue AP. The accurate and robust direction determination resulted from CSI-based method enable the user to arrive at the rogue AP with shorter walking distance and less direction adjustments. However, the RSS-based approach incurs large uncertainties of direction, and leads the user to more rooms and more direction adjustments which wastes the user much more time to reach the rogue AP. The results show that it is more efficient to locate the rogue AP by using the CSI-based method compared to RSS-based method.

VIII. Conclusion

Locating the position of the rogue AP is important to ensure the successful deployment of pervasive wireless networks. In this paper, we propose to use the fine-grained channel state information (CSI) obtained from commercial Wi-Fi device to perform accurate rogue AP localization. Our proposed framework using a single Wi-Fi device involves minimal infrastructure cost and achieves high accuracy. Two components are proposed in the localization framework including direction determination and position estimation. The direction determination component captures the blocking effect of the user to the wireless channel by using CSI amplitude for estimating the direction of the rogue AP. The determined direction of the rogue AP can facilitate the rogue AP localization by either directly pinpointing the rogue AP using spatial diversity (with the directions determined at multiple locations) or walking towards the rogue AP through obstacle avoidance direction adjustment. Our experimental results show that the proposed direction determination method using CSI is highly effective and robust to both indoor and outdoor environments. In contrast, the existing RSS-based angle estimation method cannot work in indoors and the performance in outdoors is significantly worse than that of our method. Further, our proposed CSI-based framework is more efficient and accurate in locating the rogue AP when comparing to existing RSS-based method confirming that CSI provides richer information than that of RSS for describing the wireless channel.

Acknowledgements: This work is supported in part by the NSF grants CNS0954020, CNS1318748, CNS1318751 and Army Research Office W911NF-13-1-0288.

References

[1] "Air magnet," www.airmagnet.net, 2011.

[2] L. Ma, A. Teymorian, and X. Cheng, "A hybrid rogue access point protection framework for commodity wi-fi networks," in *IEEE INFOCOM*, 2008.

[3] C. Yang, Y. Song, and G. Gu, "Active user-side evil twin access point detection using statistical techniques," *IEEE Transactions on Information Forensics and Security*, 2012.

[4] H. Han, B. Sheng, C. C. Tan, Q. Li, , and S. Lu, "A timing-based scheme for rogue ap detection," *IEEE Transactions on Parallel and Distributed Systems*, 2011.

[5] K. Gopalakrishnan, M. Govindarasu, D. W. Jacobson, and B. M. Phares, "Cyber security for airports," *International Journal for Traffic and Transport Engineering*, 2013.

[6] R. Beyah and A. Venkataraman, "Rogue-access-point detection: Challenges, solutions, and future directions," *IEEE Security and Privacy*, 2011.

[7] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 mac layer spoofing using received signal strength," in *IEEE INFOCOM*, 2008.

[8] R. Beyah, S. Kangude, G. Yu, B. Strickland, and J. Copeland, "Rogue access point detection using temporal traffic character- istics," in *IEEE GLOBECOM*, 2004.

[9] C. Mano, A. Blaich, Q. Liao, Y. Jiang, D. Cieslak, D. Salyers, and A. Striegel, "Ripps: Rogue identifying packet payload slicer detecting unauthorized wireless hosts through network traffic conditioning," *ACM Transaction on Information and System Security*, 2008.

[10] D. Schweitzer, W. Brown, and J. Boleng, "Using visualization to locate rogue access points," *Journal of Computing Sciences in Colleges*, 2007.

[11] F. Adelstein, P. Alla, R. Joyce, and G. Richard, "Physically locating wireless intruders," in *Information Technology: Coding and Computing (ITCC)*, 2004.

[12] D. Yang, G. Xue, X. Fang, and J. Tang, "Crowdsourcing to smartphones: Incentive mechanism design for mobile phone sensing," in *ACM International Conference on Mobile Computing and Networking*, 2012.

[13] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Mobicom*, 2008.

[14] S. Jana and S. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," in *Mobicom*, 2008.

[15] T. M. Le, R. P. Liu, and M. Hedley, "Rogue access point detection and localization," in *IEEE PIMRC*, 2012.

[16] M. Gonzalez, J. Gomez, M. Lopez-Guerrero, V. Rangel, and M. de Oca, "Guide-gradient: A guiding algorithm for mobile nodes in wlan and ad-hoc networks," in *Wireless Personal Communications*, 2011.

[17] D. Han, D. Andersen, M. Kaminsky, K. Papagiannaki, and S. Seshan, "Access point localization using local signal strength gradient," in *Passive and Active Measurement Conference*, 2009.

[18] Z. Zhang, X. Zhou, W. Zhang, Y. Zhang, G. Wang, B. Zhao, and H. Zheng, "I am the antenna: Accurate outdoor ap location using smartphones," in *MOBICOM*, 2011.

[19] S. Shah, S. Srirangarajan, and Tewfik, "Implementation of a directional beacon-based position location algorithm in a signal processing framework," *IEEE Transactions on Wireless Communications*, 2010.

[20] A. Subramanian, P. Deshpande, J. Gaojgao, and S. Das, "Drive-by localization of roadside wifi networks," in *IEEE INFOCOM*, 2008.

[21] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Predictable 802.11 packet delivery from wireless channel measurements," in *ACM SIGCOMM Computer Communication Review*, 2010.

[22] I. Jolliffe, "Principal component analysis," *Springer Series in Statistics*, 2002.

[23] I. Std., "802.11n-2009: Enhancements for higher throughput," Available at http://www.ieee802.org, 2009.

[24] I. Research, "Intel 5300 mimo channel measurement tool," http://ils.intel-research.net/ 80211n-channel-measurement-tool.