3DLoc: Three Dimensional Wireless Localization Toolkit

Jizhi Wang, Yinjie Chen, Xinwen Fu, Jie Wang
University of Massachusetts Lowell
{jwang1, ychen1, xinwenfu, wang}@cs.uml.edu

Wei Yu
Towson University
wyu@towson.edu

Nan Zhang
George Washington University
nzhang10@gwu.edu

Abstract

In this paper, we present $3DLoc$: an integrated system of hardware and software toolkits for locating *an 802.11-compliant mobile device in a three dimensional (*3D*) space. $3DLoc$ features two specialized antennas: an azimuth antenna and an elevation antenna, for detecting the azimuth and elevation angles of a mobile device respectively in real time. To improve positioning accuracy in real-world urban settings, we propose various signal processing techniques such as clustering and wavelet-transform based denoising, and present theoretical analysis of the accuracy of these techniques. With different antenna configurations, 3DLoc is able to track single or multiple targets in one round of azimuth scanning and elevation scanning. We conduct extensive experiments to demonstrate the efficiency and accuracy of $3DLoc$. $3DLoc$ can be used in various applications, including wireless network forensics for locating anonymous criminal mobile devices.*

1. Introduction

Network forensics plays a crucial role in fighting cyber crimes such as child pornography and cyber terrorism for public safety and homeland security. A challenging task in wireless network forensics is the physical positioning of criminals. To this end, this paper presents $3DLoc$, an integrated system of hardware and software toolkits for locating one or more 802.11-compliant mobile devices simultaneously in a three dimensional (3D) space.

The positioning of wireless devices, with or without cooperation of the devices, is a topic that has been extensively studied in wireless networking [1]–[3]. While the power of existing techniques such as E911 [4] is evidenced by their versatile deployment on mobile phones and PDAs, we argue that most of the existing techniques are not designed for, and thus do not meet, the requirements of crime scene investigations in wireless network forensics. Through interviewing with law enforcement, we identified two key requirements: (i) The ideal positioning toolkit should be infrastructure-free, training-free, portable, and operable by one or at most two officers, so that it can be quickly deployed to crime scenes. (ii) The ideal positioning toolkit should locate the target device in a 3D space, an example being the positioning of a device inside a room of a multi-story building from outside on the street. In order to do so, the toolkit must consider the complication of radio signal reflection, cancelation and absorption in an urban environment.

To the best of our knowledge, no existing technique is capable of meeting both requirements. To avoid the infrastructural requirement, techniques [5] have been proposed to locate targets from a single point-of-operation by moving the positioning device or leveraging the WiFi infrastructure already existing in urban areas. Nonetheless, all these techniques require extensive training in the target area which is prohibitive for crime scene investigations. Existing publicly available WiFi access point (AP) position databases [6] maintain only 2D coordinates and cannot be used for positioning a mobile via intersecting the coverage areas of APs that are in range of the target in a 3D space [5]. Those techniques are not suitable for 3D positioning.

Our objective is to provide an infrastructure-free, training-free and portable device for locating suspect mobile devices. It is extremely challenging (if not impossible) for such a device to measure the distance between the target and the device directly via signal strength in all possible 3D environments, especially when the physical constraints for signal propagation is unknown. As such, our design goal is to precisely determine the 3D angles between the positioning device and the target(s) due to the following reasons:

(i) From the view of a single-position device, the location of a target is determined by its polar coordinates - i.e., the distance and 3D angles between the device and the target. Due to the small transmission range caused by attenuation and shadow fading of wireless signals, the 3D angles are a more effective factor for discriminating between the locations of mobile devices, and thereby help the law enforcement officers to the maximum extent.

(ii) When two officers are available, they can use two angle-detecting devices at different locations to pinpoint the precise location of target devices. Since our device is

Jizhi Wang is now with Shandong Computer Science Center, Jinan, China 250014 (Email: wangjzh@keylab.net). He conducted this work under Dr. Xinwen Fu's supervision while visiting UMass Lowell. *The work is partially supported by NSF under grants 0943479, 0907964, 0958477, 0852673 and 0852674. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of those sponsors.*

portable, one officer can take two positions and pinpoint the mobile location. This idea is nothing new compared to triangulation. But the challenge we tackle is how to identify 3D angles accurately enough so two positioning devices will be sufficient for accurate target positioning.

In particular we propose $3DLoc$ which consists of two main components: a pair of specialized antennas which detect the azimuth and elevation angles of the target device, respectively, and an antenna rotor which rotates the antenna. The two specialized antennas feature distinct characteristics: The azimuth antenna has a wide vertical beamwidth while the elevation antenna has a narrow one. The reasons why such a design is effective are subtle - we defer a detailed discussion to Section 3.2 in this paper.

$3DLoc$ uses a set of novel algorithms to determine the target 3D. In particular, we pre-process the monitored signal strengths with density-based clustering to filter out reflective components. Then, we perform signal denoising using discrete wavelet transformation (DWT) to identify the 3D angles of a target device. We demonstrate in our theoretical analysis and experimental evaluation that $3DLoc$ achieves a small standard error within a short amount of time.

The contributions of this paper are summarized as follows:

- *Application Novelty:* To the best of our knowledge, our work is the first to identify, study and fulfill law enforcement's pressing need of an infrastructure-free, training-free, and portable forensics device that is operable by one or at most two officers.
- *Solution Novelty:* We propose novel clustering-based pre-processing and DWT-based denoising techniques to generate accurate 3D angle estimates from raw signal measurements. To the best of our knowledge, this is the first time DWT is used for the 3D positioning of 802.11-compliant mobile devices. No existing work [2], [3] has given extensive study of those positioning error causing factors in such a systematic way as we did in this paper.
- Our contribution also includes a comprehensive set of theoretical analysis and experimental results which demonstrates the effectiveness of $3DLoc$ in real-world environments. Our theoretical analysis provides rigid bounds for the angle estimation error.

Because of the space limit, please request our technical report on the study of distance estimation theory from angle measurements, positioning of multiple targets and related experimental results.

The rest of this paper is organized as follows. In Section 2, we introduce the problem definition of suspect positioning for forensics purposes in urban environments, overview $3DLoc$ and introduce its basic architecture and functionalities. Section 3 presents the main steps for $3DLoc$ to locate a single still target device. Section 4 provides the analysis of accuracy and efficiency of $3DLoc$ and presents the approach calculating the location of a suspect mobile. We also discuss the limitations of $3DLoc$ in this section. Section 5 presents the experimental evaluation of $3DLoc$. We review the related work in Section 6, and conclude this paper in Section 7.

2. System Overview

In this section, we first define the problem of locating 802.11-compliant mobile devices based on the requirements of law enforcement officers. Then, we provide an overview of the system architecture and the functionalities of $3DLoc$.

2.1. Problem Definition

With the ubiquitous deployment of open-access WiFi networks, criminals may now utilize such networks provided by various places such as hotels, restaurants, and libraries to conduct anonymous criminal activities. As a result, IP or MAC addresses may not be sufficient for law enforcement to physically locate a suspect. For example, by network monitoring, an officer may track child porn downloading traffic to a WiFi AP. By looking up the AP's association table and bridge learn table [7], the officer can obtain the target's private IP and MAC address corresponding to its public IP. The officer may also apply traffic analysis approaches to map the public IP to a private IP and MAC [8]–[10]. However, the free private IP cannot be linked to a specific user. The mobile MAC can be easily altered in both Window and Linux systems and may not be used for identifying the suspect either. Moverover, the suspect mobile is in a 3D space such as a building and no existing device can locate such a mobile in a straightforward way.

Our target application is to help law enforcement officers on locating suspect wireless devices in wireless network crime scenes. One common scenario is to identify which room (of a building) a radioactive mobile device is in from another adjacent building or outside on the street. The distance between the officer and target cannot be too far due to wireless signal propagation fading in complex environments. Fortunately, in urban environments, it is usually possible for the authorities to find a position with such a close distance without alerting the criminal suspects. The antennas we use feature a gain of around 15dBi, which extends the line-of-sight distance to larger than $1,000$ meters [5].

Problem Definition: Suppose that by network forensics, the law enforcement has identified the IP and/or MAC address of an 802.11-compliant mobile device downloading illegal contents such as child porn. The objective of $3DLoc$ is to efficiently estimate the 3D angles and distance between the $3DLoc$ system and the target device.

Performance Measures: As a positioning system designed for forensics purposes, the performance of $3DLoc$ should be measured in three metrics: secrecy, accuracy and efficiency: (i) *Secrecy:* The criminal suspect should be oblivious to the existence of the forensics system. As we shall explain in the paper, $3DLoc$ only passively receives and measures signals, and thus is always perfect in terms of secrecy. (ii) *Accuracy:* We define the accuracy measure as the estimation error on the 3-dimensional angles and distance between $3DLoc$ and the target device. We shall present in the paper a thorough theoretical and experimental analysis of the accuracy of $3DLoc$. (iii) *Efficiency:* Since the target device may not remain radioactive for an extended period of time, it is critical for $3DLoc$ to generate the estimate in an efficient manner. We define the efficiency measure as the minimum target mobile traffic rate required for $3DLoc$ to generate accurate angle estimates.

2.2. System Architecture of $3DLoc$

Figure 1 depicts the architecture of $3DLoc$ while Figure 2 shows a photo of its prototype. $3DLoc$ consists of two main components: (i) a *rotating* subsystem, and (ii) a *positioning* subsystem. In terms of functionality, the rotating subsystem is supposed to turn the antennas by adjusting their azimuth and elevation angles to *point to* the exact direction towards the device being monitored. In order to do so, the rotating subsystem receives rotation instructions from the positioning subsystem, which uses rotating antennas to collect the target traffic signal strength with regard to the antenna angle, processes the measurements, and computes target azimuth and elevation angles.

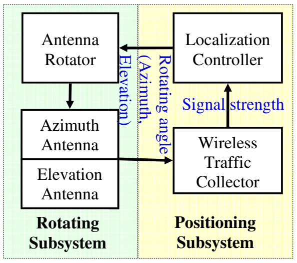

Figure 1. Modules

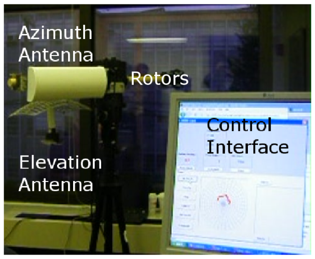

Figure 2. Prototype

The rotating subsystem consists of three main hardware components: an *antenna rotor* (Yaesu G5500 [11]) and a pair of unidirectional antennas: *azimuth* and *elevation*. The antenna rotor adjusts the azimuth and elevation angles for wireless signal reception by rotating the azimuth and elevation antennas in the azimuth and elevation surfaces, respectively. The rotating subsystem is controlled by the positioning subsystem via a set of APIs of a rotor control interface (RCI) board [12] connecting the antennas to computers. The APIs can read the current angles of the two antennas. The angle reading is independent from the antenna alignment and determined by the rotor mechanics.

The positioning subsystem consists of two main software components: (i) a *wireless traffic collector*, and (ii) a *localization controller*. The wireless traffic collector is a revised version of *tcpdump*, which collects wireless traffic from the azimuth and elevation antennas and extracts the target mobile signal strength based on the pre-known identity such as the MAC address of the target device. It then transmits the measured signal strength to the localization controller.

The localization controller analyzes the signal strength of wireless frames from the mobile to generate an optimal rotation plan for the antennas. The controller also collects antenna angle information via RCI APIs. Antenna angles are correlated with wireless traffic frames via time synchronization between the two processes of traffic collecting and angle collecting. After that, the controller generates rotation instructions which are sent to the rotating subsystem via RCI APIs and adjust the azimuth and elevation angles of the antennas to point towards the mobile device.

2.3. Functionalities of $3DLoc$

3DLoc is designed to locate suspects downloading and conducting illegal activities on their WiFi devices. In those cases, the mobile device is relatively still. In this paper, we focus on locating single still targets and leave the moving target positioning as our future work.

3. Locating Single Target

3.1. Overview

In this section, we describe four main steps for $3DLoc$ to locate a single still wireless device, as illustrated in Figure 3.

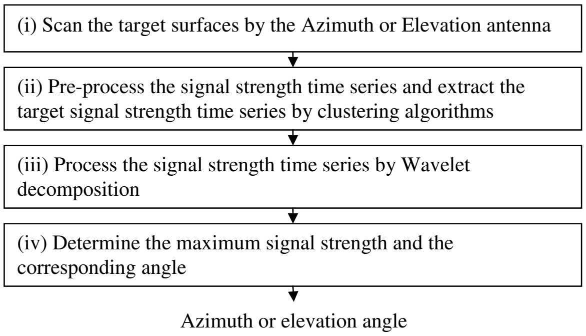
(i) Scan the target surfaces by the Azimuth or Elevation antenna
(ii) Pre-process the signal strength time series and extract the target signal strength time series by clustering algorithms
(iii) Process the signal strength time series by Wavelet decomposition
(iv) Determine the maximum signal strength and the corresponding angle
Azimuth or elevation angle

Figure 3. Locating Still Targets

The first step uses the azimuth and elevation antennas to record the signal strength readings from various directions. We shall discuss in Section 3.2 why two antennas are needed, and the desired beamwidth for each antenna.

In an ideal environment where there is no obstacle or interference between or surrounding the $3DLoc$ system and the target device, the computation of 3D angles after obtaining the signal strength readings is almost trivial: just point the azimuth and elevation antennas to the directions with the strongest signal strength within their rotation surfaces, respectively, and we obtain the 3D angles toward the target.

In urban environments, however, complex building structures and even furniture layouts may reflect, scatter and/or diffract WiFi signals. As a result, the signal strength reading directly measured by the antennas is noisy. It includes not only the direct propagation of the signal, but also many reflected components and noise interferences. The second and third steps of $3DLoc$ aim to extract the direct propagation component from the measurements because only this component is the best indication of the direction toward the target. In particular, in Step 2, we use clustering to pre-process the readings and remove the reflective components. The technical details of this pre-processing step are explained in Section 3.3. Then, we use DWT to remove noise interferences in Step 3. The details of this denoising step are provided in Section 3.4. Finally, the fourth step determines the 3D angles toward the target based on the direct-propagation component, as explained in Section 3.5.

3.2. Scan Target Surfaces

Why Two Antennas? $3DLoc$ aims to point its antenna(s) toward the target wireless device. It is possible to achieve this objective using one antenna through the following brute-force approach: The antenna is first placed at elevation angle 0° and rotates to cover 360° of the azimuth surface. Then, after raising the antenna by Δ°_{step} in the elevation surface, the same azimuth rotation is repeated. The iteration continues until the whole elevation surface is covered. Then the 3D angles between the positioning device and the target can be determined based on all signal strength readings.

The main problem of this brute force approach is its (in)efficiency: Particularly in our case, a scan of the azimuth or elevation surface requires around 60 seconds to complete. When $\Delta_{step} = 10°$, the entire process will cost around $60 \times 180°/10° + 60 = 1140$ seconds, i.e., 19 minutes. This is unacceptable in practice because the radioactive sessions of many criminal activities may not last such long to allow the suspect to be located.

To address this efficiency issue, we propose to use two antennas in $3DLoc$, one for the azimuth and the other for the elevation surface. Our rotation plan is a two-step process: First, we place the azimuth antenna at elevation $0°$ and rotate it continuously around $360°$ azimuth surface to determine the *azimuth angle* of the target device. The elevation antenna is then rotated to this azimuth angle. Next, we rotate the elevation antenna continuously to cover the elevation surface and determine the elevation angle of the mobile. The elevation antenna is then rotated to this elevation angle and it should point to the target mobile. Therefore, a rotation time of around 60 seconds for the azimuth and elevation rotations, leading to a total positioning time of around 2 minutes, an order of magnitude shorter than the single-antenna brute force approach.

Antenna Selection Criteria: Antenna design involves a complex series of tradeoffs over many geometrical, electrical and mechanical parameters [13]. We focus on characteristics desired by $3DLoc$.

For the azimuth antenna, we select one that has wide elevation (i.e., vertical) beamwidth and narrow azimuth (i.e., horizontal) beamwidth. The wide elevation beamwidth is desired so that the azimuth antenna can cover almost the entire elevation surface from $0°$ to $180°$ at which the target device may be located. The narrow azimuth beamwidth is desired so that the azimuth angle of the target device can be determined with smaller error.

For the elevation antenna, we select one with narrow beamwidth in both azimuth and elevation surfaces. The azimuth beamwidth can be narrow because the azimuth angle of the target device is already determined by the azimuth antenna in the first step. The narrow elevation beamwidth is desired so that the elevation angle of the target device can be determined with smaller error.

In our real system implementation of $3DLoc$ (shown in Figure 2), the azimuth antenna is a 2.4 GHz 14 dBi *sector panel* WLAN antenna with 3dB beamwidth of $120°$ vertically (elevation) and $15°$ horizontally (azimuth). The elevation antenna is a 2.4 GHz 15 dBi die-cast *grid* antenna with beamwidth of $16°$ vertically and $21°$ horizontally. The RF patterns of the two antennas are illustrated in Figures 4 and 5, respectively.

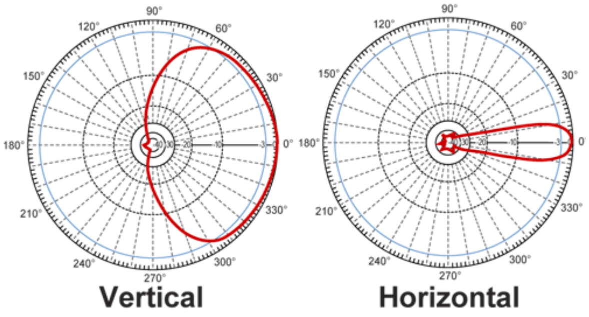

Figure 4. RF Pattern of Azimuth Antenna

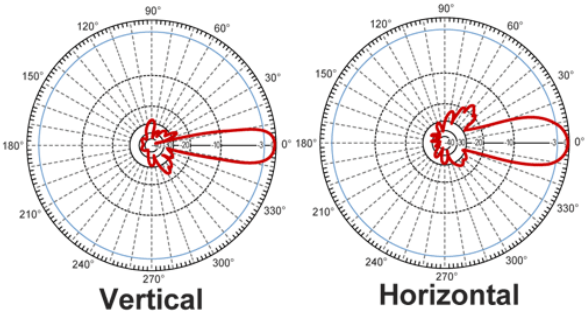

Figure 5. RF Pattern of Elevation Antenna

3.3. Pre-process Signal Strength

Recall from the overview that the objective of this pre-processing step is to remove all reflective components. The *original data* in Figure 6 depicts an example of the raw signal strength received by the azimuth antenna of $3DLoc$ in one round of azimuth surface scan. The x axis is time (seconds) while the y axis is measured *signal strength* (dBm). One can see that the antenna captures both line-of-sight signals (i.e., the upper curve) and reflected signals (i.e., the lower curve). Therefore, if the signal strength reading is directly used to locate the target device, significant error may occur because of the reflected signal components. It also would not help to take a moving average of multiple readings, because the irregular reflected signals could still lower the average, which leads to angle estimation errors. Using moving max may also distort the line-of-sight data. Thus, in order to maintain localization accuracy, it is critical to *identify and remove* the reflected signal strength readings from those sensed by the antenna.

We propose to use *clustering* to remove the reflected signals from the antennas readings. The clustering algorithm separates readings at different moments into different clusters, such that the intra-cluster variance (of signal strength) is minimized while the inter-cluster variance is maximized. Since the signal strength readings form an irregular shape (as shown in Figure 6), we select a density-based clustering algorithm [14].

Given the output of the clustering algorithm, we select the cluster with the highest average strength as the principal component for our subsequent analysis, and *remove* the other clusters as reflected signal. The bottom chart of Figure 6 depicts the six clusters generated by the density-based clustering algorithm from the raw signal strength readings at the top chart. One can see that Cluster 1 represents the strength of signals directly received through line-of-sight, and is reserved for subsequent processing.

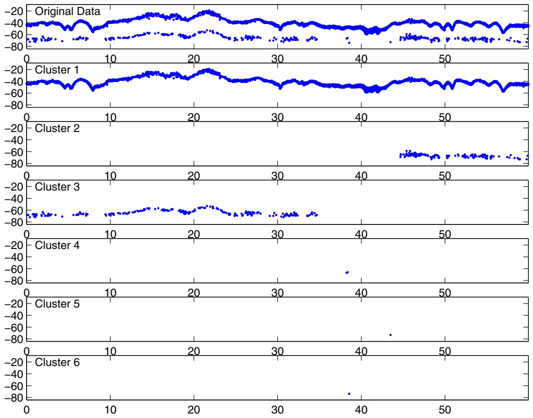

Figure 6. Density-based Clustering

3.4. Signal Strength Denoising

While the preprocessed signal strength reading becomes significantly more stable, it is still the *composition* of not only direct propagation from the target device, but also other noise-like components. Note that such noise may either increase or decrease the signal strength reading. Since our objective is to identify the line-of-sight angle between $3DLoc$ and the target device by finding the strongest direct-propagation signal strength, it is important to remove the noise component from the signal strength readings.

According to the physical model of signal propagation [15], [16], the signal strength reading is a function of the distance between the antenna and the target device. In particular, let d (in meter) and $P(d)$ (in dBm) be the antenna-device distance and the observed signal strength received by the antenna from distance d, respectively. We have

$$P(d) = P(1) - 10\alpha \log(d) - W + X_\sigma, \qquad (1)$$

where α is the pass loss exponent, W (in dB) the wall attenuation degree, and X_σ a normally distributed variable with mean of 0 and variance of σ^2.

In Equation (1), the item X_σ is the noise we aim to remove. To do so, our basic idea is to use wavelet transform to decompose the received signal, and remove all decomposed components with a decomposition level greater than a threshold L. Due to space limit, please refer to [17] for a detailed description of wavelet transform. After that, we compute the denoised signal strength and select the angle with the strongest signal strength value.

The premise of this approach is its ability to filter out noise while retaining the original signal information. According to (1), the noise as Gaussian white noise has its energy evenly distributed across the frequency domain. Therefore, the leftover noise after denoising keeps *at most* $1/2^L$ of the original noise energy.

We now discuss our selection of L (as the cutoff decomposition level). Let B and B' be the bandwidth of the original and the noisy RF antenna pattern bandwidth, respectively. We define

$$L = \log_2 \frac{B'}{B}. \qquad (2)$$

Note that $B' \geq B$ due to the presence of noise. Thus, there is always $L \geq 0$.

Figure 8 depicts the results of applying wavelet decomposition on the example shown in Figure 6 after clustering. At a level i, we use the low frequency component cA_i to reconstruct the signal and derive the approximation. One can see that the approximation becomes smoother with the increasing level - indicating less noise is kept after denoising.

One thing to note is that for wavelet transform, the signal strength time series must be one sampled at a fixed time interval, denoted as *sampling interval*. We use a nearest neighbor interpolation of the preprocessing data to derive a sampled signal strength time series.

3.5. Determine Mobile Angles

Once the denoised signal strength time series is derived, we can derive the maximum signal strength at the corre-

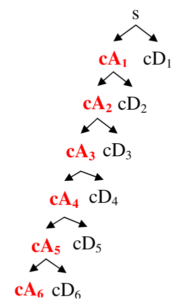

Figure 7. DWT Decomposition Tree

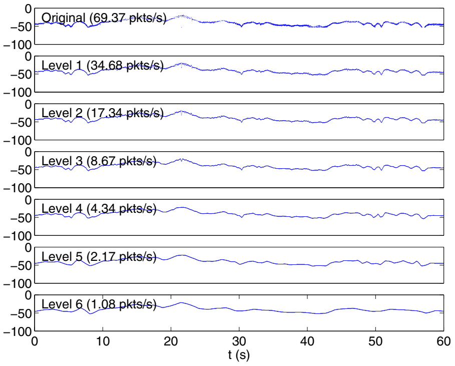

Figure 8. Wavelet Approximation at Different Levels

sponding time. In our current system, the signal strength measurement is a different process from the antenna angle measurement. We use the same sampling interval as the one for wavelet transform to interpolate the antenna angle time series. In the angle interpolation, we use the linear interpolation since the angle rotation in a short period is approximately linear from our experimental results as shown in Figure 9. Therefore, we derive the angle of the mobile corresponding to the time at which the maximum signal strength is derived.

4. Analysis for Locating Targets

In this section, we analyze the positioning accuracy and the efficiency of $3DLoc$ and present the calculation of a target's position from two angle measurements at two positions.

4.1. Accuracy

The randomness in the WiFi signal propagation model Formula (1) leads to the possibility of observing the maximum signal strength at an angle different from the direction of the target device. According to the antenna RF pattern, given the same distance between the target device and the antenna, the more difference there is between the antenna's pointing angle and the line-of-sight angle between the antenna and the target device, the smaller the average signal strength will be. Denote this angle difference as *angle deviation*. Suppose that for a given distance, the average signal strength decreases Δ dB at an angle deviation of δ. That is,

$$\begin{aligned} P(d,0) &= \mu + X_\sigma, & (3)\\ P(d,\delta) &= \mu - \Delta + X_\sigma, & (4) \end{aligned}$$

where $P(d,\delta)$ is the *observed* signal strength with distance of d and angle deviation of δ.

Let $Y = P(d,\delta) - P(d,0)$. Clearly, there is an error on the estimated direction if and only if there exists δ causing $Y > 0$. We conducted extensive experiments to verify the independence of X_σ at different angles. Two antennas are used to simultaneously collect target wireless ICMP traffic from different angles. The sequence numbers of ICMP packets are used to correlate traffic dumped at the two antennas. Our experiments show that $P(d,\delta)$ at different δ and $P(d,0)$ have a very small correlation coefficient of around 0.1 or smaller, which can be treated as negligible correlation in general [18]. This is because noise component X_σ in $P(d,\delta)$ and $P(d,0)$ is the random component caused by the complicated environment and X_σ can be treated as independent from each other. According to [15], [16], variance σ^2 of X_σ is fixed within a specific environment. Therefore, we approximate $P(d,\delta)$ and $P(d,0)$ as independent and identically-distributed random variables both following normal distribution. Under this approximation, Y is also following a normal distribution as follows:

$$Y = N(\mu - \Delta - \mu, \sigma^2 + \sigma^2) = N(-\Delta, 2\sigma^2). \qquad (5)$$

Δ at a specific angle deviation δ is determined by the antenna RF pattern such as those in Figures 4 and 5.

We may use a δ, whose corresponding Δ_B gives a very small probability ϵ such as 2.5% that $Y \geq 0$, as the angle estimation error bound.

$$\begin{aligned} Pr(Y > 0) &= \epsilon, & (6)\\ N(-\Delta_B, 2\sigma^2) &= \epsilon. & (7) \end{aligned}$$

Based on normal distribution properties, when $\epsilon = 2.5\%$, $\Delta_B = 2\sqrt{\sigma_Y} = 2\sqrt{2}\sigma$. Denote the corresponding angle deviation as δ_B. The error bound is

$$ErrorBound = \delta_B. \qquad (8)$$

According to [15], [16], [19], [20], σ is within the range of $[0, 12]$. A larger σ implies more severe signal fluctuations due to irregularities in the surroundings of the receiving and transmitting antennas.

Note that the error bound in (8) is the worst-case bound in presence of noise. After we apply wavelet transform to remove the noise, we obtain better mobile angle estimation as demonstrated by our experiments in Section 5.

Therefore, we have the following theorem for the mobile angle estimation error bound.

Theorem 1: Given noise variance σ^2 and a small probability ϵ, solve the following equation for signal strength decrease Δ_B,

$$N(-\Delta_B, 2\sigma^2) = \epsilon. \qquad (9)$$

The angle deviation δ_B corresponding to Δ_B in the antenna RF pattern is the worst case mobile angle error bound.

We make the following observations from Theorem 1:

(i) The error bound does not change with the distance since the antenna RF pattern does not change in the free space given a constant distance within a specific environment. Thus, the main factor for the error bound is the antenna RF pattern and beamwidth (which determines the change of Δ with δ).

(ii) The smaller the noise variance σ^2 is, the smaller the error bound will be. In particular, the error is usually fairly small for σ^2 values in practice.

(iii) The smaller the azimuth beamwidth of the azimuth antenna or the elevation beamwidth of the elevation antenna is, the smaller the error bound will be. Intuitively, for an antenna with small beamwidth, a relatively small angle deviation δ renders a large attenuation Δ, where the deviation δ falls with the antenna's side lobes with very small antenna gain compared with the main lobe.

4.2. Efficiency

If the mobile does not emit any signal, we have no way to localize it since we cannot measure the antenna RF pattern and the maximum signal strength direction. Therefore, the process of measuring the mobile signal strength is the process of sampling the antenna RF pattern. The sampling rate affects the reconstruction of the RF pattern.

Nyquist sampling theory tells us that if the RF antenna pattern contains no frequencies higher than B Hz, the sampling rate should be at least $2B$. That is, the mobile should send wireless frames at a rate of $2B$. RF pattern diagrams in Figures 4 and 5 don't give the signal strength change in terms of the rotating time. We obtain such information by measuring the rotating function of our rotors. We summarize this observation in Theorem 2.

Theorem 2: Given an antenna RF pattern in terms of time $f(t)$. If the bandwidth of $f(t)$ is B Hz, the required traffic rate from the target mobile should be greater than $2B$ in order to reconstruct $f(t)$ and derive the maximum value of $f(t_m)$ at t_m.

From Theorem 2, we can derive t_m, the time we measured the maximum signal strength. During the antenna rotating process, we also record the angle of the antenna with time. Therefore, from t_m we can derive the pointing angle of the antenna when the antenna has a line-of-sight view of the target mobile, i.e., the target mobile angle.

Once the mobile is located and we don't need to reconstruct the whole RF antenna pattern, the sampling rate can be smaller. Assume the antenna pattern main lobe has bandwidth of B_M, according to Nyquist sampling theory, the lower bound of the sampling rate is $2B_M$.

4.3. Discussion

In this paper, our technique assumes that the cluster with highest power as in Figure 6 is the line of sight (LOS) toward the mobile. This may not always holds in reality because of the complication of radio signal reflection. An example is if the LOS is obstructed by a metal object, then the reflected component may actually have higher power.

In our focused context of wireless network forensics, this problem is not particularly serious. Since $3DLoc$ is a portable and flexible device, the law enforcement may take a few measurements at different positions and exclude those unreasonable measurements by taking advantage of the environmental constraints. This helps avoid the reflecting metal. More measurements produce a better result because the least square method used for calculating a target's location can be applied to correct such measuring errors to some extent. However, metal reflection is indeed a great challenge for locating the mobile. We may produce the guidelines of detecting unfriendly environments and avoiding them. We leave this as our future work.

5. Evaluation

We conducted extensive experiments to evaluate the performance of $3DLoc$. In this section, we first describe the experiment setup, and then present experimental results on deriving the required sampling rate to reconstruct an antenna RF pattern. At last, we present the angle estimation accuracy.

5.1. Experiment Setup

To emulate the forensics case, we placed $3DLoc$ in the office in one building and the target devices (i.e., 802.11-compliant laptops) are in classrooms and offices in another building across the street. There is no line-of-sight view of the WiFi device. This scene is denoted as *remote case* and represents the case that the target is behind walls and windows in hotels and other places. The distance between $3DLoc$ and the targets is around 45 meters. The measured azimuth angle difference is around $100°$ and the elevation angle difference is around $60°$. To test our system for short distance targets (the case that police car in the parking lot of a small hotel), we put $3DLoc$ six meters away from the target in an office. An office is actually a very complicated environment with intense signal reflection. This scene is denoted as *office case*.

To derive benchmarking reference angle and distance measurements, we purchased Pacific Laser Systems PLS5 System NEW 5 Beam Point-to Point Self Leveling Layout Laser with Detector [21] and Leica DISTO D8 [22].

An example demonstration of positioning in the office case is at *http://www.youtube.com/watch?v=EiLJoptgI28*.

5.2. Sampling Rate (Mobile Traffic Rate)

Theorem 2 gives the way of deriving minimum sampling rate for reconstructing an antenna RF pattern. Minimum sampling rate implies minimum mobile traffic rate required for accurate localization. Since the antenna RF pattern data is not provided by the company that produced it, we derive the raw RF pattern data indirectly from the images of RF pattern diagram shown in Figures 4 and 5. We measure a rotor's rotating function 20 times and use the average as the approximation. It takes about 60 seconds for both azimuth and elevation rotors to rotate the antenna system. Therefore, we can use the rotating functions and derived RF patterns for spectrum analysis. Figure 9 gives one instance of rotating functions for the azimuth and elevation antennas. It shows that our antennas rotate with time in an almost linear fashion based on regression analysis.

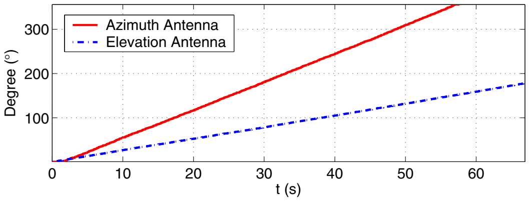

Figure 9. Antenna Rotating Functions

For the Azimuth antenna illustrated in Figure 4, we need to calculate the sampling rate based on the horizontal RF pattern. Its bandwidth is 0.13 pkts/s (packets/second) corresponding to a sampling rate of 0.26 pkts/s. For the elevation antenna illustrated in Figure 5, we need to calculate the sampling rate based on the vertical RF pattern. Its bandwidth is 1.65 pkts/s corresponding to a sampling rate of 3.30 pkts/s. Our experimental results below verified this theory on the sampling rate.

5.3. Angle Accuracy

In our experiments, obvious positioning errors such as scans without obvious peaks are excluded. Those cases are caused by extreme environment disturbance.

Figure 10 shows the mean error of estimated azimuth and elevation angles via wavelet decomposition when a mobile is put inside classrooms of the opposite building across the street from our office. The distance is around 45 meters. It can be seen that with the increasing sampling ratio, the mean error becomes stable. We can achieve almost zero azimuth angle estimation error and 2° elevation angle estimation error. Moreover, the required traffic rate (sampling rate) for achieving small angle error is small. For example, when the traffic rate is 6.14 pkts/s, the azimuth angle error is around 0.4° and the elevation angle error is around 2.4°. If a wireless frame is 1500 bytes, 6.14 pkts/s corresponds to 9.21 KBytes/s, which is a reasonably low requirement for localizing suspects using WiFi for malicious conducts such as downloading illegal multimedia. We observe similar low sampling rate in all later experiments.

Figures 11 and 12 compare the performance of maximum signal strength (MaxSS) and wavelet denoising. In the approach of MaxSS, we extract the angles corresponding to the multiple measured maximum signal strength points from the raw measurements and use the median one as the mobile angle. By adopting the median angle, MaxSS removes the impact of noise to some extent. We can see that overall the wavelet denoising approach achieves better performance. It has a smaller angle estimation confidence interval. The estimation achieves much better performance in the azimuth angle estimation and similar performance in the elevation angle estimation. The wavelet denoising algorithm produces more trustable results than MaxSS.

$3DLoc$ also excels in short distance. Figure 13 shows the mean error of estimated azimuth and elevation angles via wavelet decomposition when a mobile is put inside an office. It can be seen that with the increasing sampling ratio, the mean error becomes stable. We achieve almost zero azimuth angle estimation error and 1° elevation angle estimation error. Moreover, the required traffic rate (sampling rate) for achieving small angle error is small. For example, when the traffic rate is 6.14 pkts/s, the error is around 1°.

Figures 14 and 15 compare the performance of two angle estimation approaches in the office case. We can see that overall the wavelet denoising approach achieves better performance. It has a smaller angle estimation confidence interval. The estimation achieves much better performance in the azimuth angle estimation and equal performance in the elevation angle estimation. The wavelet denoising algorithm produces more trustable results than MaxSS.

The small angle estimation error makes $3DLoc$ a realistic toolkit for law enforcement. At an angle estimation error ϵ_a in radian, the absolute distance error ϵ_d for locating the target can be approximated as follows,

$$\epsilon_d \approx \epsilon_a d, \tag{10}$$

where d is the distance from the antennas to the target mobile. Therefore, angle errors of 1° and 2° correspond to distance errors of 0.87 and 1.75 meters when the mobile is 50 meters away from the antennas. Theorem 1 tells us that for good localization, the law enforcement cannot be too far away from the target in complicated environments.

6. Related Work

There has been a large body of work on device positioning in WiFi and sensor networks. Due to space limitation, we only review the existing work most related to our paper:

Most existing techniques provide localization in a two-dimensional space (e.g., longtitude/latitude) only. Positioning systems are classified as outdoor and indoor systems, respectively, which feature vastly different requirements and techniques. The most popular outdoor positioning system is GPS [23]. Many cellular mobile networks also belong to this category, and allow the tracking of powered-on devices through the operator's base-transceiver stations. Indoor positioning systems include RADAR [24], LANDMARC

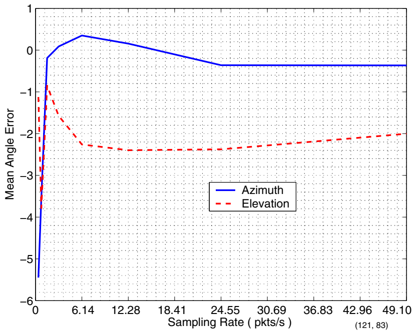

Figure 10. Mean Angle Estimation Error - Remote Case

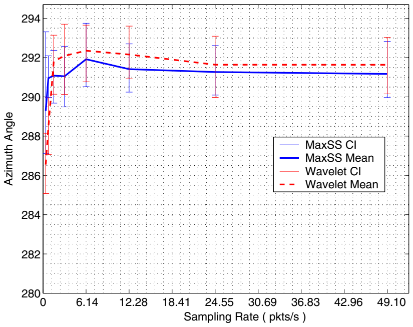

Figure 11. Azimuth Angle vs Sampling Rate - Remote Case (Reference azimuth angle $292°$)

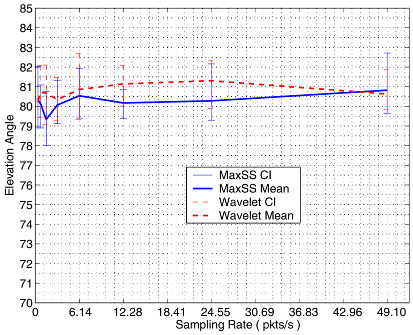

Figure 12. Elevation Angle vs Sampling Rate - Remote Case (Reference elevation angle $80°$)

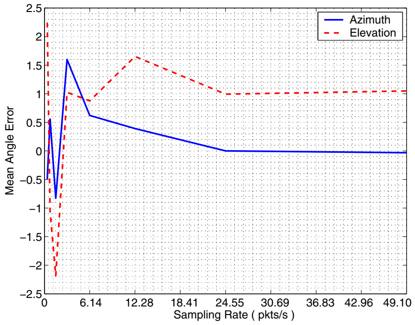

Figure 13. Mean Angle Estimation Error - Office Case

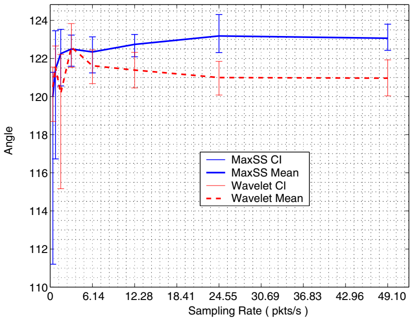

Figure 14. Azimuth Angle vs Sampling Rate - Office Case (Reference azimuth angle $121°$)

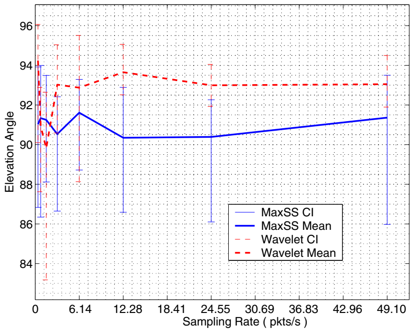

Figure 15. Elevation Angle vs Sampling Rate - Office Case (Reference elevation angle $92°$)

[1], the digital Marauder's Map [5], Lighthouse [25], and VORBA [2]. All these systems position a mobile device based on the measured signal strength. In particular, the former three utilize a dense grid of omnidirectional base stations, while the latter two rely on base stations with revolving unidirectional antennas. Active Badge [26], Active Bat [27] and Cricket [28] can provide better localization accuracy than outdoor systems due to the usage of a large number of positioning-support sensors.

In [29], the authors use electronically steerable Phocus Array antennas from Fidelity Comtech [30] for wardriving and collecting RSSIs with directional information. Multiple measurements are taken at different positions and arrows are drawn in the direction of the AP. Therefore, an AP is at the position which all the arrows point to. In [3], the authors take RSSIs from wardriving and use the gradient information derived from RSSIs to infer the position of an AP. An AP is in the direction along which RSSIs increase the most and the direction is represented by an arrow. Then the AP is at the position all arrows point to. In [31], the authors built an AP equipped with a rotating directional antenna that broadcasts its direction in beacon frames. Such an AP is denoted as a directional beaconing access point (DBAP). Therefore, a mobile may position itself by using the angle of emission information from multiple DBAPs and the area intersection approach similar to those used in [2].

Some recent work recognizes the importance of 3D positioning and provides such capability [32], [33]. Nonetheless, these techniques require either the pre-installation of a positioning infrastructure (e.g., pervasive RFID tags [32]), or extensive training on the signal strength of surrounding base stations at different locations [33]. These strategies are not practical for WiFi in urban environments due to the associated high cost of periodical training due to environment and infrastructure change and the requirement of locating a suspect in real time (i.e., it will be hard to install the infrastructure or perform training on a crime scene).

7. Conclusion

In this paper, we developed $3DLoc$, a three dimensional localization system for 802.11-compliant mobile devices. $3DLoc$ consists of two antennas: azimuth antenna with wide vertical beamwidth and narrow horizontal beamwidth and elevation antenna with both narrow vertical and horizontal beamwidth. The two antennas are steered by a pair of chained rotors: azimuth rotor and elevation rotor. A set of localization algorithms have been proposed. A density-based clustering technique is used to remove reflected WiFi signals. We conducted a careful analysis of the angle estimation error sources and proposed to use Wavelet transform techniques in order to filter out the noise. We derived the minimum required mobile traffic rate for successful localization based on the antenna RF pattern and Nyquist sampling theory. Our experiments validate the effectiveness of $3DLoc$, which has an error of around 1° azimuth angle estimation error, 2° elevation angle estimation error.

$3DLoc$ can also be used for other applications such as wireless network monitoring for identifying non-compliant wireless network devices and topology discovery in addition to wireless network forensics. Our future work includes further experiments in unfriendly environments and calibration of $3DLoc$ and refinement of its structure design to increase the portability for various applications.

References

[1] L. M. Ni, Y. L. Yiu, C. Lau, and A. P. Patil, "LANDMARC: Indoor location sensing using active RFID," in *Proceedings of PerCom*, 2003, pp. 407–415.

[2] D. Niculescu and B. Nath, "VOR base stations for indoor 802.11 positioning," in *Proceedings of MOBICOM*, 2004.

[3] D. Han, D. G. Andersen, M. Kaminsky, K. Papagiannaki, and S. Seshan, "Access point localization using local signal strength gradient," in *Proceedings of Passive & Active Measurement (PAM)*, 2009.

[4] Federal Communications Commission, "Enhanced 911 - wireless services," http://www.fcc.gov/911/enhanced/, 2006.

[5] X. Fu, N. Zhang, A. Pingley, W. Yu, J. Wang, and W. Zhao, "The digital marauder's map: A new threat to location privacy in wireless networks," in *Proceedings of ICDCS*, 2009.

[6] Arkasha and Bobzilla, "WiGLE - wireless geographic logging engine - plotting wifi on maps," http://www.wigle.net/, 2008.

[7] Agere Systems Inc., "WDS (wireless distribution system)," http://www.pafree.net/media/TB-046.pdf, 2002.

[8] W. Yu, X. Fu, S. Graham, D. Xuan, and W. Zhao, "Dsss-based flow marking technique for invisible traceback," in *Proceedings of the 2007 IEEE Symposium on Security and Privacy (S&P)*, 2007.

[9] X. Fu, Y. Zhu, B. Graham, R. Bettati, and W. Zhao, "On flow marking attacks in wireless anonymous communication networks," in *Proceedings of ICDCS*, 2005.

[10] Z. Ling, J. Luo, W. Yu, X. Fu, D. Xuan, and W. Jia, "A new cell counter based attack against tor," in *Proceedings of 16th ACM Conference on Computer and Communications Security (CCS)*, 2009.

[11] "Yaesu g5500 - complete az-el rotation system," http://www.universal-radio.com/CATALOG/hamrot/ysurot.html, 2009.

[12] "Antenna rotator system - rci boards," http://www.ea4tx.com/products/ars-rci.htm, 2009.

[13] V. Bhavsar, N. Blas, and H. Nguyen, "Measurement of antenna radiation patterns laboratory manual," http://ndl.ee.ucr.edu/manual.pdf, 2000.

[14] A. K. Jain and R. C. Dubes, *Algorithms for clustering data*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1988.

[15] D. B. Faria, "Modeling signal attenuation in IEEE 802.11 wireless lans - vol. 1." Stanford University, Tech. Rep., July 2005.

[16] G. D. Durgin, T. S. Rappaport, and H. Xu, "Measurements and models for radio path loss and penetration loss in and around homes and trees at 5.85 ghz," *ACM Transactions on Communications*, vol. 46, no. 11, pp. 1484–1496, 1998.

[17] M. Misiti, Y. Misiti, G. Oppenheim, and J.-M. Poggi, "Wavelet toolbox 4 users guide," http://www.mathworks.com/access/helpdesk_r13/help/pdf_doc/wavelet/wavelet_ug.pdf, pp. 6–66, march 2009.

[18] I. Johnston, "An introductory handbook on probability, statistics, and excel — section four: Correlation," http://records.viu.ca/~Johnstoi/maybe/maybe4.htm, 2009.

[19] R. Hekmat and P. V. Mieghem, "Degree distribution and hopcount in wireless ad-hoc networks," in *Proceedings of The 11th IEEE International Conference on Networks (ICON)*, 2003.

[20] T. S. Rappaport, *Wireless Communications: Principles and Practice (2nd Edition)*. Prentice Hall PTR, 2002.

[21] "Pacific laser systems pls-60541 pls5 5 beam point-to point self leveling layout laser," http://www.amazon.com/Pacific-Laser-Systems-pls-60541-Leveling/dp/B001F2GU9M, 2009.

[22] "Leica disto d8, the versatile one for in- and outdoor," http://ptd.leica-geosystems.com/en/Laser-Distancemeter-Leica-DISTO-D8_78069.htm, 2009.

[23] P. Enge and P. Misra, "Special issue on global positioning system," *Proceedings of the IEEE*, vol. 87, no. 1, pp. 3–15, January 1999.

[24] P. Bahl and V. N. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," in *Proceedings of INFOCOM*, 2000.

[25] K. Römer, "The lighthouse location system for smart dust," in *Proceedings of MobiSys*, 2003.

[26] R. Want, A. Hopper, V. Falcao, and J. Gibbons, "The active badge location system," *ACM Transactions on Information Systems*, vol. 10, no. 1, January 1992.

[27] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster, "The anatomy of a context-aware application," in *Proceedings of MOBICOM*, 1999.

[28] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, "The Cricket Location-Support System," in *Proceedings of MOBICOM*, 2000.

[29] A. P. Subramanian, P. Deshpande, J. Gao, and S. R. Das, "Drive-by localization of roadside wifi networks," in *Proceedings of INFOCOM*, 2008.

[30] Fidelity Comtech, Inc., "802.11 phocus array antenna system by fidelity comtech," http://www.fidelity-comtech.com/, 2009.

[31] K. Kawauchi, T. Miyaki, and J. Rekimoto, "Directional beaconing: A robust wifi positioning method using angle-of-emission information," in *Proceedings of LoCA*, 2009.

[32] C. Wang, H. Wu, and N.-F. Tzeng, "Rfid-based 3-d positioning schemes," in *Proceedings of INFOCOM*, 2007.

[33] A. Varshavsky, A. LaMarca, J. Hightower, and E. de Lara, "The skyloc floor localization system," in *Proceedings of PerCom*, 2007.