11-2013

From RSSI to CSI: Indoor localization via channel response

Zheng YANG

Zimu ZHOU
Singapore Management University, zimuzhou@smu.edu.sg

Yunhao LIU

From RSSI to CSI: Indoor Localization via Channel Response

ZHENG YANG, Tsinghua University
ZIMU ZHOU, Hong Kong University of Science & Technology
YUNHAO LIU, Tsinghua University

The spatial features of emitted wireless signals are the basis of location distinction and determination for wireless indoor localization. Available in mainstream wireless signal measurements, the Received Signal Strength Indicator (RSSI) has been adopted in vast indoor localization systems. However, it suffers from dramatic performance degradation in complex situations due to multipath fading and temporal dynamics.

Break-through techniques resort to finer-grained wireless channel measurement than RSSI. Different from RSSI, the PHY layer power feature, channel response, is able to discriminate multipath characteristics, and thus holds the potential for the convergence of accurate and pervasive indoor localization. Channel State Information (CSI, reflecting channel response in 802.11 a/g/n) has attracted many research efforts and some pioneer works have demonstrated submeter or even centimeter-level accuracy. In this article, we survey this new trend of channel response in localization. The differences between CSI and RSSI are highlighted with respect to network layering, time resolution, frequency resolution, stability, and accessibility. Furthermore, we investigate a large body of recent works and classify them overall into three categories according to how to use CSI. For each category, we emphasize the basic principles and address future directions of research in this new and largely open area.

Categories and Subject Descriptors: C.2.m [**Computer-Communication Networks**]: Miscellaneous

General Terms: Design, Algorithms

Additional Key Words and Phrases: Indoor localization, RSSI, CSI, human detection

ACM Reference Format:
Yang, Z., Zhou, Z., and Liu, Y. 2013. From RSSI to CSI: Indoor localization via channel response. ACM Comput. Surv. 46, 2, Article 25 (November 2013), 32 pages.
DOI: http://dx.doi.org/10.1145/2543581.2543592

1. INTRODUCTION

Wireless indoor localization spawns numerous location-based applications in a wide range of living, production, commence, and public services. This flourish of mobile and pervasive computing has sharpened the urge for accurate, robust, and off-the-shelf indoor localization schemes. Compared with outdoor positioning, indoor localization is more challenging, since GPS signals are rarely accessible, yet room-level or even submeter precision is often required. Due to the ubiquitous deployment of wireless networks and devices, the past two decades have witnessed extensive wireless indoor localization techniques, including acoustic signals [Peng et al. 2007; Yang et al. 2011], ultrasound [Harter et al. 1999; Priyantha et al. 2000], FM [Chen et al. 2012], infrared

This work is supported in part by the NSFC under grant 61171067, the NSFC Major Program under grant 61190110, and the NSFC Distinguished Young Scholars Program under grant 61125202.
Authors' addresses: Z. Yang and Y. Liu, School of Software and TNList, Tsinghua University, Beijing, China; Z. Zhou, Department of Computer Science & Engineering, Hong Kong University of Science & Technology, Hong Kong.

DOI: http://dx.doi.org/10.1145/2543581.2543592

[Want et al. 1992], RFID [Ni et al. 2004; Zhao et al. 2007], Bluetooth [Bargh and de Groote 2008], cellular [Otsason et al. 2005; ur Rehman et al. 2008], ZigBee [Zhang and Ni 2009; Wilson and Patwari 2010], WiFi [Bahl and Padmanabhan 2000; Youssef and Agrawala 2005; Youssef et al. 2007], UWB [Fontana 2004; Gezici et al. 2005], etc. In essence, the spatial features of emitted wireless signals lay the basis of location distinction and determination.

Available in mainstream wireless signal measurements, the Received Signal Strength Indicator (RSSI) characterizes the attenuation of radio signals during propagation and has been adopted in a large body of indoor localization systems. Although RSSI (used as either a radio fingerprint or path loss power) can achieve meter-level localization accuracy in simple environments, it suffers from dramatic performance degradation in complex situations due to multipath fading and temporal dynamics. Most of the present reliable RSSI-based positioning systems still stay at room-level accuracy, answering the location query like which room people or assets are in.

Break-through techniques resort to finer-grained wireless channel measurement than RSSI. Different from RSSI as the MAC layer superimposition of multipath signals with fast changing phases, the PHY layer power feature, channel response, is able to discriminate multipath characteristics. In a conceptual sense, channel response is to RSSI what a rainbow (color spectrum) is to a sunbeam, where components of different wavelengths are separated.

Previously, channel response was measured by professional equipment [Nerguizian et al. 2006; Nerguizian and Nerguizian 2007; Patwari and Kasera 2007; Zhang et al. 2008], obstructing its wide usability. However, the popularity of WiFi and Orthogonal Frequency Division Multiplexing (OFDM) technology has changed the landscape. In 802.11 a/g/n standards, channel response can be partially extracted from off-the-shelf OFDM receivers in the format of Channel State Information (CSI), which reveals a set of channel measurements depicting the amplitudes and phases of every subcarrier [Halperin et al. 2010]. Some pioneer works based on CSI have demonstrated submeter-level accuracy for location determination with only WiFi-compatible Network Interface Cards (NICs) [Wu et al. 2012; Sen et al. 2012b]. Such results definitely advance wireless indoor localization to a broader range of applications.

As the PHY layer counterpart of RSSI, CSI holds potential for the convergence of accurate and pervasive indoor localization and has attracted numerous recent research efforts [Wu et al. 2012; Sen et al. 2012b; Zhang et al. 2012a; Sen et al. 2012a; Xiao et al. 2012b; Zhou et al. 2013].

In this article, we surveyed this new trend of channel response in localization. The differences between CSI and RSSI are highlighted with respect to network layering, time resolution, frequency resolution, stability, and accessibility. We also investigated a large body of recent works and classified them overall into three categories according to how CSI is used: (i) extracting the radio power of individual multipath components as ranging metric or radio fingerprint; (ii) estimating time or angle information with dedicated signal sources; (iii) analyzing the influence of human presence and mobility on CSI to implement device-free passive human detection and localization. For each category, we emphasize the principles and address future avenues in this new and largely open area of location-aware technologies. We conclude with the development and opportunity of channel response measurement in nowadays 802.11 standards.

2. WIRELESS INDOOR LOCALIZATION OVERVIEW

In general, wireless indoor localization schemes map *physical measurements* derived from wireless signals into either geometric parameters such as relative distance and direction from the reference points, or prelabeled landmarks directly. This section

first reviews conventional physical measurements, followed by two classical mapping methods, *geometric mapping* and *fingerprinting*.

2.1. Physical Measurements

Power, *time,* and *angle* features are among conventional physical measurements and vary in accessibility, complexity, and accuracy.

2.1.1. Power. Signal power is widely used in both geometric mapping (especially in ranging) and fingerprinting due to its handy access. The MAC layer signature, RSSI, is one of the most prevalent power features, which is accessible in wireless techniques ranging from UWB, ZigBee, and WiFi to cellular networks. The main drawback of RSSI lies in its temporal fluctuations in complex indoor environments, making it a fickle and coarse-grained feature. The multipath-rich indoor environment complicates the wireless propagations and derails RSSI-based ranging. More accurate power-based ranging needs better characterizing and modeling of the small-scale multipath effects [Wu et al. 2012]. Practical WLAN fingerprinting, on the other hand, compensates for the unreliability of RSSI by peer-assisted error control [Liu et al. 2012a] or rich sensor hints [Azizyan et al. 2009].

2.1.2. Time. Typical time features extracted from wireless signals include Time Of Arrival (TOA) and Time Difference Of Arrival (TDOA) and are commonly employed in ranging. In general, time-based ranging is impressively accurate under Line-Of-Sight (LOS) conditions. Unlike power-based schemes, the accuracy of time- based ranging improves with signal bandwidth. Ultra-Wide Bandwidth (UWB) radio therefore enjoys sheer prevalence due to its high time resolution and extremely large bandwidth [Gezici et al. 2005]. Another line of research focuses on long wavelength signals like acoustic signals on off-the-shelf platforms [Yang et al. 2011; Zhang et al. 2012b; Nandakumar et al. 2012]. The main drawback of time-based ranging is that external signal sources are often required, inducing additional energy consumption. Moreover, high-resolution time-based schemes require a high Analog-Digital Converter (ADC) sampling rate at the PHY layer.

2.1.3. Angle. Angle information provides an orthogonal dimension with regard to distance for geometric mapping. Angle can be combined with distance estimates to enable single-anchored localization. Compared with distance estimates, though, the cost of angle measurements is higher. Directional antennas are often capable of obtaining both angle and distance estimates while avoiding interferences from other directions, yet at the cost of dedicated infrastructure [Niculescu and Nath 2004; Pongthawornkamol et al. 2010; Cidronali et al. 2010]. A tricky alternative is to involve human interaction in angle estimation [Zhang et al. 2011; Sen et al. 2012a]. Recently, antenna arrays have also attracted increasing interest with the rapid development of Multiple Input Multiple Output (MIMO) techniques [Xiong and Jamieson 2012, 2013].

2.2. Mapping Methods

To convert physical measurements into locations, mainstreams adopt either *geometric mapping* or *fingerprinting*.

2.2.1. Geometric Mapping. In geometric mapping, intermediate geometric parameters such as distance or direction with regard to the reference points are first derived from certain physical measurements. These relative parameters are then converted into locations using geometric algorithms (e.g., triangulation). Distance-based mapping, in particular, is often termed as *ranging* and is more popular than direction-based mapping since, in general, direction measurements are more difficult to derive with

pervasive devices. Nevertheless, *direction* information is directly measurable at the receiver, while the derivation of *distance* involves wireless propagation rules. The prevalent Log-normal Distance Path Loss (LDPL) model, for instance, relates the received signal power to the propagation distance and forms the basis for power-based ranging. Other techniques derive time parameters such as TOA and TDOA and calculate distances based on geometric relations of propagating paths.

Despite its clear physical underpinning, the performance of geometric mapping heavily relies on LOS conditions. The rich multipath effects indoors, though, often blur the monotonous relations between physical measurements and distances, complicate propagation modeling, and degenerate ranging accuracy. Furthermore, as discussed in Section 2.1, it often involves a high sampling rate and dedicated infrastructure to obtain the desired time or angle measurements as inputs for geometric mapping.

2.2.2. Fingerprinting. As an alternative to analyzing sophisticated signal propagations, fingerprinting adopts a pattern-matching approach. The main idea is to collect signal features of all possible locations in the area of interest to build a fingerprint database (known as site survey or calibration). Localization is then simply the process of matching the measured fingerprints at an unknown location with those in the database and returning the location corresponding to the best-fitted fingerprint.

Fingerprinting-based schemes relax the requirements on the physical measurements to be discriminative and reproducible. Features at each location should differ from all the others to avoid ambiguity, and the fingerprints of the same location measured at different times should resemble each other to ensure the effectiveness of the database.

The primary drawback of fingerprinting lies in its cumbersome efforts when building and updating the database. Recently, there has been active research in reducing or crowdsourcing this manual labor [Wu et al. 2013; Yang et al. 2012; Wang et al. 2012].

2.3. Summary

Although the scope of this survey is restricted to wireless signals, the current trend to employ sensor-rich smartphones for indoor localization has extended the concept of physical measurements to a partially semantic perspective. Some schemes integrate ambience features (e.g., sound, light, color, WiFi, etc.) to perform logical localization (i.e., locations are labeled as Starbucks and McDonalds, etc.) [Azizyan et al. 2009]. Others utilize human mobility by stitching traces recorded by inertial sensors [Constandache et al. 2010; Rai et al. 2012]. These sensor hints have improved localization accuracy in a human-centric and context-aware manner and are complementary to wireless-based features. In this survey, we mainly focus on signal power features due to their widespread adoption and easy accessibility and review novel interplays among time, angle, and power features.

As for the mapping methods, the principles have remained almost identical for decades, yet careful consideration is needed when designing localization systems with specific physical measurements. During our review on channel response- based localization, we strive to explain how appropriate features are tailored for different mapping methods.

3. FROM RSSI TO CHANNEL RESPONSE

The primary hurdle in wireless indoor localization lies in the rich multipath fading and temporal dynamics indoors. Albeit ubiquitous, traditional power features like RSSI fail to provide sufficient distinction and robustness in complex indoor environments, as RSSI is the superimposition of multipath signals with fast changing phases.

Originated from wireless channel sounding, several recent works have dived deep into the PHY layer and leveraged the finer-grained power feature, channel response,

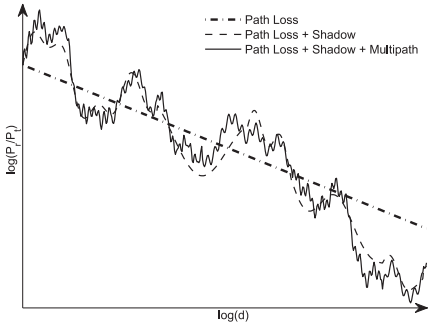

Fig. 1. Spatial variations due to multipath.

to discriminate multipath characteristics. This section aims to provide the basics for this new feature.

3.1. RSSI Variation Due to Multipath Shadowing

In a typical indoor environment, a transmitted signal propagates to the receiver through multiple paths. Each path contributes to a differently delayed, attenuated, and phase-shifted signal. Hence, the received signal is a combination of numerous alias versions of the original signal. The complex baseband signal voltage measured at the receiver at a specific time, therefore, is denoted as [Patwari and Wilson 2011]:

$$V = \sum_{i=1}^{N} \|V_i\| e^{-j\theta_i}, \tag{1}$$

where V_i and θ_i are the amplitude and phase of the i^{th} multipath component (note that the signal modulation schemes are implicitly considered), and N is the total number of components. RSSI is then simply the received power in decibels (dB):

$$RSSI = 10 \log_2 \left(\|V\|^2 \right). \tag{2}$$

As a superposition of multipath components, RSSI not only varies over distance on the order of the signal wavelength but also fluctuates over time even at a static link. A slight change in certain multipath components may add up to significant constructive or destructive relative phases of the delayed signals, which, as a consequence, lead to considerable fluctuations in RSSI. In fact, the variations of RSSI even at an immobile receiver in 1 minute can be as large as 5 dB in a typical laboratory environment [Wu et al. 2012]. Other empirical studies have also shown that RSSI readings vary at both small (seconds) and large (hours) granularities and can be as high as 7 dB in a typical student cubicle [Lim et al. 2006].

3.2. Effect of RSSI Variation on Localization

3.2.1. Ranging Bound. In power-based ranging, RSSI is mapped into the distance from the transmitter by the prevalent Log-normal Distance Path Loss (LDPL) model [Seidel and Rappaport 1992]:

$$PL(d)[dB] = \overline{PL(d_0)} + 10n \lg \left(\frac{d}{d_0} \right) + X_\sigma, \tag{3}$$

where $PL(d)$ denotes the measured path loss at distance d. $\overline{PL(d_0)}$ is the average path loss at reference point d_0 and n is the path loss exponent. X_σ is a zero-mean normal random variable reflecting the attenuation in decibel caused by shadowing.

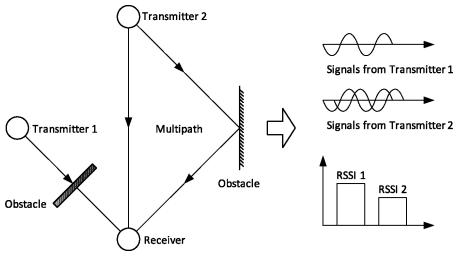

Fig. 2. Destructive phase superposition.

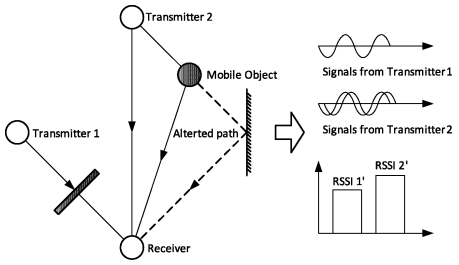

Fig. 3. Constructive phase superposition.

The LDPL model characterizes the variation of received signal power over distance due to path loss and shadowing. Path loss stems from the dissipation of transmission power in the propagation channel, while shadowing results from the obstacles that attenuate signal power through absorption, reflection, scattering, and diffraction.

As discussed in Section 2, power-based ranging assumes that RSSI monotonically decreases with distance. In theory, the average path loss strictly follows such trend. Due to the random shadowing effect X_σ, though, the monotonic trend only holds on a relatively large scale, which is bounded by the variance of shadowing σ. The multipath-rich indoor environment leads RSSI to fluctuate on the order of signal wavelength and contributes to large shadowing X_σ. As a result, it is almost impossible to distinguish locations in the vicinity, because the large deviation of multipath shadowing blurs the monotonic trend. This fundamentally limits the accuracy of RSSI-based ranging. As illustrated in Figure 1, the combined effects of path loss, shadow, and multipath contribute to significant variations of the ratio between the received power P_r and the transmitted power P_t in dB with regard to distance d in logarithm [Goldsmith 2005].

3.2.2. Fingerprint False Match. The complex indoor wireless propagating conditions also derail the performance of RSSI-based fingerprinting. Concretely, it is common that environmental dynamics such as humans or moving objects may affect a portion of the multipath components, which contribute to amplitude fluctuations of received signals. As an illustration, given the multipath conditions from Transmitter 2 to the Receiver (Figure 2), the received signals from Transmitter 2 result in destructive phases and thus reduced RSSI. In contrast, some dynamic obstacles (e.g., moving handhelds in an office or the opening and closing of doors) in Figure 3 might temporarily alter the multipath conditions. Consequently, it is possible that the previous destructive phases turn into constructive ones, hence contributing to enhanced RSSI for Transmitter 2. These temporal fluctuations of RSSI due to environmental dynamics at a stationary receiver induce a mismatch between the prestored fingerprints in the database (e.g., the 2D vector fingerprint $\{RSSI1, RSSI2\}$ in Figure 2) and the measured ones even at the same location ($\{RSSI1', RSSI2'\}$ in Figure 3). Thus, the matching performance degrades as the previous radio map no longer reflects the current statistical signal characteristics.

3.3. Characterizing Multipath

The fundamental drawback of RSSI is that it fails to capture the multipath effects. To fully characterize the individual paths, the wireless propagation channel is modeled as a temporal linear filter, known as Channel Impulse Response (CIR). Under the

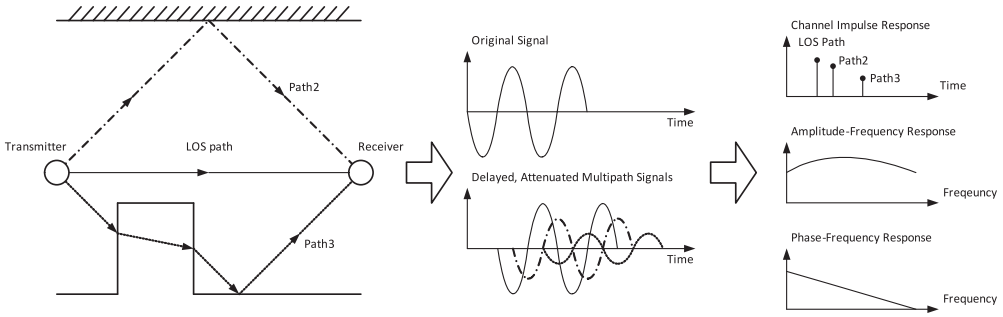

Fig. 4. Multipath propagations, received signals, and channel responses.

time-invariant assumption, CIR $h(\tau)$ is denoted as:

$$h(\tau) = \sum_{i=1}^{N} a_i e^{-j\theta_i} \delta(\tau - \tau_i), \tag{4}$$

where a_i, θ_i, and τ_i are the amplitude, phase, and time delay of the i^{th} path, respectively. N is the total number of multipath and $\delta(\tau)$ is the Dirac delta function. Each impulse represents a delayed multipath component, multiplied by the corresponding amplitude and phase.

In the frequency domain, the constructive and destructive phases also cause frequency-selective fading, which is characterized as the Channel Frequency Response (CFR). CFR consists of amplitude-frequency response and phase-frequency response. Figure 4 shows a multipath propagating condition, the transmitted signals and the received signals, and illustrative channel responses. Given infinite bandwidth, CIR is equivalent to CFR. And CFR is the Fourier transform of CIR.

Both CIR and CFR depict the small-scale multipath effect and are widely used for channel measurement. Note that CIR and CFR are with respect to complex *amplitude*, while another pair of parameters in terms of signal *power* is Power Delay Profile (PDP) and Power Spectrum Density (PSD).

To sum up, channel response is to RSSI what a rainbow is to a sunbeam, where components of different wavelengths are separated. Channel response possesses finer-grained frequency resolution and equivalently higher time resolution to distinguish multipath components, yet at the cost of slight modification of firmware or hardware on off-the-shelf platforms, just as the prism used to disperse the sunlight. Table I offers a brief comparison of channel response and RSSI. Note that although CIR resembles a sequence of RSSI, the underlying time resolution is much higher, and thus differs from RSSI sequence-based localization [Fang and Lin 2010]. On the other hand, it is possible to obtain raw received signal power at the PHY sampling rate with a modified wireless adapter [Golden and Bateman 2007]. To avoid ambiguity, we restrict the concept of RSSI as the value reported from the MAC layer in this survey.

3.4. Deriving Channel Response

In the time domain, the received signal $r(t)$ is the temporal convolution of transmitted signal $s(t)$ and channel impulse response $h(t)$:

$$r(t) = s(t) \otimes h(t). \tag{5}$$

Accordingly, the received signal spectrum $R(f)$ is simply the multiplication of the transmitted signal spectrum $S(f)$ and the channel frequency response $H(f)$ in the

frequency domain:

$$R(f) = S(f) \times H(f). \tag{6}$$

As demonstrated in Equations (5) and (6), CIR can be derived from the deconvolution of received and transmitted signals, while CFR is the ratio of the received and the transmitted spectrums. Since the calculation of convolution is nontrivial, the common trick to derive CIR is to convert temporal convolution into multiplication in the frequency domain, followed by an inverse Fourier transform. In case of a flat transmission power spectrum, CIR is approximated by [Patwari and Kasera 2007]:

$$h(t) = \frac{1}{P_s}\mathfrak{F}^{-1}\{S^*(f)R(f)\}, \tag{7}$$

where $\mathfrak{F}^{-1}$ denotes the inverse Fourier transform. $R(f)$ is the Fourier transform of the received signal $r(t)$, that is, its spectrum. $S^*(f)$ is the complex conjugate of the Fourier transform of the transmitted signal $s(t)$. And P_s approximates the transmitted signal power, which, under the flat transmission assumption, is nearly a constant within the band of interest.

Precisely measuring and modeling the wireless channel often involves dedicated infrastructures such as Vector Network Analyzer (VNA) or Software Defined Radio (SDR) [Nerguizian et al. 2006; Patwari and Kasera 2007; Zhang et al. 2008]. On the other hand, although the derivation of CIR/CFR is modulation independent, it might be more convenient to implement the process on commercial devices with particular modulation schemes. For instance, if OFDM is adopted, such as in IEEE 802.11a/g/n, the receivers are then readily capable of calculating CFR/CIR, since the amplitudes and phases on each subcarrier provide a sampled version of the signal spectrum, while FFT/IFFT operations are integrated in OFDM receivers.

Recent advances in the wireless community have taken this one step further. Leveraging the off-the-shelf Intel 5300 NIC and a modified driver, a group of sampled versions of CFRs within the WiFi bandwidth are revealed to upper layers in the format of Channel State Information (CSI) [Halperin et al. 2010]. Each CSI depicts the amplitude and phase of a subcarrier:

$$H(f_k) = \|H(f_k)\|e^{j\sin(\angle H)}, \tag{8}$$

where $H(f_k)$ is the CSI at the subcarrier with central frequency of f_k, and $\angle H$ denotes its phase. Hence a group of CSIs $H(f_k), (k = 1, \ldots, K)$, reveals K sampled CFRs at the granularity of subcarrier level.

In fact, this sample version of CFR has been employed in recent adaptive wireless communication systems to improve reliability [Halperin et al. 2010] and throughput [Bhartia et al. 2011], as well as for precise indoor localization on off-the-shelf platforms [Wu et al. 2012; Sen et al. 2012a; Sen et al. 2012b; Xiao et al. 2012a].

3.5. Summary

In the context of wireless indoor localization with pervasive devices, previous studies suggested that RSSI-based schemes, at best, can expect localization errors around 3 m and 9 m with probabilities of 50% and 97%, unless more complex environmental models or additional infrastructures are applied [Elnahrawy et al. 2004]. This survey has dipped one major environmental issue, multipath, and introduced the concept of channel response to characterize multipath effects. Recent works have reported 1.2m and 1.8m with probabilities of 50% and 90%, respectively, for CSI-assisted ranging [Wu et al. 2012], and mean accuracy of 89% for 1m $\times$ 1m boxes by CSI-based fingerprinting [Sen et al. 2012b]. The fundamental advance, as discussed throughout this section,

Table I. RSSI vs. Channel Response

Category	Layering	Resolution	Stability	Accessibility
RSSI	MAC	Time: Packet level Frequency: N/A	Low	Handy access
Channel Response	PHY	Time: Multipath cluster Frequency: Subcarrier level	High for CFR as a whole structure	WiFi NIC

is that RSSI is a coarse-grained and unstable signal power feature, while channel response, which depicts the multipath effects, opens a much broader designing space.

However, one concern is that the finer-grained channel response might also mean severer temporal fluctuations, since instead of a single-valued RSSI, now there are a set of random variables, each representing a propagating path. From an information-centric perspective, a set of joint random variables (i.e., multipath components) convey richer information (and naturally more randomness) compared with the summation of them (i.e., RSSI). It should be noted, though, that by carefully postprocessing the finer-grained yet potentially more temporally unstable multipath components, it is possible to derive a more robust and location-specific signal feature. In principle, for geometric mapping, it is achieved by separating the LOS path, which, if existing, resembles a marginal random variable, hence possessing a smaller variance than the summation of all paths. For fingerprinting, the objective is to derive a robust pattern from multipath components by leaning techniques, while RSSI can be considered as the trivial process of summating evenly over all paths. In the subsequent sections, we elaborate on the postprocessing procedures in practice.

4. THE POWER AS POWER

CIR depicts individual multipath components in the time domain and facilitates to separate the LOS path for accurate ranging. Also, both CIR and CFR offer features with higher dimensions, and thus finer-grained distinctions, which is appropriate for fingerprinting. This section reviews recent works on indoor localization with channel responses as power features. Table II lists several representative systems.

4.1. Mitigating Multipath Shading for Ranging

As discussed in Section 3.2, power-based ranging is based on radiation laws. More specifically, the power-distance relationship is characterized as [Rappaport 2002]:

$$P_r = \frac{P_t G_t G_r \lambda^2}{(4\pi d)^n}, \tag{9}$$

where P_r and P_t are the received and transmitted signal power, respectively. G_r and G_t denote the antenna gains at the receiver and transmitter, respectively. λ is the wavelength of the transmitted signal, d is the transmitted distance, and n is the environmental attenuation factor. In fact, Equation (9) is where Equation (3) originates and it is obvious that ranging is effective only when the transmitted distance d equals the transmitter-receiver distance, that is, when d corresponds to the LOS path.

Note that in Equation (9), the received power actually varies with wavelength, and hence frequency. On the other hand, as discussed in Section 3.3, *frequency diversity* also associates with multipath effects. Therefore, it is possible to resolve the LOS path and estimate its propagating distance by exploiting frequency diversity at the same location. And depending on whether *multipath mitigation* and *distance estimation* are integrated or conducted sequentially, two representative approaches follow.

4.1.1. Simultaneous Multipath Distance Estimation. Suppose there are N paths, each with a propagation distance $d_i, i = 1, \ldots, N$. And further assume each path reflects only once

Table II. Channel Response as Power Feature

System	Category	Platform	Performance	Limitations
MuD [Zhang et al. 2012a]	Ranging	TelosB	30% relative ranging error	Manual frequency sweep Low multipath resolution
FILA [Wu et al. 2012]	Ranging	WiFi NIC	1.8 m error	Low multipath resolution Insufficient bandwidth
WBNN-Locate [Nerguizian et al. 2006]	Fingerprinting	VNA	2 m for 90% trained data	Not off-the-shelf
PinLoc [Sen et al. 2012b]	Fingerprinting	WiFi NIC	89% accuracy 6% false positive	Intensive site survey Spot localization

with a reflection coefficient Γ_i. Assume d_1 corresponds to the LOS path and $\Gamma_1 = 1$, by definition. The received power of each path is then represented as a complex value $P(d_i, \Gamma_i, \lambda_k)$, with its amplitude proportional to the power of the i^{th} path and its phase denoting the corresponding time delay, and is measured at wavelength λ_k:

$$P(d_i, \Gamma_i, \lambda_k) = \frac{P_t G_t G_r \Gamma_i \lambda_k^2}{(4\pi d_i)^n} e^{-j\frac{2\pi d_i}{\lambda_k}}, \tag{10}$$

where d_i and Γ_i are the propagation distance and reflection coefficient of the i^{th} path, respectively.

The total received power P_k measured at frequency $f_k = c/\lambda_k$ is then the summation over all the N multipath components:

$$P_k = \left\| \sum_{i=1}^{N} P(d_i, \Gamma_i, \lambda_k) \right\|. \tag{11}$$

The set of received power measured at K frequencies is proportional to channel amplitude-frequency response, that is, the amplitude of CFRs.

Zhang et al. [2012a] built a tracking system named MuD based on a set of equations as in Equation (11) by assigning $n = 2$. Orthogonal decomposition is then applied to these equations and a function $P(x, \lambda_k) : \mathbb{R}^{2N} \to \mathbb{R}$ is obtained:

$$P(x, \lambda_k) = c\lambda_k^2 \left(\left(\sum_{i=1}^{N} \frac{\Gamma_i \cos\left(\frac{d_i}{\lambda_k}\right)}{d_i^2} \right)^2 + \left(\sum_{i=1}^{N} \frac{\Gamma_i \sin\left(\frac{d_i}{\lambda_k}\right)}{d_i^2} \right)^2 \right)^{\frac{1}{2}}, \tag{12}$$

where $x = (c, \Gamma_2, \ldots, \Gamma_N, d_1, \ldots, d_N) \in \mathbb{R}^{2N}$, and $c = \frac{P_t G_t G_r}{(4\pi)^2}$.

The solution to this set of equations is formulated as a curvature fitting problem. The problem, however, normally has no stable solution. To obtain a feasible solution for the nonlinear optimization, the authors employed practical constraints to convert the ill-conditioned numerical problem into a well-conditioned one. The constant c is hardware related and therefore derivable from hardware manuals or measurable via chamber training. The number of paths and the propagation distances and reflection coefficients for the Non-Line-Of-Sight (NLOS) paths are also bounded to simplify the problem.

MuD is implemented on TelosB nodes by configuring the nodes to rapidly switch channels for signal measurements at different frequencies. Due to the limited number of channels provided in ZigBee, at most 16 measurements at different frequencies are available, which fundamentally bounds the number of resolvable paths.

In a nutshell, this approach combines distance estimation and multipath mitigation into a set of nonlinear equations exploiting frequency diversity and strives to solve all parameters simultaneously. Despite its simplicity in building up the equations,

the large amount of unknown variables and the nonlinearity of the problem make the theoretical solutions numerically unstable without practical constraints. In terms of implementation, sequentially measuring multiple channels is similar to a manual frequency sweep for channel sounding. Nevertheless, high-resolution frequency sweep involves dedicated channel sounders.

4.1.2. Extracting LOS Path for Ranging. Although frequency diversity reflects multipath effects from the spectral perspective, the multipath components actually twist in the frequency domain. Therefore, it might be necessary to resolve all multipath components as in MuD, even though only the LOS path is needed for ranging. Intuitively, since different paths propagate to the receiver with distinguishable time delays, it is more natural to extract only the LOS path from the time domain for ranging and ignore all other paths.

Wu et al. [2012] proposed to extract the dominant cluster of paths from CIR for accurate ranging. The prototype, FILA, is implemented on OFDM-based WiFi with off-the-shelf NICs. Unlike ZigBee, modern radio like OFDM adopts multicarrier modulation, where symbols are transmitted through multiple carriers simultaneously. Thus, the manual frequency sweep operation in Zhang et al. [2012a] is embedded in multicarrier radios, in a parallel manner. Consequently, a sampled version of CFR is already exposed in the PHY layer. These CFR samples are then converted into CIRs by inverse Fourier transform. After obtaining CIR, FILA takes a threshold-based method to separate the signal power corresponding to the LOS path. More specifically, given a measured CIR $h(\tau)$, the paths with amplitudes smaller than 50% of the first peak value in $h(\tau)$ are filtered out, thus retaining the LOS or the shortest NLOS paths.

Instead of applying the radiation rules directly, the filtered CIR samples are once again converted into the frequency domain. Note in Equation (9), the received power P_r is a function of the transmitted wavelength λ and therefore the frequency of the subcarrier. FILA adopts a weighted summation on the filtered CSIs to normalize the power to the central frequency within the band:

$$CSI_{eff} = \frac{1}{K} \sum_{k} \frac{f_k}{f_c} \times \|A\|_k, \tag{13}$$

where CSI_{eff} is the final input for distance estimation. K is the total number of subcarriers. f_c is the central frequency, and $\|A\|_k$ is the amplitude of the filtered CSI on the k^{th} subcarrier. The propagation distance approximating the LOS path d_{LOS} is then calculated as:

$$d_{LOS} = \frac{1}{4\pi} \left[\left(\frac{v}{f_c \times CSI_{eff}} \right)^2 \times \sigma \right]^{\frac{1}{n}}, \tag{14}$$

where v is the velocity of the transmitted wave, n is the attenuation factor, and σ denotes all other hardware factors including transmitted power, antenna gains, and so forth. The parameters n and σ are pretrained for each indoor scenario.

Although the ranging accuracy of FILA improves impressively by exploiting CSI instead of RSSI, the time resolution of the derived CIR samples remains only sufficient to distinguish clusters of paths rather than individual multipath components due to the limited bandwidth in current WiFi protocols. We envision that future WiFi protocols with larger bandwidth would further improve the performance of fine-grained power-based ranging.

4.2. Exploiting Multipath Signature for Fingerprinting

As discussed in Section 2.2, the signal features extracted for fingerprinting should be distinguishable across space and reproducible over time. Channel response is a good

Table III. Fingerprints Extracted from Channel Response

System	Bandwidth	Domain	Feature	Fingerprint Modeling
WBNN-Locate [Nerguizian et al. 2006]	200MHz	Time	Amplitude Phase	7 Statistical Quantities
[Jin et al. 2010]	60MHz	Time	Amplitude	Vector of CIR Amplitudes
[Patwari and Kasera 2007]	40MHz	Time	Amplitude	Vector of CIR Amplitudes
[Zhang et al. 2008]	40MHz	Time	Amplitude Phase	Phase-calibrated Vector of CIR
FIFS [Xiao et al. 2012a]	20MHz	Frequency	Amplitude	Summation over Independent Subcarrier Power
PinLoc [Sen et al. 2012b]	20MHz	Frequency	Amplitude Phase	Gaussian Mixture Model for CFR Clusters

candidate for precise fingerprinting since it conveys rich information of the small-scale multipath characteristics. Both CIR [Nerguizian et al. 2006; Jin et al. 2010] and CFR [Sen et al. 2012b; Xiao et al. 2012a] have been used in fingerprinting, as well as various extensions such as Power Delay Profile (PDP) [Triki and Slock 2007] and Power Delay Doppler Profile (PDDP) [Oktem and Slock 2010]. While the dimensional extension of channel response with respect to RSSI naturally brings richer information, it involves several challenges in extracting location-dependent signatures. One major concern is whether the finer-grained channel response is indeed more location dependent than RSSI in the presence of temporal dynamics. In terms of implementation, it also involves careful consideration in extracting compressed signatures to avoid the curse of dimensionality while retaining the spatial discrimination. A brief comparison of channel response-based fingerprints are listed in Table III.

4.2.1. Location Distinction with Channel Response. One primary challenge in traditional RSSI-based fingerprinting lies in the temporal fluctuations of RSSI. More specifically, given a certain extent of variation of measured RSSI, it is often difficult to figure out whether the variation stems from location change or temporal dynamics. In contrast, with the ability to characterize multipath components, channel response might be able to distinguish temporal variations from spatial ones, and hence is more resilient to environmental dynamics.

This intuition comes from the observation that the propagating paths to different locations tend to be less similar with those to the same location, even accounting for the temporal changes of paths. Therefore, from the statistical perspective, the self-correlation of channel responses measured from a specific location at different times is stronger than the cross-correlation of those measured at different locations.

Patwari et al. experimentally measured location distinction based on temporal link signature [Patwari and Kasera 2007], which can be regarded as a normalized version of CIR amplitudes. Location distinction refers to identifying whether the location of the transmitter i has changed based on the measurements at the receiver j. Given $M-1$ measurements of temporal link signatures, $H_{i,j} = \{h^m_{i,j}\}^{M-1}_{m=1}$, where $h^m_{i,j}$ denotes the m^{th} measurement of the temporal link signature between transmitter i and receiver j. The temporal variation of $H_{i,j}$ is calculated as the historical average difference $\sigma_{i,j}$ between each pair of the $M-1$ measurements:

$$\sigma_{i,j} = \frac{1}{(M-1)(M-2)} \sum_{g \in H_{i,j}} \sum_{h \in H_{i,j} \setminus g} \|h - g\|, \tag{15}$$

where $\|h-g\|$ is the Euclidean distance between h and g.

The M^{th} measurement $h_{i,j}^{M}$ is then compared with the history measurements $H_{i,j}$:

$$d_{i,j} = \frac{1}{\sigma_{i,j}} \min_{h \in H_{i,j}} \left\| h - h_{i,j}^{M} \right\|, \tag{16}$$

where $d_{i,j}$ is the distance between the new measurement and the history. If $d_{i,j}$ is greater than a predefined threshold γ, then the variation is decided as a location change rather than normal temporal dynamics. Otherwise, the new measurement is included in the history for update.

Zhang et al. [2008] reported similar results considering both the amplitude and phase of CIR . The l_2 distance metric between two signatures g and h is defined as a new ϕ_2 distance metric:

$$\|g - h\|_{\phi_2}^2 = \min_{\phi \in (0, 2\pi)} \|g e^{j\phi} - h\|_{l_2}^2. \tag{17}$$

ϕ_2 distance is used to minimize the random phase shift between two measurements due to lack of time and frequency synchronization.

Although channel response-based signatures outperform RSSI-based ones in spatial discrimination and resilience to temporal variations, the large-scale temporal behavior (e.g., days or weeks) still varies due to significant changes in multipath characteristics at the same location. In Zhang et al. [2008], experiments have shown that the large-scale temporal dynamics of channel response-based signatures tend to be in distinct states. Therefore, the large-scale temporal dynamics are modeled as a Markov chain in practice.

4.2.2. CIR-Based Fingerprinting. Since CIR directly portrays the small-scale multipath wireless channel in the time domain, it is reasonable to take CIR as fingerprint for fine-grained localization, as the multipath characteristics vary on the order of wavelength.

Nerguizian et al. [2006] implemented a CIR-based fingerprinting localization system for underground mines with dedicated infrastructure, for example, channel sounders and Vector Network Analyzers (VNAs). In the WBNN-Locate system, CFR is first obtained by a frequency sweep with central frequency of 2.4GHz and a span of 200MHz. The sweep space is 1MHz and results in 201 CFR samples, which are then converted into CIR by inverse Fourier transform. Afterward, up to seven parameters are extracted from the 201 CIR samples, including the mean excess delay, the rms delay spread, the maximum excess delay, the total received power, the number of multipath components, the power of the first path, and the arrival time of the first path. These parameters are chosen to compress the raw CIR data while retaining the time-spread characteristics. The parameters are then input to an Artificial Neural Network (ANN) for classification.

Despite the clear physical concept of the extracted parameters, it potentially risks subjective emphasis on certain parameters to combine heterogeneous inputs such as maximum excess delay and number of multipath components into a single ANN. A more natural way to limit the input size is to compress CIR directly. The WBNN-Locate system is refined in Nerguizian and Nerguizian [2007] by conducting Discrete Wavelet Transform (DWT) on the original CIR samples. The transformed wavelet coefficients are then truncated by a predefined threshold.

In the context of ubiquitous computing, though, the high bandwidth (200MHz) and the dedicated channel sounder are far from pervasive deployment.

4.2.3. CFR-Based Fingerprinting. Instead of transforming CFR into CIR, Sen et al. [2012b] implemented a meter-level spot localization system called PinLoc with off-the-shelf Intel 5300 NIC. Although CIR and CFR convey equivalent information

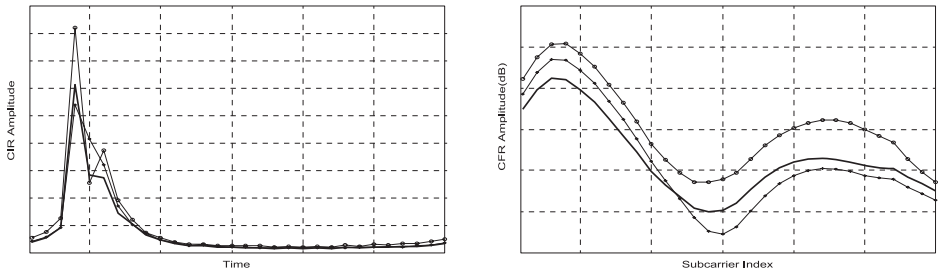

Fig. 5. Variations of CIR and CFR at three locations.

about the wireless channel, CFR tends to be more preferable given the limited bandwidth:

—Most variations of CIR distribute within only a few time indices, while the frequency diversity spans the entire range of CFR indices, making the structures among CFR more distinguishable with each other. Figure 5 illustrates the variations of CIR/CFR amplitudes at three locations.
—The lack of synchronization and insufficient number of samples make it rather error prone to estimate the first path according to the time indices based on a certain signal power threshold. On the contrary, there is no alignment issue for CFR since each component of CFR corresponds to a fixed subcarrier.

The key observation in PinLoc is that the probability density function (pdf) of CFRs on a single subcarrier at the same location demonstrates clustered distributions on the complex plane. Thus, the channel response on subcarrier f is modeled as a Gaussian mixture distribution with U_f^i and V_f^i as its mean and variance, respectively. Note that in OFDM systems, each subcarrier fades independently. It is then reasonable to use a multidimensional Gaussian random vector $(\mathbf{U}^i, \mathbf{V}^i)$ as one combination of clusters across all subcarriers, where $\mathbf{U}^i = (U_1^i, \ldots, U_F^i)$ and $\mathbf{V}^i = (V_1^i, \ldots, V_F^i)$, respectively, and $F = 30$. Hence, the channel response for a specific location is modeled as a Gaussian mixture distribution $(w_k, \mathbf{U}_k, \mathbf{V}_k)$, where w_k is the weight of $(\mathbf{U}^k, \mathbf{V}^k)$. To reduce the number of cluster combinations while retaining location-dependent features, only K representative combinations of clusters with larger weights are preserved. For each packet $\mathbf{P}$ with $\{P_f\}_{f=1}^F$ as the corresponding CFRs, the log probability of $\mathbf{P}$ belonging to the representative combination of clusters $(\mathbf{U}^i, \mathbf{V}^i)$ is calculated as:

$$d(\mathbf{P}, \mathbf{U}^i) = \sum_{f=1}^{F} \log V_f^i + \sum_{f=1}^{F} \frac{\left\| P_f - U_f^i \right\|^2}{\left(V_f^i\right)^2}, \tag{18}$$

which is the log likelihood metric for signature classification.

Another trick in PinLoc is that the localization process is conducted on a set of $1m \times 1m$ grids, known as *spots*, where CFRs measured at about four randomly picked locations within the spot are taken as signatures for each spot. The rationale is that the correlations among signatures across different spots are low, thus indicating high spatial distinctions. On the other hand, since CFR experiences dramatic change even at the granularity of wavelength, it is highly possible that CFRs measured even about 1 meter away can have low correlations with all prelabeled signatures. It improves localization robustness and avoids high probability of not locating in any locations by taking CFRs measured at different locations within the spot as the candidate set of signatures for that spot.

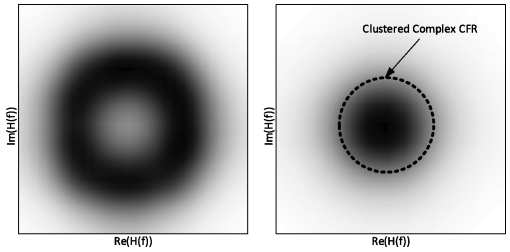

Fig. 6. Complex CFR on two subcarriers: unclustered CFRs due to uniformly distributed phases.

4.3. Designing Issues in Channel Response as Power Features

4.3.1. Bandwidth Limitations. The bandwidth is a major constraint in devising fine-grained localization systems based on channel response, for it primarily bounds the time resolution and hence the distinguishable multipath components of the system. More formally, given the system bandwidth B and the maximum excess delay τ_{max}, the number of CIR samples relevant to multipath N is approximated as:

$$N = \lfloor B \times \tau_{max} \rfloor. \tag{19}$$

For instance, given a bandwidth of 60MHz, which yields a time resolution of 16.67ns, at most 30 CIR samples would correspond to the multipath components since typical maximum excess delay indoors is less than 500ns [Jin et al. 2010].

The insufficient bandwidth makes each received multipath component look like a rounded peaked triangular shape rather than a narrow impulse. And the paths are not resolvable if they arrive within the system time resolution. Hence, in Wu et al. [2012], only clusters of multipath components are distinguishable with a bandwidth of 20MHz given 30 samples of CIR.

Bandwidth also affects the accuracy of fingerprinting. According to the simulations in Jin et al. [2010], given an extreme bandwidth (e.g., 100MHz), the performance gap among different classification methods is negligible. In terms of current WiFi with a bandwidth of only 20MHz (without channel bonding), the localization accuracy might hover around 3m if the features are not carefully designed. To achieve meter-level precision, more representative features should be extracted from channel responses.

4.3.2. Feature Selection. For fingerprinting schemes, it is nontrivial to select the most location-dependent features from channel response. Although it is possible to simply take the raw CIR or CFR samples as signatures, the high dimension complicates the computational complexity of the training and classification procedures. In addition, given insufficient bandwidth, a portion of the derived CIR or CFR samples might be irrelevant to multipath characteristics and has to be filtered out. As listed in Table III, given limited bandwidths, the robustness of CIR- and CFR-based features differs. CIR is less sensitive to single path changes since the paths are largely independent in the time domain. Conversely, the paths are twisted in the frequency domain, leading to variations over the entire CFRs. In addition, it also involves considerable challenges if phase information is included in the fingerprint in the presence of location-irrelevant phase shift [Zhang et al. 2008; Sen et al. 2012b]. As shown in Figure 6, different subcarriers or propagating conditions might result in relatively uniform or clustered phase distributions. Therefore, careful fingerprint modeling is required if phase information is employed.

Furthermore, the finer-grained channel response signatures increase the burden of the site survey since more locations might become distinguishable. The quality of each signature may also need to be considered to assist in selecting more representative and

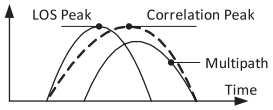

Fig. 7. Correlation error.

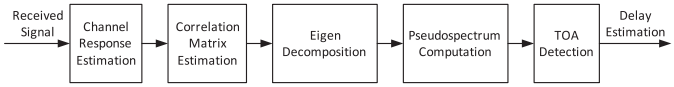

Fig. 8. Work-flow of MUSIC super-resolution algorithm.

distinct features as previous works for RSSI-based signatures [Chen et al. 2006; Fang and Lin 2012].

5. BEYOND POWER: INTERPLAY WITH TIME AND ANGLE

As discussed in Section 2.1, time and angle information are typically used for ranging. Compared with power-based ranging, time- and angle-based geometric mapping do not rely on channel models. Unlike RSSI, channel response is widely adopted in time or angle estimation with dedicated signal sources or infrastructure.

5.1. Time Estimation Based on CIR

Two mainstream time-based schemes are UWB and acoustic ranging. UWB signals are short baseband pulses spanning a wide range of bandwidth simultaneously, thus yielding high time resolution. We refer readers to Gezici et al. [2005] for a comprehensive survey on UWB-based ranging. Acoustic signals are also prevalent in accurate ranging due to their relatively low propagating speed [Zhang et al. 2012b; Sun et al. 2011].

Time-based ranging often involves sophisticated signal processing techniques, where the detection of signal arrival lies in the core. Conventional time estimation techniques roughly fall into two categories. One method converts CFR into CIR by inverse Fourier transform and selects the index of the first peak value as the estimated time delay of the LOS path [Gezici et al. 2005]. The other is based on cross-correlation techniques like matched filtering [Gezici et al. 2005; Golden and Bateman 2007; Geiger 2010]. But standard correlation-based methods may fail to resolve multipath components that are too close to each other. For instance, Pseudo-Noise (PN) correlation estimation is often incapable of distinguishing signals arriving within the chip interval of the PN sequence in spread spectrum systems [Dumont et al. 1994; Saarnisaari 1997]. That is, the time corresponding to the power peak of the LOS path might not coincide with that of the resultant correlation, as shown in Figure 7. Thus, more sophisticated super-resolution techniques have been applied for accurate time delay estimation, such as the root MUltiple SIgnal Classification (Root-MUSIC) algorithm [Dumont et al. 1994; Li and Pahlavan 2004], the Total Least Squares version of Estimation of Signal Parameters via Rotational Invariance Technique (TLS-ESPRIT) [Saarnisaari 1997], and so forth.

Li and Pahlavan [2004] employed frequency domain super-resolution and various diversity techniques for TOA estimation and compared ranging performance with traditional estimation strategies via simulation. In Li and Pahlavan [2004], CFR is first sampled with a network analyzer, which generates swept frequency signals centered at 1GHz. CFR samples are then transformed into a temporal pseudo-spectrum using Root-MUSIC algorithm. And the TOA of the LOS path is estimated by detecting the index in the delay axis of the first peak of the pseudo-spectrum. The simplified work flow of the MUSIC algorithm is illustrated in Figure 8.

Concretely, rewrite the formula of CIR in Equation (4) as:

$$h(\tau) = \sum_{i=1}^{N} \alpha_i \delta(\tau - \tau_i), \tag{20}$$

where $\alpha_i = a_i e^{-j\theta_i}$. The corresponding CFR is then:

$$H(f) = \sum_{i=1}^{N} \alpha_i e^{-j2\pi f \tau_i}. \tag{21}$$

This formula resembles a harmonic signal model, if the time and frequency variables in Equation (21) are exchanged. Therefore, spectral estimation techniques suitable for harmonic signals (e.g., the MUSIC algorithm) can be used for time-domain analysis.

Given K frequencies equally spaced by Δf and assuming additive white noise, the measured CFR samples are denoted as:

$$x(k) = H(f_k) + w(k) = \sum_{i=1}^{N} \alpha_i e^{-j2\pi f_k \tau_i} + w(k), \tag{22}$$

where $f_k = f_1 + (k-1)\Delta f, k = 1, \ldots, K$, and $w(k)$ is the zero-mean additive while noise with standard variance σ_k. Equation (22) is then reassembled into vector form as:

$$\mathbf{x} = \mathbf{H} + \mathbf{w}, \tag{23}$$

where

$$\begin{aligned} \mathbf{x} &= [x(1) \quad x(2) \quad \ldots \quad x(K)]^T \\ \mathbf{H} &= [H(f_1) \quad H(f_2) \quad \ldots \quad H(f_K)]^T. \end{aligned}$$

The MUSIC algorithm is based on eigenvalue decomposition of the autocorrelation matrix of the measured signal vector $\mathbf{x}$:

$$\mathbf{R_{xx}} = E\{\mathbf{x}\mathbf{x}^H\}. \tag{24}$$

If $K > N$, then the K-dimensional subspace can be divided into two orthogonal subspaces, known as signal subspace and noise subspace by the eigenvectors of $\mathbf{R_{xx}}$. The eigenvectors corresponding to the largest N eigenvalues are called signal eigenvectors, while the remaining are called noise eigenvectors. The multipath delays $\{\tau_i\}_{i=1}^{N}$ are determined by maximizing the MUSIC pseudo-spectrum, where the optimal solution should have zero projection in the noise subspace.

As discussed in Li and Pahlavan [2004], it is nontrivial to obtain true correlation matrix $\mathbf{R_{xx}}$ based on quite a limited number of channel measurements. Hence, several enhancements and diversity techniques have been proposed to improve the estimation accuracy of the correlation matrix.

According to the simulation results, the performance of super-resolution techniques surpasses that by conventional TOA estimation methods with relatively narrow bandwidth (e.g., 20MHz). Therefore, it might significantly improve the accuracy of time-based ranging in WLAN systems with practical super-resolution techniques.

5.2. Designing Issues in Channel Response as Time Features

5.2.1. NLOS Propagation Condition. NLOS propagation induces a positive bias in time-based ranging. In practice, NLOS conditions can be identified based on the statistics of the arriving signals and have been explored in UWB systems [Gezici et al. 2005]. For instance, the variance under NLOS conditions tends to be larger than that in the LOS

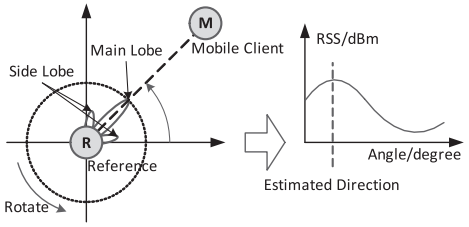

Fig. 9. Direction estimation with directional antenna.

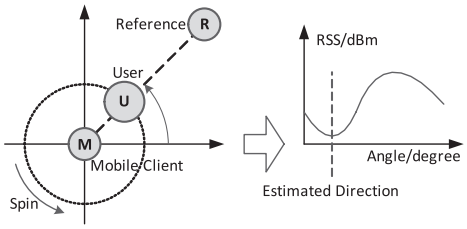

Fig. 10. Direction estimation with body blocking effect.

path. NLOS identification and mitigation have also been explored in cellular networks [Cong and Zhuang 2005] based on the prior NLOS error distribution from multiple base stations. Bahillo et al. [2010] experimentally verified the viability of prior NLOS measurements correction (PNMC) techniques indoors with WiFi-based customized hardware. PNMC techniques are designed to estimate the portion of NLOS conditions in the received signals [Mazuelas et al. 2009]. A more comprehensive survey on NLOS identification in TOA-based localization is provided in Guvenc and Chong [2009]. For WLAN TOA localization, though, further investigation is still needed into whether NLOS identification and mitigation techniques are readily applicable on commercial platforms.

5.2.2. Towards Protocol-Based Ranging. Time-based ranging usually involves external signal sources and heavily relies on sophisticated signal processing. Recent works have explored practical WLAN ranging based on MAC layer carrier sense combined with an RSSI indicator [Giustiniano and Mangold 2011]. The distance is measured by estimating the MAC idle time during a data/ACK round. Despite the dispersed WiFi signal employed, the system achieves medium accuracy and requires only a limited calibration in multipath situations. The key observation is to correlate SNR with the valid ACK, since the detection time of ACK varies with different levels of SNR. We envision that the channel responses embedded in standard CSI of current IEEE 802.11 protocol would also open new opportunities to mitigate protocol- or hardware-related time delays in time-based ranging.

5.3. Distinguishing AOA

Angle information is usually obtained with directional antennas [Niculescu and Nath 2004; Pongthawornkamol et al. 2010; Cidronali et al. 2010] or antenna arrays [Wong et al. 2008; Xiong and Jamieson 2012, 2013]. In most directional antenna-based schemes, a rotating directional antenna is used to infer AOA as the direction toward the strongest peak in received signal strength, as shown in Figure 9. Nevertheless, the best angle estimation does not necessarily coincide with the direction of the strongest signal power in multipath-rich indoor scenarios. In Niculescu and Nath [2004], the strongest two peaks as well as the entire signal power distribution over all directions are exploited to develop several heuristics for accurate triangulation.

In the context of pervasive computing, though, directional antennas are still far from handy access. A tricky alternative was proposed in Zhang et al. [2011], by using the so-called blocking obstacle effect to derive AOA on off-the-shelf mobile phones with little human intervention. The key insight is that the body of a user holding a smartphone will block part of the incoming signal. Therefore, the received signal would experience considerable drop when the user stands close to the phone-AP straight line. Thus, as the user rotates in place, the received signal power would demonstrate a peak (dip) when the user faces (backs to) the AP, which resembles an upside-down version of the

signal power received by a revolving directional antenna. Figure 10 shows this blocking effect.

As with the case for traditional directional antennas, the proposed system, Borealis, also has to deal with angle information estimated from noisy raw signal strengths. Borealis first simplifies the range of angles where signal power drops sharply as a blocking sector β:

$$\beta = 180^\circ - 2\left(\arctan\frac{2p}{b} - \arcsin\frac{bp}{d\sqrt{4p^2+b^2}}\right), \tag{25}$$

where p and d are the user-phone distance and user-AP distance, respectively. Under general configurations, $\beta \approx 90^\circ$.

Then, a sliding window-based search is adopted to estimate the optimal direction. More concretely, the RSSI measurements are grouped by a window of size β, and the group with the largest relative signal degradation is selected. Afterward, the direction opposite to its center is estimated as the AP direction.

Formally, for a window S_j of size β, the relative signal degradation is calculated by subtracting the average signal strength of the window from the average signal strength outside the window:

$$\mathit{Diff}(j) = \frac{\sum_{\theta \notin S_j} \mathit{RSSI}(\theta_i)}{N - |S_j|} - \frac{\sum_{\theta \in S_j} \mathit{RSSI}(\theta_i)}{|S_j|}, \tag{26}$$

where $|S_j|$ is the number of measurement within S_j, and $\mathit{RSSI}(\theta_i)$ is the measured RSSI in dBm at azimuth of θ_i.

The selected window S^* is then:

$$S^* = \arg\max_{S_j} \mathit{Diff}(j). \tag{27}$$

The AP direction is estimated as the opposite direction of the central orientation of S^*.

Borealis is designed for outdoor AP localization, while in indoor scenarios, the rich multipath effects derail the RSSI-based schemes. Sen et al. proposed SpinLoc [Sen et al. 2012a], which uses the signal power of the LOS path for AP direction estimation. SpinLoc exploited the sampled CFRs reported by Intel 5300 NIC and converted the CFRs into CIRs by inverse Fourier transform. The power of the first index in CIR is taken as the signal strength for the LOS path, known as Energy of the Direct Path (EDP). A set of EDPs are calculated when the user spins in place. Then the EDPs are smoothed by a moving average filter. Finally, the opposite direction corresponding to the lowest EDP is estimated as the AP direction. The angle information is then converted into location by a simple triangulation method. SpinLoc yields a median localization accuracy of 7m.

Antenna array-based AOA estimation is another thread of classical approaches. Compared with traditional rotating directional antennas, antenna arrays are more preferable due to the increasing popularity of Multiple-Input Multiple-Output (MIMO) techniques in standard WLAN protocols (e.g., IEEE 802.11n).

For instance, Wong et al. [2008] investigated the feasibility of AOA-based indoor localization with sets of CIRs measured at a 4×4 MIMO system. The CIR for the m^{th} channel $h_m(t)$ where $m = 1, \ldots, 16$, is estimated by the correlation of a real baseband PN sequence $u(t)$ and the corresponding received baseband sequence $r_m(t)$:

$$h_m(t) = \int u(\tau) r_m(\tau + t) d\tau. \tag{28}$$

Afterward, the AOA estimator can be applied to the measured CIRs. In Wong et al. [2008], a simple Maximum Likelihood (ML) estimator is employed, which selects the earliest detectable component in CIR and estimates its AOA:

$$\hat{\phi} = \arg\min_{\phi} \sum_{m=1}^{M} \left\| \frac{h_m(\tau_{min})}{h_1(\tau_{min})} - e^{j\pi(m-1)cos\phi} \right\|^2, \tag{29}$$

where $\hat{\phi}$ is the estimated AOA, and τ_{min} denotes the time delay of the earliest path among all CIRs of the M linearly spaced antennas.

More advanced AOA estimation algorithms like the Space Alternating Expectation Maximization (SAGE) [Fessler and Hero 1994] are also explored in Wong et al. [2008]. Experiments have demonstrated a medium localization accuracy of 2m with four antenna elements. Recently, ArrayTrack [Xiong and Jamieson 2012, 2013] applied the MUSIC algorithm for AOA estimation and spatial smoothing for NLOS mitigation with four antenna elements at AP and two at each client. ArrayTrack achieves a 25-cm location accuracy in stationary environments. Despite the impressive accuracy, the limited number of antennas in current WLAN still poses considerable challenges in practical angle-based localization in MIMO systems. However, we envision future commercial WLAN devices would possess folded-more antenna elements to meet the increasing demands for advanced MIMO techniques.

5.4. Designing Issues in Channel Response as Angle Features

Compared with power and time features, the derivation of angle information involves relatively dedicated infrastructure. On the other hand, since direction is orthogonal to distance in localization, angle information is often combined with other schemes to improve localization accuracy, such as RSSI-based ranging [Cidronali et al. 2010] and TOA-based ranging [Seow and Tan 2008; Zhang and Wong 2009]. As in the case of time-based ranging, angle-based methods also have to deal with NLOS and multipath conditions. The direct path needs to be extracted from the received signals or CIR, as in Sen et al. [2012a].

Angle information also enables novel localization schemes via frequency changes from Doppler shifts [Chang et al. 2008]. The key component is Doppler angulation, which determines the relative angle between a stationary client and reference node by artificially creating relative movements with a rotating directional antenna on the reference node. We envision that the current time-invariant channel response would also be extended to the Doppler domain to depict such fast relative locomotion and open new possibilities for angle-based geometric mapping.

6. SMART AMBIENCE: ROBUST PASSIVE DETECTION AND LOCALIZATION

The triple convergence of pervasive, context-aware, and human-centric computing has raised increasing research interest in perceiving surrounding objects (e.g., humans) from ambient devices, which is termed *Device-free passive* (DfP) [Youssef et al. 2007]. Common device-free tasks include detecting, counting, locating, tracking, and identifying the users in the area of interest passively. In this survey, we focus on the primary tasks of detection and localization, that is, detecting the presence of or further locating a person by already deployed wireless monitors, while the person carries no detectable devices. This passive manner of detection and localization is accomplished by correlating the impact of human presence on the wireless signals to certain *changes* of the received signal features. We refer the readers to Patwari and Wilson [2010] for a comprehensive survey on Radio-Frequency (RF) device-free localization and mainly focus on the principles and how channel response features can be applied.

6.1. Signal Metrics

As with active localization, a large body of studies on passive detection and localization exploit the handy signature, RSSI, from either WiFi-enabled infrastructure [Youssef et al. 2007; Kosba et al. 2012] or ZigBee sensors [Zhang et al. 2007; Wilson and Patwari 2010]. The signal metrics used in these schemes roughly fall into two categories: (i) shadowing (mean)-based metric [Wilson and Patwari 2010; Chen et al. 2011] and (ii) variance-based metric [Zhang et al. 2007; Wilson and Patwari 2011; Kosba et al. 2012]. The former manages to detect both immobile and moving users but performs well only under LOS conditions. The latter is more robust in NLOS environments but cannot detect stationary users, since they usually induce no significant RSSI variance.

To be able to detect both stationary and mobile users and under both LOS and NLOS conditions, recent works mostly rely on fingerprinting approaches with sophisticated probabilistic techniques [Chen et al. 2011; Xu et al. 2012] and employ finer-grained signal metrics, for example, RSSI histograms [Moussa and Youssef 2009; Zhao et al. 2013].

Very recent works also explored employing CSI-based features in passive detection [Xiao et al. 2012b; Zhou et al. 2013] and reported a marginal detection rate improvement due to better temporal stability of features extracted from CSI [Xiao et al. 2012b].

6.2. Modeling-Based Passive Detection and Localization

Modeling-based passive detection and localization schemes strive to extend the LDPL model to correlate the position of targeted object with respect to the static Transmitter-Receiver (TX-RX) link to certain signal metrics and compensate for the multipath effect in a probabilistic manner [Zhang and Ni 2009; Wilson and Patwari 2010, 2012; Patwari and Wilson 2011]. Nevertheless, these models are based on the assumption that the multipath components are unresolvable, since numbers of passive solutions are designed with low-cost ZigBee sensors. With the widespread use of WLAN, it is envisioned that higher- resolution CIR would enable future models under resolvable multipath components, and taking a deterministic approach.

6.2.1. RSSI-Based Probabilistic Model. Zhang et al. [2007] proposed an RF-based transceiver-free localization and tracking system by ZigBee sensors deployed on the ceiling as a mesh network. The affected signal power by human movements is simplified by a two-way propagating model. As illustrated in Figure 11, the LOS path and the ground-reflected path dominate all other multipath components in static environments. Assuming $n = 2$, the received power from the LOS path P_1 is calculated by Equation (9). Similarly, the received power from the ground-reflected path is:

$$P_2 = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 (d^2 + h^2)}. \tag{30}$$

When a user steps into the monitored area, the affected signal power is calculated according to the radar equation [Pozar 1997]:

$$P_{obj} = \frac{P_t G_t G_r \lambda^2 \sigma}{(4\pi)^3 r_1^2 r_2^2}, \tag{31}$$

where r_1, r_2 denote the TX-human, RX-human distances, respectively. σ is the radar cross section of the person. Under common settings, the signal strength difference between static environment and human presence is approximated as:

$$\Delta P \approx P_{obj.} \tag{32}$$

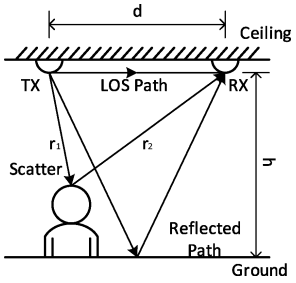

Fig. 11. Two-way model.

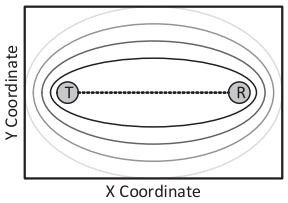

Fig. 12. Scattering dominant.

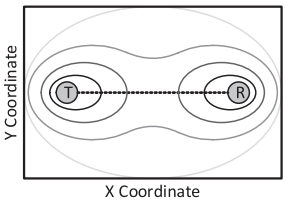

Fig. 13. Reflection dominant.

It then follows that the received signal would undergo larger variance when the person presents closer to the midpoint of each Parallel Lines (PL) and Vertical Lines (VL) with respect to the TX-RX link.

In Zhang and Ni [2009], the model is further approximated as the border of an ellipse given a fixed signal power variance and is experimentally verified in Zhang et al. [2010]. Patwari and Wilson [2011] theoretically proved that the model holds in a scatter-dominant environment. As illustrated in Figure 12, when scattering dominates the multipath propagation, the variance of RSSI increases when the person moves closer to the TX-RX link. In contrast, in a reflection-dominant environment, the variance of RSSI is larger when the person locates closer to the TX or RX, as illustrated in Figure 13.

Although the model in Zhang et al. [2007] is built upon a separable multipath at first sight, it surrenders to a threshold and probabilistic model [Zhang and Ni 2009; Zhang et al. 2010] as the ultimate signal metric is RSSI.

To compensate for the noise of irrelevant RSSI dynamics, most systems leverage dense-deployed networks and infer human presence in an ad hoc manner. For instance, in Radio Tomographic Imaging (RTI) [Wilson and Patwari 2010, 2011], the objective is to determine a spatial vector $\mathbf{x} \in \mathbb{R}^N$ indicating the location of power attenuation, from a set of measurements $\mathbf{y} \in \mathbb{R}^M$, where N and M denote the amount of grids in the network and the total number of links between sensor pairs. One link and the corresponding grids are illustrated in Figure 14. In Wilson and Patwari [2010], $\mathbf{y}$ represents the additional attenuation induced by human presence, while in Wilson and Patwari [2011], the variations of RSSI are used.

More specifically, the RTI problem is formulated as:

$$\mathbf{y} = \mathbf{W}\mathbf{x} + \mathbf{n}, \tag{33}$$

where $\mathbf{y}$ represents all RSSI differences with respect to the static measurements. $\mathbf{W} \in \mathbb{R}^{M \times N}$ is the weight matrix where w_{ij} is the corresponding weight of the j^{th} grid for the i^{th} link. $\mathbf{n}$ is the noise vector and $\mathbf{x}$ is the image to be estimated. The weight matrix is determined by an elliptical model with foci at each sensor pair.

6.2.2. CIR-Based Deterministic Model. Modeling-based device-free localization leveraging CIR is mostly seen in the area of UWB radar [Chang and Sahai 2004]. Given the CIR measured by UWB transceivers, the excess time delays (i.e., the time delays of $\{\tau_i\}_{i=1}^N$ in Equation (20)) compared with the LOS path delay τ_1 reveal the additional propagating distance compared with the LOS path. As shown in Figure 15, assume that the only change induced by object presence is a new multipath in the CIR, and consider the same reflecting path as discussed in Section 6.2.1. Then the object would be located on an ellipse with TX and RX as foci, and with the major axis decided by the propagating

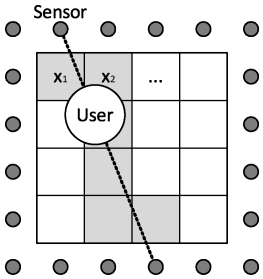

Fig. 14. A single affected link of RTI.

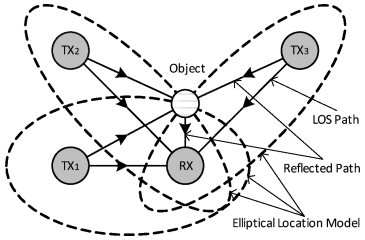

Fig. 15. CIR-based deterministic model and localization.

distance of the reflecting path. With multiple such ellipses, the intersection estimates the object's location.

As with Section 6.2.1, this simplified model can also be extended by considering a cluster of paths with the single-bounce path being the shortest [Reggiani et al. 2009]. The major distinction is that the models here are deterministic and do not rely on a dense-deployed network to perform computational-intensive statistical inferences. The tradeoff, though, is to measure CIRs and separate multipath components.

Note that with current WLAN-based CIR (e.g., those derived from Intel 5300 NIC), it is only possible to resolve clusters of multipath components [Wu et al. 2012], making it infeasible to directly apply the aforementioned deterministic models. However, it is at least possible to harness the CFRs as multiple independent RSSIs measured at different frequencies to improve the robustness of the probabilistic models. Future wideband WLAN standards (e.g., 802.11ac with 180MHz) might enable finer-grained multipath resolution and, consequently, put deterministic models into pervasive practice.

6.3. Fingerprinting-Based Passive Detection and Localization

In general, fingerprinting-based schemes are more flexible than model-based schemes, yet at the cost of cumbersome site survey. Youssef et al. grounded the concept of Device-free Passive (DfP) for WiFi networks and proposed both RSSI mean and variance-based solutions [Youssef et al. 2007]. Also, enhancements were proposed to prune irrelevant variations by outlier detection techniques [Kosba et al. 2012], discriminant analysis [Xu et al. 2012], and so forth, to remove static environment (i.e., empty room) calibration [Zhao et al. 2013] and to perform more robustly under clustered multipath conditions [Xu et al. 2012; Zhao et al. 2013]. Similar to Section 4.2, CIR and CFR naturally offer new possibilities in selecting finer-grained signal features. Recent works have explored the primary device-free task of detection with off-the-shelf CSI [Xiao et al. 2012b; Zhou et al. 2013].

Xiao et al. [2012b] implemented an indoor device-free motion detection system named FIMD to achieve a higher detection rate and robustness to narrow-band interference. Compared with the state-of-the-art WiFi device RASID [Kosba et al. 2012], FIMD gets a marginally higher detection rate due to the more temporally stable features extracted from CSI.

As noted in Xiao et al. [2012b], RSSI demonstrates high variability as susceptible to the measurement itself. And, consequently, a slow dynamic due to object locomotion might be hidden by the inherent RSSI variance, which leads to miss detection. As with CFR-based fingerprinting in Section 4.2.3, FIMD also leverages the frequency diversity of CFR, yet with the objective to extract variance-based features.

Recall from Equation (8) that $H(f_k)$ denotes the CSI at the subcarrier with central frequency of f_k, and a group of CSIs $H(f_k), (k = 1, \ldots, K)$ are available on off-the-shelf WiFi NICs. The input of FIMD is CSIs measured starting from time i and over a sliding window W with length $n+1$. More specifically, denote $\mathbf{H}_i$ as the group of CSIs measured at time i:

$$\mathbf{H}_i = [H_i(f_1) \quad H_i(f_2) \quad \ldots \quad H_i(f_K)]^T. \tag{34}$$

And let $\mathbb{H}$ be the CSIs within the sliding window W:

$$\mathbb{H} = [\mathbf{H_i} \quad \mathbf{H_{i+1}} \quad \ldots \quad \mathbf{H_{i+n}}]. \tag{35}$$

Then the correlations between each column of $\mathbb{H}$ are calculated by the correlation matric $\mathbf{C}$ over $n+1$ sequential packets:

$$\mathbf{C} = \begin{bmatrix} C(i,i) & \ldots & C(i,i+n) \\ \vdots & \ddots & \vdots \\ C(i+n,i) & \ldots & C(i+n,i+n) \end{bmatrix}, \tag{36}$$

where $C(i, j)$ is the correlation ratio between $\mathbf{H_i}$ and $\mathbf{H_j}$.

The proposed feature $\mathbf{V}$ is the maximum eigenvalue of the correlation matrix $\mathbf{C}$:

$$\mathbf{V} = \max(eigen(\mathbf{C})/(n+1)). \tag{37}$$

The intuition is that in static environments, the correlation between each column of $\mathbb{H}$ (i.e., CSIs of sequential packets) would be high. In contrast, if the eigenvalues of the correlation matrix decrease significantly, the low correlation might indicate strong disturbance of channel states due to object motion. In Xiao et al. [2012b], experiments have shown that the maximum and second maximum eigenvalues are sufficient to capture the changes. Compared with the variance of RSSI, the proposed features enjoy two benefits: (i) RSSI is susceptible to transmitted power, while $\mathbf{V}$ is independent of power control, and (ii) such features are robust to narrow-band interferences at 2.4GHz.

Zhou et al. [2013] uses CSI in fingerprinting from another perspective. The performance of the basic monitoring unit in fingerprinting is not as well studied as in model-based schemes. As discussed in Section 6.2, most existing models of monitoring units for device-free systems are experimentally fitted and vary in coverage shapes. In essence, as illustrated in Figure 16, most coverage models demonstrate boundaries along the TX-RX link, rather than a disk centered at the RX. Therefore, the presence of user U_1 would be more easily detected compared with that of user U_2. The disk-like coverage, in contrast, provides an alternative to decomposing the whole monitoring network and is also desirable in some applications [Meguerdichian et al. 2001].

In Zhou et al. [2013], the concept of *Omnidirectional Passive Human Detection* (Omni-PHD) is introduced, which refers to the problem of passive human detection with a coverage of disk-like boundary, by employing link-centric unit architectures. And two levels of Omni-PHD are envisioned:

—Equalized Decision: Determine whether a person presents within a near-disk region or not, with equally guaranteed confidence along all directions.
—Azimuth Distinction: Discriminate the particular azimuth of the human presence within a near-disk region, with equally guaranteed confidence along all directions.

Although there are challenges entailed by the link-centric architecture, omnidirectional detection still seems promising for the following reasons:

—While the state of the art exploits the fickle and coarse-grained RSSI, channel response features from the PHY layer have opened new possibilities. On one hand,

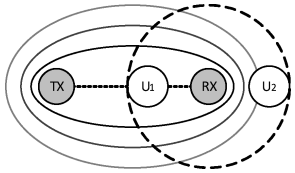

Fig. 16. Disk coverage with link structure.

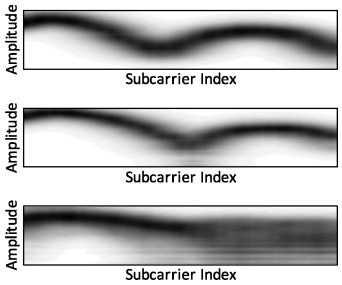

Fig. 17. Density distributions of CFR amplitudes.

channel response is more sensitive to human presence. On the other hand, the structure of channel response is more temporally stable than RSSI, thus possessing stronger resistance to background dynamics.

—By fingerprinting, it is possible to harness the anisotropic propagation circumstances to virtually tune the shape of the cell coverage.

In Zhou et al. [2013], a K-dimensional vector of the amplitude histograms of CFRs is employed, and the Earth Mover̄s Distance (EMD) [Rubner et al. 2000] is used as the metric for signature classification.

Figure 17 demonstrates the density distributions of the CFR amplitudes measured in a static environment with no one around (uppermost), with no one in the monitored area but with background human movement (middle), and with one person in the monitored area (lowermost). The upper two subfigures verify the stability of the CFR structures while the uppermost and the lowermost confirm that the CFR structures disperse in case of close obstruction. Hence, the amplitudes of CFR discriminate irrelevant background unstableness from the desired local perturbations due to human locomotion, which is almost impossible with the MAC layer RSSI-based descriptors [Kleisouris et al. 2010]. Detection rates of about 90% along four directions in typical office environments have been reported [Zhou et al. 2013].

As a preliminary exploration, though, the channel response distribution is modeled as a simple histogram, and only the amplitudes of CFRs are used. It is envisioned that future work would take a deeper scrutiny on feature extraction on passive detection with more flexible coverage shapes.

7. DISCUSSIONS AND RESEARCH DIRECTIONS

The motivation of wireless indoor localization is dual: using the same wireless devices to serve as both communication and localization tools. And the finer-grained channel response features have advanced both goals, where localization has been the primary focus of this survey. In this section, we briefly summarize the challenges of PHY layer-assisted indoor localization and also provide two other closely related and largely open research areas.

7.1. Dive Deeper: PHY Localization

As discussed in Section 3.5, channel response broadens the designing space of wireless indoor localization but also incurs limitations and challenges.

7.1.1. Multipath Resolvable, yet LOS Path Dependent. The fundamental advance of CSI from RSSI is its ability to resolve multipath via frequency diversity. For geometric mapping-based frameworks, though, CSI still fails to overcome the limitation of relying on the LOS path for accurate distance or direction estimation. One compensation is to

employ multiple TX-RX links to reduce the possibility of all LOS paths being blocked. Note that we leave out how multiple CSI-enabled devices cooperate to locate the target. We refer the readers to Liu and Yang [2011] for localization in a networked perspective. It might pose new challenges on handling the multiple orthogonal RSSIs introduced by frequency diversity from different and redundant APs for networked error control or outlier measurement removal.

7.1.2. Bandwidth, Coverage, and Energy. As discussed in Section 4.3, the system bandwidth constrains the resolution of multipath to clusters of components [Wu et al. 2012; Jin et al. 2010] and also makes it infeasible to apply deterministic models from the radar communities directly for passive detection [Chang and Sahai 2004; Reggiani et al. 2009]. While it is reasonable to expect upcoming wireless standards to have wider bandwidth (e.g., 802.11ac with up to 180MHz), which leads to higher time resolution, it also introduces more transmission power given a constant transmitting range. To conserve energy as well as prevent interferences with cobandwidth devices, it raises a tradeoff between bandwidth and coverage, which has to be considered as well if the systems are to be deployed in large scale. Furthermore, recent trends like Dynamic Spectrum Access (DSA) tend to use frequency in a fine-grained, noncontiguous, and demand-adaptive manner [Tan et al. 2010; Yang et al. 2010; Chai et al. 2012]. And it remains open whether CSI-based features would perform well under such settings.

7.1.3. Toward Truly Mobile and Real-Time. Currently, most existing works leveraging CSI are mostly proof-of-concept prototypes. In practice, the real-time performance would be one major concern. Although some reported better real-time performance since multiple CSIs are available simultaneously [Wu et al. 2012; Xiao et al. 2012b], others stated minute-long measurements for high-accuracy fingerprinting [Sen et al. 2012b]. Since current off-the-shelf CSIs are only available with Intel 5300 NIC and the modified driver [Halperin et al. 2010], it poses a challenge to employ CSIs on mobile handhelds. Even when CSIs become available on mobile devices, the upcoming device diversity, device orientation, and placement problems would be of great challenge to apply CSIs properly.

7.1.4. Combining Spatial Diversity. Compared with RSSI, CSI mainly extends into the frequency domain. The development of MIMO techniques would certainly bring the previously prohibitive AOA features into the context of pervasive computing, where channel response is combined with spatial diversity to tackle multipath. Recent works [Xiong and Jamieson 2013; Joshi et al. 2013] proposed novel solutions to remove multipath effects in AOA localization and with more off-the-shelf devices, opening new directions in wireless indoor localization.

7.2. Twin Applications: RSSI- and CIR-Based Wireless Security

Parallel with wireless localization, recent works on secured wireless communication have also explored harnessing the location-dependent and information-rich wireless channels for physical layer authentication [Xiao et al. 2008; Xiao et al. 2009; Jiang et al. 2013] and encryption key generation [Mathur et al. 2008; Ye et al. 2010].

Similar to location distinction [Patwari and Kasera 2007; Zhang et al. 2008], PHY layer authentication utilizes the fact that the channel responses in clustered multipath environments are location specific and decorrelates with each other on the order of wavelength, making it difficult to predict or spoof the channel states of the targeted TX-RX pair. Thus, the intended receiver can track the channel response for each message and detect spoofing attacks by comparing the newly measured channel response with the history. Xiao et al. [2008, 2009] proposed a general channel response-based authentication and spoofing detection framework through theoretical hypothesis testing.

Very recently, Jiang et al. [2013] designed a spoofing detection prototype on commercial WiFi, with the impact of environmental dynamics also considered. They reported 8× detection accuracy over RSSI-based schemes.

Besides the randomness of the wireless channel, physical layer secret key generation also relies on the reciprocity of the wireless channel within the coherent time. Mathur et al. [2008] proposed a key extraction scheme from an unauthenticated wireless channel via the amplitudes of CIR. To enable off-the-shelf applications, they also tested the feasibility of key generation with coarse-grained RSSI, and as with RSSI-based localization, have triggered increasing research interests due to the ubiquity of RSSI [Jana et al. 2009; Liu et al. 2012b]. Nevertheless, with CSI measurable on off-the-shelf devices now, channel response-based schemes would also be put into pervasive applications, which enjoy higher bit generation rates. Moreover, spatial diversity can also be combined to enrich the randomness of wireless channels [Wallace and Sharma 2010].

Physical layer wireless security and localization share the same principle that the wireless channels, though seemingly random, are location dependent and information rich. The key distinction is that wireless localization, especially channel response-based fingerprinting, aims to combat the temporal fluctuations to ensure reproducible signatures, while some wireless security applications like key generation strive to avoid temporal correlations to ensure randomness. Therefore, it is scenario specific to extract proper features from the channel responses.

7.3. Close the Loop: Location-Aware Wireless Communication

Although it is common to consider wireless localization as an application based on wireless communication, recent works have demonstrated that upper layers might also benefit a PHY layer or, at least, conduct localization and other wireless tasks simultaneously. For instance, the coarse-grained sensor readings on mobile devices have been employed to improve wireless performance via rate adaption [Ravindranath et al. 2011], while a pioneer work proposed a novel algorithm to locate and identify the type of coexisted radio interferences at the same time, even if the LOS path is severely buried by multipath [Joshi et al. 2013]. Since channel response depicts the location-dependent wireless propagating conditions, it is promising to trigger more novel location-aware applications.

8. CONCLUSION

In this survey, we briefly reviewed the principles and applications of channel response-assisted indoor localization. Compared with conventional RSSI, CSI characterizes the small-scale multipath fading and thus acts as a finer-grained descriptor of the wireless channel. From the time domain, CIR resolves individual multipath components with different time delays. Extending to the frequency domain, CFR depicts frequency-selective fading within the band of interest. Moreover, consisting of both amplitude and phase, channel response conveys much richer information than a single-valued RSSI. Therefore, channel response opens new opportunities to both ranging-based and fingerprinting-based localization schemes. It also holds potential for more robust and flexible device-free passive applications. As for accessibility, channel response at the granularity of the subcarrier level is now available on commercial wireless network cards as well.

Tracing back to decades ago, channel response was only accessible with dedicated infrastructure and was mainly used for channel modeling. Although channel response-based indoor localization also dates back almost 10 years ago, the extra instruments impede ready deployment. Meanwhile, the increasing bandwidth of WLAN standards has triggered vast frequency-aware optimizations targeting better spectrum utility, higher throughput, more reliable transmission, and so forth. Nevertheless, it was only

less than five years ago that upper layer applications were able to obtain a sampled version of CFRs on off-the-shelf platforms. And this fundamentally raises renewed interest in channel response-assisted indoor localization, with special emphasis on finer-grained precision and pervasive deployment.

Despite pioneer works in both geometric and fingerprinting-based schemes, the realm of indoor localization via channel response still involves considerable challenges. The current available resolution from channel response features is constrained by the underlying bandwidth, which proves to be only sufficient to differentiate clusters of multipath components with the current IEEE 802.11n standard. It also remains unsettled how to extract representative features that are location dependent, temporal stable, and noise resilient. Nevertheless, we envision with the development of OFDM as well as MIMO techniques that channel response-assisted indoor localization would embrace more opportunities in the near future.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers and the associate editor for their valuable comments.

REFERENCES

AZIZYAN, M., CONSTANDACHE, I., AND ROY CHOUDHURY, R. 2009. SurroundSense: Mobile phone localization via ambience fingerprinting. In *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom'09)*.

BAHILLO, A., MAZUELAS, S., LORENZO, R. M., FERNÁNDEZ, P., PRIETO, J., DURÁN, R. J., AND ABRIL, E. J. 2010. Accurate and Integrated Localization System for Indoor Environments based on IEEE 802.11 Round-trip Time Measurements. *EURASIP J. Wireless Commun. Networking 2010,* 6, 6:1–6:13.

BAHL, P. AND PADMANABHAN, V. 2000. RADAR: an In-building RF-based user location and tracking system. In *Proceedings of IEEE International Conference on Computer Communications (INFOCOM'00)*.

BARGH, M. S. AND DE GROOTE, R. 2008. Indoor localization based on response rate of Bluetooth inquiries. In *Proceedings of ACM International Workshop on Mobile Entity Localization and Tracking in GPS-less Environments (MELT'08)*.

BHARTIA, A., CHEN, Y.-C., RALLAPALLI, S., AND QIU, L. 2011. Harnessing frequency diversity in Wi-Fi networks. In *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom'11)*.

CHAI, E., LEE, J., LEE, S.-J., ETKIN, R., AND SHIN, K. G. 2012. Building efficient spectrum-agile devices for dummies. In *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom'12)*.

CHANG, C. AND SAHAI, A. 2004. Object tracking in a 2D UWB sensor network. In *Proceedings of Asilomar Conference on Signals, Systems and Computers (Asilomar'04)*.

CHANG, H.-L., TIAN, J.-B., LAI, T.-T., CHU, H.-H., AND HUANG, P. 2008. Spinning beacons for precise indoor localization. In *Proceedings of ACM Conference on Embedded Networked Sensor Systems (SenSys'08)*.

CHEN, X., EDELSTEIN, A., LI, Y., COATES, M., RABBAT, M., AND MEN, A. 2011. Sequential Monte Carlo for simultaneous passive device-free tracking and sensor localization using received signal strength measurements. In *Proceedings of ACM International Conference on Information Processing in Sensor Networks (IPSN'11)*.

CHEN, Y., LYMBEROPOULOS, D., LIU, J., AND PRIYANTHA, B. 2012. FM-based indoor localization. In *Proceedings of ACM International Conference on Mobile Systems, Applications, and Services (MobiSys'12)*.

CHEN, Y., YANG, Q., YIN, J., AND CHAI, X. 2006. Power-efficient access-point selection for indoor location estimation. *IEEE Trans. Knowl. Data Eng. 18,* 7, 877–888.

CIDRONALI, A., MADDIO, S., GIORGETTI, G., AND MANES, G. 2010. Analysis and Performance of a Smart Antenna for 2.45-GHz Single-Anchor Indoor Positioning. *IEEE Transactions on Microwave Theory and Techniques 58,* 1, 21–31.

CONG, L. AND ZHUANG, W. 2005. Nonline-of-Sight Error Mitigation in Mobile Location. *IEEE Trans. Wireless Commun. 4,* 2, 560–573.

CONSTANDACHE, I., BAO, X., AZIZYAN, M., AND CHOUDHURY, R. R. 2010. Did you see Bob?: Human localization using mobile phones. In *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom'10)*.

DUMONT, L., FATTOUCHE, M., AND MORRISON, G. 1994. Super-resolution of multipath channels in a spread spectrum location system. *IEEE Electron. Lett. 30,* 19, 1583–1584.

ELNAHRAWY, E., LI, X., AND MARTIN, R. 2004. The limits of localization using signal strength: A comparative study. In *Proceedings of IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON'04)*.

FANG, S.-H. AND LIN, T.-N. 2010. A dynamic system approach for radio location fingerprinting in wireless local area networks. *IEEE Trans. Commun. 58,* 4, 1020–1025.

FANG, S.-H. AND LIN, T.-N. 2012. Principal component localization in indoor WLAN environments. *IEEE Trans. Mobile Comput. 11,* 1, 100–110.

FESSLER, J. AND HERO, A. 1994. Space-alternating generalized expectation-maximization algorithm. *IEEE Trans. Signal Process. 42,* 10, 2664–2677.

FONTANA, R. 2004. Recent system applications of short-pulse ultra-wideband (UWB) technology. *IEEE Trans. Microwave Theory Tech. 52,* 9, 2087–2104.

GEIGER, D. 2010. High resolution time difference of arrival using timestamps for localization in 802.11b/g wireless networks. In *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC'10)*.

GEZICI, S., TIAN, Z., GIANNAKIS, G., KOBAYASHI, H., MOLISCH, A., POOR, H., AND SAHINOGLU, Z. 2005. Localization via ultra-wideband radios: A look at positioning aspects for future sensor networks. *IEEE Signal Process. Mag.e 22,* 4, 70–84.

GIUSTINIANO, D. AND MANGOLD, S. 2011. CAESAR: Carrier sense-based ranging in off-the-shelf 802.11 wireless LAN. In *Proceedings of ACM Conference on Emerging Networking EXperiments and Technologies (CoNEXT'11)*.

GOLDEN, S. A. AND BATEMAN, S. S. 2007. Sensor measurements for Wi-Fi location with emphasis on time-of-arrival ranging. *IEEE Trans. Mobile Comput. 6,* 10, 1185–1198.

GOLDSMITH, A. 2005. *Wireless Communications*. Cambridge University Press, New York, NY, USA.

GUVENC, I. AND CHONG, C.-C. 2009. A Survey on TOA Based Wireless localization and NLOS mitigation techniques. *IEEE Commun. Surv. Tutorials 11,* 3, 107–124.

HALPERIN, D., HU, W., SHETH, A., AND WETHERALL, D. 2010. Predictable 802.11 packet delivery from wireless channel measurements. In *Proceedings of ACM SIGCOMM Conference (SIGCOMM'10)*.

HARTER, A., HOPPER, A., STEGGLES, P., WARD, A., AND WEBSTER, P. 1999. The anatomy of a context-aware application. In *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom'99)*.

JANA, S., PREMNATH, S. N., CLARK, M., KASERA, S. K., PATWARI, N., AND KRISHNAMURTHY, S. V. 2009. On the effectiveness of secret key extraction from wireless signal strength in real environments. In *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom'09)*.

JIANG, Z., ZHAO, J., LI, X.-Y., HAN, J., AND XI, W. 2013. Rejecting the Attack: Source Authentication for WiFi Management Frames using CSI Information. In *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*.

JIN, Y., SOH, W.-S., AND WONG, W.-C. 2010. Indoor localization with channel impulse response based fingerprint and nonparametric regression. *IEEE Trans. Wireless Commun. 9,* 3, 1120–1127.

JOSHI, K., HONG, S., AND KATTI, S. 2013. PinPoint: Localizing Interfering Radios. In *Proceedings of USENIX Symposium on Networked Systems Design and Implementation (NSDI)*.

KLEISOURIS, K., FIRNER, B., HOWARD, R., ZHANG, Y., AND MARTIN, R. P. 2010. Detecting Intra-room Mobility with Signal Strength Descriptors. In *Proceedings of ACM International Symposium on Mobile ad hoc Networking and Computing (MobiHoc)*.

KOSBA, A., SAEED, A., AND YOUSSEF, M. 2012. RASID: A Robust WLAN Device-free Passive Motion Detection System. In *Proceedings of IEEE International Conference on Pervasive Computing and Communications (PerCom'12)*.

LI, X. AND PAHLAVAN, K. 2004. Super-Resolution TOA Estimation with Diversity for Indoor Geolocation. *IEEE Trans. Wireless Commun. 3,* 1, 224–234.

LIM, H., KUNG, L.-C., HOU, J. C., AND LUO, H. 2006. Zero-Configuration, Robust Indoor Localization: Theory and Experimentation. In *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*.

LIU, H., GAN, Y., YANG, J., SIDHOM, S., WANG, Y., CHEN, Y., AND YE, F. 2012a. Push the Limit of WiFi based Localization for Smartphones. In *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom'06)*.

LIU, H., YANG, J., WANG, Y., AND CHEN, Y. 2012b. Collaborative Secret Key Extraction Leveraging Received Signal Strength in Mobile Wireless Networks. In *Proceedings of IEEE International Conference on Computer Communications (INFOCOM'12)*.

Liu, Y. and Yang, Z. 2011. *Location, Localization, and Localizability: Location-awareness Technology for Wireless Networks*. Springer New York.

Mathur, S., Trappe, W., Mandayam, N., Ye, C., and Reznik, A. 2008. Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel. In *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom)*.

Mazuelas, S., Lago, F., Blas, J., Bahillo, A., Fernandez, P., Lorenzo, R., and Abril, E. 2009. Prior NLOS measurement correction for positioning in cellular wireless networks. *IEEE Trans. Vehicular Technol. 58,* 5, 2585–2591.

Meguerdichian, S., Koushanfar, F., Potkonjak, M., and Srivastava, M. 2001. Coverage problems in wireless ad-hoc sensor networks. In *Proceedings of IEEE International Conference on Computer Communications (INFOCOM'01)*.

Moussa, M. and Youssef, M. 2009. Smart devices for smart environments: Device-free passive detection in real environments. In *Proceedings of IEEE International Conference on Pervasive Computing and Communications (PerCom'09)*.

Nandakumar, R., Chintalapudi, K. K., and Padmanabhan, V. N. 2012. Centaur: Locating Devices in an Office Environment. In *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom'12)*.

Nerguizian, C., Despins, C., and Affes, S. 2006. Geolocation in mines with an impulse response fingerprinting technique and neural networks. *IEEE Trans. Wireless Commun. 5,* 3, 603–611.

Nerguizian, C. and Nerguizian, V. 2007. Indoor fingerprinting geolocation using wavelet-based Features Extracted from the Channel impulse response in conjunction with an artificial neural network. In *Proceedings of IEEE International Symposium on Industrial Electronics (ISIE'07)*.

Ni, L. M., Liu, Y., Lau, Y. C., and Patil, A. P. 2004. LANDMARC: Indoor location sensing using active RFID. *Wireless Networks 10,* 6, 701–710.

Niculescu, D. and Nath, B. 2004. VOR base stations for indoor 802.11 positioning. In *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom'04)*.

Oktem, T. M. and Slock, D. T. M. 2010. Power delay Doppler profile fingerprinting for mobile localization in NLOS. In *Proceedings of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'10)*.

Otsason, V., Varshavsky, A., LaMarca, A., and de Lara, E. 2005. Accurate GSM indoor localization. In *Proceedings of ACM International Conference on Ubiquitous Computing (UbiComp'05)*.

Patwari, N. and Kasera, S. K. 2007. Robust location distinction using Temporal link signatures. In *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom'07)*.

Patwari, N. and Wilson, J. 2010. RF sensor networks for device-free localization: Measurements, models, and algorithms. *Proceedings of the IEEE 98,* 11, 1961–1973.

Patwari, N. and Wilson, J. 2011. Spatial models for human motion-induced signal strength variance on static links. *IEEE Trans. Inf. Forensics Security 6,* 3, 791–802.

Peng, C., Shen, G., Zhang, Y., Li, Y., and Tan, K. 2007. BeepBeep: A high accuracy acoustic ranging system using COTS mobile devices. In *Proceedings of ACM International Conference on Embedded Networked Sensor Systems (SenSys'07)*.

Pongthawornkamol, T., Ahmed, S., Nahrstedt, K., and Uchiyama, A. 2010. Zero-knowledge real-time indoor tracking via outdoor wireless directional antennas. In *Proceedings of IEEE International Conference on Pervasive Computing and Communications (PerCom'10)*.

Pozar, D. 1997. *Microwave Engineering* 2nd Ed. Wiley.

Priyantha, N. B., Chakraborty, A., and Balakrishnan, H. 2000. The cricket location-support system. In *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom'00)*.

Rai, A., Chintalapudi, K. K., Padmanabhan, V. N., and Sen, R. 2012. Zee: Zero-effort Crowdsourcing for indoor localization. In *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom)*.

Rappaport, T. 2002. *Wireless Communications: Principles and Practice (2nd)*. Prentice Hall PTR.

Ravindranath, L., Newport, C., Balakrishnan, H., and Madden, S. 2011. Improving Wireless Network Performance using Sensor Hints. In *Proceedings of the USENIX Conference on Networked Systems Design and Implementation (NSDI'11)*.

Reggiani, L., Rydstrom, M., Tiberi, G., Strom, E., and Monorchio, A. 2009. Ultra-wide band sensor networks for tracking point scatterers or relays. In *Proceedings of IEEE International Symposium on Wireless Communication Systems (ISWCS'09)*.

Rubner, Y., Tomasi, C., and Guibas, L. J. 2000. The earth mover's distance as a metric for image retrieval. *Int. J. Comput. Vision 40,* 2, 99–121.

SAARNISAARI, H. 1997. TLS-ESPRIT in a time delay estimation. In *Proceedings of IEEE Vehicular Technology Conference (VTC'97)*.

SEIDEL, S. AND RAPPAPORT, T. 1992. 914 MHz path loss prediction models for indoor wireless communications in multifloored buildings. *IEEE Trans. Antennas and Propagation 40,* 2, 207–217.

SEN, S., CHOUDHURY, R. R., AND NELAKUDITI, S. 2012a. SpinLoc: Spin once to know your location. In *Proceedings of ACM Workshop on Mobile Computing Systems and Applications (HotMobile'12)*.

SEN, S., RADUNOVIC, B., CHOUDHURY, R. R., AND MINKA, T. 2012b. You are facing the Mona Lisa: Spot localization using PHY layer information. In *Proceedings of ACM International Conference on Mobile Systems, Applications, and Services (MobiSys'12)*.

SEOW, C. K. AND TAN, S. Y. 2008. Localization of omnidirectional mobile device in multipath environments. *Progress in Electromagnetics Research PIER 85*, 323–348.

SUN, Z., PUROHIT, A., CHEN, K., PAN, S., PERING, T., AND ZHANG, P. 2011. PANDAA: Physical arrangement detection of networked devices through ambient-sound awareness. In *Proceedings of ACM International Conference on Ubiquitous Computing (UbiComp'11)*.

TAN, K., FANG, J., ZHANG, Y., CHEN, S., SHI, L., ZHANG, J., AND ZHANG, Y. 2010. Fine-grained channel access in wireless LAN. In *Proceedings of ACM SIGCOMM Conference (SIGCOMM'10)*.

TRIKI, M. AND SLOCK, D. T. M. 2007. Mobile localization for NLOS propagation. In *Proceedings of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07)*.

UR REHMAN, W., DE LARA, E., AND SAROIU, S. 2008. CILoS: A CDMA indoor localization system. In *Proceedings of ACM International Conference on Ubiquitous Computing (UbiComp'08)*.

WALLACE, J. AND SHARMA, R. 2010. Automatic secret keys from reciprocal MIMO wireless channels: Measurement and Analysis. *IEEE Trans. Inf. Forensics Security 5,* 3, 381–392.

WANG, H., SEN, S., ELGOHARY, A., FARID, M., YOUSSEF, M., AND CHOUDHURY, R. R. 2012. No need to war-drive: Unsupervised indoor localization. In *Proceedings of ACM International Conference on Mobile Systems, Applications, and Services (MobiSys'13)*.

WANT, R., HOPPER, A., FALCÃO, V., AND GIBBONS, J. 1992. The active badge location system. *ACM Trans. Inf. Syst. 10,* 1, 91–102.

WILSON, J. AND PATWARI, N. 2010. Radio tomographic imaging with wireless networks. *IEEE Trans. Mobile Comput. 9,* 5, 621–632.

WILSON, J. AND PATWARI, N. 2011. See-through walls: Motion tracking using variance-based radio tomography networks. *IEEE Trans. Mobile Comput. 10,* 5, 612–621.

WILSON, J. AND PATWARI, N. 2012. A fade-level skew-laplace signal strength model for device-free localization with wireless networks. *IEEE Trans. Mobile Comput. 11,* 6, 947–958.

WONG, C., KLUKAS, R., AND MESSIER, G. G. 2008. Using WLAN infrastructure for angle-of-arrival indoor user location. In *Proceedings of IEEE Vehicular Technology Conference (VTC'08)*.

WU, C., YANG, Z., LIU, Y., AND XI, W. 2013. WILL: Wireless indoor localization without site survey. *IEEE Trans. Parallel Distrib. Syst. 24,* 4, 839–848.

WU, K., XIAO, J., YI, Y., GAO, M., AND NI, L. 2012. FILA: Fine-grained indoor localization. In *Proceedings of IEEE International Conference on Computer Communications (INFOCOM'12)*.

XIAO, J., WU, K., YI, Y., AND NI, L. M. 2012a. FIFS: Fine-grained indoor fingerprinting system. In *Proceedings of IEEE International Conference on Computer Communications and Networks (ICCCN'12)*.

XIAO, J., WU, K., YI, Y., WANG, L., AND NI, L. 2012b. FIMD: Fine-grained device-free motion detection. In *Proceedings of IEEE 18th International Conference on Parallel and Distributed Systems (ICPADS'12)*.

XIAO, L., GREENSTEIN, L., MANDAYAM, N., AND TRAPPE, W. 2008. Using the physical layer for wireless authentication in time-variant channels. *IEEE Trans. Wireless Commun. 7,* 7, 2571–2579.

XIAO, L., GREENSTEIN, L. J., MANDAYAM, N. B., AND TRAPPE, W. 2009. Channel-based spoofing detection in frequency-selective Rayleigh channels. *IEEE Trans. Wireless Commun. 8,* 12, 5948–5956.

XIONG, J. AND JAMIESON, K. 2012. Towards Fine-grained Radio-based Indoor Location. In *Proceedings of ACM Workshop on Mobile Computing Systems and Applications (HotMobile'12)*.

XIONG, J. AND JAMIESON, K. 2013. ArrayTrack: A fine-grained indoor location system. In *Proceedings of USENIX Symposium on Networked Systems Design and Implementation (NSDI'13)*.

XU, C., FIRNER, B., ZHANG, Y., HOWARD, R., LI, J., AND LIN, X. 2012. Improving RF-based device-free passive localization in cluttered indoor environments through probabilistic classification methods. In *Proceedings of ACM International Conference on Information Processing in Sensor Networks (IPSN'12)*.

YANG, J., SIDHOM, S., CHANDRASEKARAN, G., VU, T., LIU, H., CECAN, N., CHEN, Y., GRUTESER, M., AND MARTIN, R. P. 2011. Detecting driver phone use leveraging car speakers. In *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom'11)*.

YANG, L., HOU, W., CAO, L., ZHAO, B. Y., AND ZHENG, H. 2010. Supporting demanding wireless applications with frequency-agile radios. In *Proceedings of USENIX Conference on Networked Systems Design and Implementation (NSDI'10)*.

YANG, Z., WU, C., AND LIU, Y. 2012. Locating in fingerprint space: Wireless indoor localization with little human intervention. In *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom'12)*.

YE, C., MATHUR, S., REZNIK, A., SHAH, Y., TRAPPE, W., AND MANDAYAM, N. B. 2010. Information-theoretically secret key generation for fading wireless channels. *IEEE Trans. Inf. Forensics Secur. 5,* 2, 240–254.

YOUSSEF, M. AND AGRAWALA, A. 2005. The Horus WLAN location determination system. In *Proceedings of ACM International Conference on Mobile Systems, Applications, and Services (MobiSys'05)*.

YOUSSEF, M., MAH, M., AND AGRAWALA, A. 2007. Challenge: Device-free passive localization for wireless environments. In *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom'07)*.

ZHANG, D., LIU, Y., GUO, X., GAO, M., AND NI, L. 2012a. On distinguishing the multiple radio paths in RSS-based ranging. In *Proceedings of IEEE International Conference on Computer Communications (INFOCOM'12)*.

ZHANG, D., LIU, Y., AND NI, L. M. 2010. Link-centric probabilistic coverage model for transceiver-free object detection in wireless networks. In *Proceedings of IEEE International Conference on Distributed Computing Systems (ICDCS'10)*.

ZHANG, D., MA, J., CHEN, Q., AND NI, L. M. 2007. An RF-based system for tracking transceiver-free objects. In *Proceedings of IEEE International Conference on Pervasive Computing and Communications (PerCom'07)*.

ZHANG, D. AND NI, L. 2009. Dynamic clustering for tracking multiple transceiver-free objects. In *Proceedings of IEEE International Conference on Pervasive Computing and Communications (PerCom'09)*.

ZHANG, J., FIROOZ, M. H., PATWARI, N., AND KASERA, S. K. 2008. Advancing wireless link signatures for location distinction. In *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom'08)*.

ZHANG, V. AND WONG, A.-S. 2009. Combined AOA and TOA NLOS localization with nonlinear programming in severe multipath environments. In *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC'09)*.

ZHANG, Z., CHU, D., CHEN, X., AND MOSCIBRODA, T. 2012b. SwordFight: Enabling a new class of phone-to-phone action games on commodity phones. In *Proceedings of ACM International Conference on Mobile Systems, Applications, and Services (MobiSys'12)*.

ZHANG, Z., ZHOU, X., ZHANG, W., ZHANG, Y., WANG, G., ZHAO, B. Y., AND ZHENG, H. 2011. I am the antenna: Accurate outdoor AP location using smartphones. In *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom'11)*.

ZHAO, Y., LIU, Y., AND NI, L. 2007. VIRE: Active RFID-based localization using virtual reference elimination. In *Proceedings of IEEE International Conference on Parallel Processing (ICPP'07)*.

ZHAO, Y., PATWARI, N., AND SURESH, J. M. P. 2013. Radio tomographic imaging and tracking of stationary and moving people via kernel distance. In *Proceedings of ACM International Conference on Information Processing in Sensor Networks (IPSN'13)*.

ZHOU, Z., YANG, Z., WU, C., SHANGGUAN, L., AND LIU, Y. 2013. Towards omnidirectional passive human detection. In *Proceedings of IEEE International Conference on Computer Communications (INFOCOM'13)*.

Received December 2012; revised March 2013; accepted May 2013