Precise Power Delay Profiling with Commodity Wi-Fi

Yaxiong Xie, Zhenjiang Li, *Member, IEEE,* Mo Li, *Member, IEEE,*

Abstract—Power delay profiles characterize multipath channel features, which are widely used in motion- or localization-based applications. The performance of power delay profile obtained using commodity Wi-Fi devices is limited by two dominating factors. The resolution of the derived power delay profile is determined by the channel bandwidth, which is however limited on commodity WiFi. The collected CSI reflects the signal distortions due to both the channel attenuation and the hardware imperfection. A direct derivation of power delay profiles using raw CSI measures, as has been done in the literature, results in significant inaccuracy. In this paper, we present Splicer, a software-based system that derives high-resolution power delay profiles by splicing the CSI measurements from multiple WiFi frequency bands. We propose a set of key techniques to separate the mixed hardware errors from the collected CSI measurements. Splicer adapts its computations within stringent channel coherence time and thus can perform well in presence of mobility. Our experiments with commodity WiFi NICs show that Splicer substantially improves the accuracy in profiling multipath characteristics, reducing the errors of multipath distance estimation to be less than $2m$. Splicer can immediately benefit upper-layer applications. Our case study with recent single-AP localization achieves a median localization error of $0.95m$.

Index Terms—Wireless communication; channel state information (CSI); power delay profile; resolution; bandwidth; channel combination; phase; indoor localization; time of arrival;

1 Introduction

TTH power delay profile gives the power strength of a signal received through a multipath channel as a function of propagation delay, that profiles the multipath arrivals of the signal. A power delay profile fully characterizes a multipath channel, and has been recently used in various motion- or location-based applications [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] — multipath channel dynamics can be unveiled from consecutive measures of the power delay profile, *e.g.*, tracking the power delay profile changes in a multipath channel can detect an object's movement [2, 3, 4, 11, 12], like a person's walking, falling, talking, or gestures, etc. In addition, the exact power level measured from each signal path can also be used to estimate the path length, *i.e.*, ranging between a pair of transmitters [1, 6].

A power delay profile can be measured by directly detecting multipath signals with different arrival times in the time domain, which however requires dedicated hardware of high signal sampling frequency [13, 14]. An alternative way is to measure the frequency domain CSI first and transform it into time domain power delay profile, via IFFT (Inverse Fast Fourier Transform). Fig. 1 illustrates the process (which will be detailed in §2). By adopting such a method, we are able to obtain power delay profile directly from commodity Wi-Fi devices since many Wi-Fi network interface cards (NICs), like Intel 5300, Atheros 9580, or QCA9558, support CSI measurement.

The time resolution of the derived power delay profile from CSI, *e.g.*, $\Delta\tau$ in Fig. 1(b), is limited by the bandwidth of the transmitted signal [14, 15], *e.g.*, B in Fig. 1(a), and $\Delta\tau = 1/B$. A high resolution power delay profile can differentiate subtle multipath channel changes, and consequently detect tiny activities. For the widely used 20MHz bandwidth in 802.11n [16], the power delay profile resolution is up to $50ns$, which leads to a $15m$ resolution in measuring the multipath lengths. Such a resolution imposes inevitable uncertainty in mobility detection [2, 3, 4, 5, 17], gesture recognition [18], or localization [1, 6]. For a finer grained motion detection, *e.g.*, less than $1.5m$ uncertainty to differentiate slight human body movements, at least 200MHz bandwidth is needed, which is impossible for current commodity WiFi NICs. Some recent works directly use CSI in replacement of power delay profile to learn the channel dynamics. The CSI description of the channel is, however, essentially limited by the bandwidth. In addition, CSI description is indirect and dependent of hardware uncertainty.

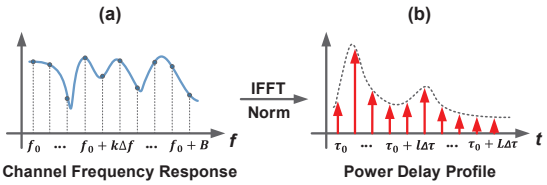


Fig. 1: Transformation from a channel frequency response to the power delay profile. (a) A channel frequency response, where f_0, Δf, and B represent starting frequency, frequency sampling resolution, and bandwidth, respectively; (b) Derived power delay profile, where τ_0 and $\Delta\tau$ represent the propagation delay of LoS path and the power delay profile resolution, respectively.

In this paper, we observe that although the width of each individual WiFi band is limited, *e.g.*, 20MHz/40MHz, the total continuous bandwidth allocated to 802.11 WiFi is wide, *e.g.*, more than 200MHz at 5GHz frequency band, which covers 10/5 different 20/40MHz channels. Furthermore, the CSIs measured from these WiFi channels can be spliced to derive a finer power delay profile with much higher time resolution. Fig. 2 reports the results of our initial measurement study in 802.11n (detailed experiment

- *Yaxiong Xie and Mo Li are with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. E-mail: {yxxie,limo}@ntu.edu.sg*
- *Zhenjiang Li is with Department of Computer Science, City University of Hong Kong, Hong Kong. E-mail: zhenjiang.li@cityu.edu.hk*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2860991, IEEE Transactions on Mobile Computing

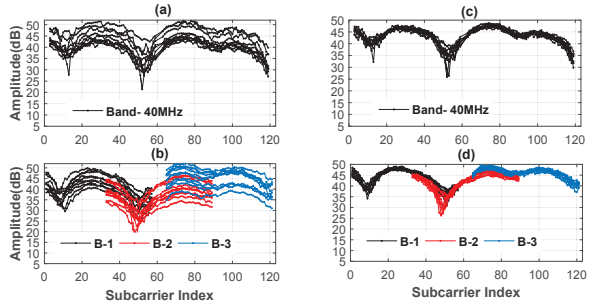


Fig. 2: CSI amplitude measurements. Raw CSI amplitudes from (a) one 40MHz 802.11n band and (b) three 20MHz bands; Amplitudes after the offset removal from (c) the 40MHz band and (d) three 20MHz bands.

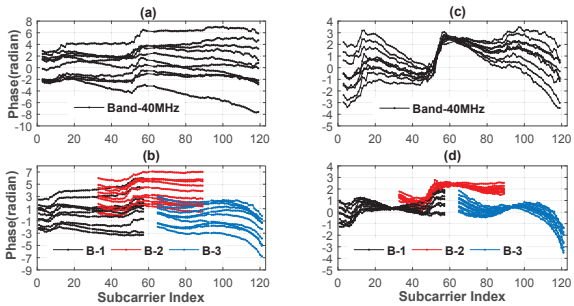


Fig. 3: CSI phase measurements. Raw CSI phases from (a) the 40MHz band and (b) three 20MHz bands; Phases after the offset removal from (c) the 40MHz band and (d) three 20MHz bands. The CSI traces in this figure are the same with Fig. 2.

settings reported in §3.1). The CSI measurements are complex values and hence contain two parts, the amplitude and the phase. Fig. 2 (a) presents the CSI amplitude measurements (multiple times) from one 802.11n 40MHz band and Fig. 2 (b) presents the CSI amplitude measurements from three 802.11n 20MHz bands that together cover the same 40MHz band in Fig. 2 (a). From Fig. 2 (a) and (b), we can observe obvious offsets between the measured CSI amplitudes at different times. After removing the amplitude offsets among all measurements, we see that the spliced CSI from 20MHz bands can be very similar in its shape to the one measured from the 40MHz band (Fig. 2 (c) and (d)).

Compared with the amplitude splicing, phase splicing may result much severer errors. Fig. 3 depicts phases of the same CSI traces in Fig. 2. The raw CSI phases[1] measured at different times have offsets as well (Fig. 3 (a) and (b)). However, even we remove their mutual offsets when splice the traces, residual phases do not have a common shape, exhibiting diverse phase shifts in different sub-carriers. Consequently, the multiple instances of CSI phase measurements from the same 40MHz channel, as depicted in Fig. 3 (c), do not match each other. The CSI traces from 20MHz bands cannot match the 40MHz measurement neither. To derive an accurate power delay profile, such phase shifts must be precisely compensated before splicing because the phase value falls in a small range of $[-\pi, \pi)$, and a slight phase error will result in significant inaccuracy in the power delay profile (as we will demonstrate in §3.1).

Challenges. Removing the CSI measurement error, however, is challenging. The CSI calculated by the commodity WiFi NICs contains the signal distortions due to both signal superimposition during the propagation and signal processing on the hardware, *e.g.*, imprecise sampling frequencies at the sender and receiver, shift of the central frequencies, and power control uncertainties. WiFi communication systems do not have to explicitly separate the two sources of signal distortions, because only end-to-end distortion needs to be captured and compensated as a whole in the equalization stage. To derive a precise power delay profile for the channel, however, it requires to precisely extract pure signal distortion caused by wireless propagation from the received signals, which on the other hand contains distortions due to channel and hardware, which is non-trivial. The sampling clock frequency uncertainty causes frequency-relevant CSI phase measurement errors in each individual channel. The central clock frequency shift and the power control uncertainty further introduce notable phase and amplitude offsets cross different channels, respectively. Based on the raw CSI measures, it is unknown how to compensate those errors for CSI splicing without the knowledge of ground-truth CSI. In addition to above challenges, wireless channels are time-varying, especially in the mobile environment. Few CSI measurements are allowed for scanning the whole WiFi band during a short coherence time. To deal with such a practical limit, we have to devise an effective method to correct and splice CSI measurements with insufficient samples and affordable computation cost.

Contributions. This paper presents a set of key techniques to address above challenges. At the high level, we exercise the observation that the CSIs collected from different frequency bands should lead to the same power delay profile that characterizes the communication channel itself. We propose an efficient method that searches for a CSI manipulation that maximizes the matching between the power delay profiles derived from CSIs obtained at different frequency bands, based on which we can perform a preliminary CSI splicing. However, the power delay profiles used for matching are derived from narrow WiFi bands with limited bandwidth, so the spliced CSI is still of low quality. We devise a wider frequency window and perform a rolling-based calibration on the spliced CSI, based on which we refine the error correction to achieve a precisely spliced CSI. To accommodate the computations in the limited coherence time, we further develop a lightweight scheduler that is able to determine the optimal number of CSIs to measure from each individual WiFI band to strike a trade-off between the error compensation and the total bandwidth that can be afforded for the CSI splicing.

We develop a system, called Splicer, to incorporate above techniques on commodity Wi-Fi routers, which currently work on the monitor mode and use the traffics by disabling the frame aggregation (not regular ones) for the CSI splicing (§4). Our benchmark experiments show that Splicer can derive high resolution power delay profiles from spliced CSI. We evaluate the derived power delay profile by estimating

1. A raw CSI phase is in the range of $[-\pi, \pi)$. For a clear representation, we expand the measured CSI phases θ, using $\theta = \theta \pm 2k\pi$, to the range of $[-\infty, +\infty]$ across different channels.

the distance between the sender and the receiver. According to our experiments, Splicer can reduce the median ranging error from $7.1m$ to $1.63m$ compared with using raw CSI traces from NICs. In light of such a high resolution, Splicer can immediately enhance the performance of a plethora of upper-layer applications without additional modification to the original application design. We demonstrate this benefit with a case study. We build the recent single-AP localization CUPID [6] on top of Splicer. Our evaluations show that the localization accuracy can be substantially improved. In particular, Splicer improves the CUPID localization accuracy by 71%, with median localization errors about $0.95m$.

2 Principle of CSI Splicing

In this section, we will lay the theoretical foundation for proposed CSI splicing mechanism. We will demonstrate the feasibility and effectiveness of splicing CSI from multiple channels for deriving a high resolution power delay profile.

Calculation of power delay profile. According to [14, 15], the channel frequency response $h(f)$ can be expressed by:

$$h(f) = \sum_{l=0}^{L} \alpha_l \cdot e^{-j \cdot 2\pi \cdot f \cdot \tau_l}, \quad (1)$$

where L is the total number of multipaths, α_l and τ_l stand for the attenuation and the propagation delay of the signal that travels through path l, respectively. Commercial Wi-Fi is capable of sampling the channel frequency response. In particular, Wi-Fi samples the response at a group of discrete frequency points $f = f_0 + k\Delta f$, where k is the index of sampling points, *i.e.*, subcarrier, and $\Delta f = 312.5kHz$ is the sampling resolution, which equals to the width of subcarrier. Fig. 1 (a) gives us an example of measured channel frequency response with the channel bandwidth $B = K\Delta f$ and subcarrier number K. Such an measurement will be reported by commodity Wi-Fi with the format of CSI.

To obtain the power delay profile, the CSI can be transformed to the channel impulse response $f(t)$ by IFFT:

$$f(t) = \sum_{l=0}^{L} \alpha_l \cdot \delta(t - \tau_l), \quad (2)$$

where $\delta(\cdot)$ is the delta function, and L, α_l, and τ_l have the same definitions as they are in Eq. (1). Fig. 1 (b) illustrates the channel impulse response transformed from Fig. 1 (a). The norm of $f(t)$, $||f(t)||_2$, then gives the power delay profile, which describes both the power level and propagation delay of the signals arrives from each multipath.

Feasibility of CSI splicing. According to Eq (1), given one multipath channel, *i.e.*, given each α_n, τ_n, and N in Eq (1), and channel bandwidth B, the channel frequency response is *deterministic* at each frequency f. We can thus obtain all M frequency response samples from either a single measurement covering the entire bandwidth or multiple measurements where each measurement covers a subset of M samples. With the M samples, we can derive a unique power delay profile using Eq. (2) and the norm operation.

Resolution of power delay profile. After the IFFT transformation, we obtain a series of signal samples in the time domain with various delays τ_l in Eq. (2). The norm of each multipath component, $||\alpha_l \cdot \delta(t - \tau_l)||_2$, indicates its power level as shown in Fig. 1 (b), where the first impulse corresponds to the Line-of-Sight (LoS) path. According to the IFFT theory, time resolution $\Delta\tau$ of power delay profile is related to the sampling resolution Δf of the channel impulse response by $\Delta\tau = 1/(N \cdot \Delta f)$, where N is the IFFT length. As $N \cdot \Delta f = B$, we have $\Delta\tau = 1/B$, where B is the bandwidth. Such a connection indicates that a wider bandwidth CSI leads to a higher resolution of power delay profile.

Given channel bandwidth B, two multipaths of propagation delays τ_1 and τ_2 are not distinguishable if $|\tau_1 - \tau_2| < 1/B$. Hence, all multipaths whose propagation delays differences are less than $1/B$ are viewed as one multipath component in the power delay profile, and the corresponding power level indicates the aggregated power level of those multipaths. Hence, the time resolution $\Delta\tau$ leads to $\frac{c}{B}$ uncertainty in terms of the length difference between non-distinguishable paths, where c is signal propagation speed. In 802.11 WiFi with 20MHz or 40MHz, the path length uncertainty is $15m$ or $7.5m$, respectively, which can merely support coarse mobility tracking and activity recognition.

3 Design

In this section, we present the design of Splicer. We first present the CSI measurement error by experiment. We then identify the error source of the observed errors and propose our method to compensate them. A lightweight scheduler is also proposed to battle the timing requirement.

3.1 CSI splicing in practice

We first locate the error sources of CSI splicing in the 802.11 physical layer in §3.1 and then present the design details to address each of them from §3.2 to §3.5.

CSI measurement errors. We first investigate how CSI measurement errors will affect the derived power delay profiles. We use Atheros 9580 NICs that support 802.11n with 20MHz/40MHz channels at the 2.4G/5G frequency band, and modify the driver to extract CSI from the physical layer. We configure one Atheros node to transmit packets with minimum payload to ensure a short transmission delay, *i.e.*, about $0.2ms$. We also disable the frame aggregation so that the Wi-Fi NIC calculates CSI for every packet. We collect the CSI traces using another Atheros node, from one 802.11n 40MHz band and three 20MHz bands. The measurement results are reported in Fig. 2 and Fig. 3, which have been discussed in §1. In this section, we further derive the power delay profiles and investigate how the CSI amplitude and phase errors may impact the final power delay profiles.

CSI amplitude. We select two arbitrary CSI traces from the same WiFi band (20MHz-2 in Fig. 2) with an amplitude offset of 7dB, and derive two power delay profiles[2]. Fig. 4 shows that although two derived power delay profiles have different power levels, *e.g.* the average difference is 7.05 dB, they follow similar shapes. We compute the variance of the power difference for each path to quantify the similarity of two power delay profiles, which is less than 1.0 dB. We observe similar results from other CSI combinations. All of these results indicate that the derived power delay profiles approximately characterize the same multipath channel environment except that their power levels are scaled due to amplitude offsets of the CSI measurements.

2. To isolate phase's impact, we use average phases of two CSI traces, so that the derived power delay profiles only differ by amplitudes.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2860991, IEEE Transactions on Mobile Computing

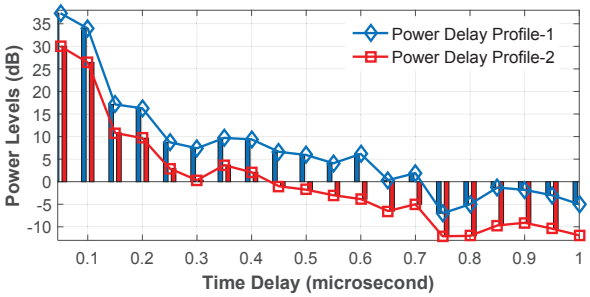


Fig. 4: Power delay profiles derived using two CSI with an amplitude offset of 7dB.

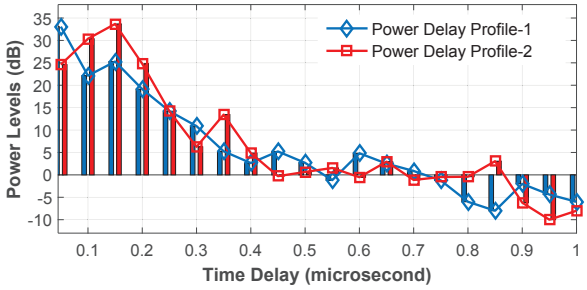


Fig. 5: Power delay profiles derived using two CSIs with raw phases and average amplitude of the CSI traces in Fig. 4.

CSI phases. We then use the raw phases of two CSI traces in Fig. 4 to derive two power delay profiles[3]. The two profiles in Fig. 5 demonstrate opposite results. One power delay profile indicates the existence of the LoS between the transmission pair (*i.e.*, the first multipath component has the strongest power level), however another one indicates that there is no LoS (NLoS) path (*i.e.*, the first arrived signal is much weaker in strength than later arrived signals). In addition, the power levels of each multipath component in these two profiles are very different, *e.g.*, the power difference of the LoS path is more than 10 dB and the variance of the power level differences is up to 4.7 dB. Fig. 5 indicates that the CSI phase errors will significantly impact the derived power delay profiles, which completely change both the power loss and the multipath channel features.

As our initial experiment results suggest, raw CSIs are mixed with hardware distortions and hence cannot be used to derive accurate power delay profiles. We identify the measurement error sources in 802.11 physical layer process and propose solutions to compensate each of them.

Sources of CSI measurement errors. Fig. 6 illustrates the wireless signal processing in the 802.11 NICs. An incoming signal from the antenna is down converted to the base band signal $s(t)$ and sampled by Analog-to-Digital (ADC) to derive the digital $s[n]$. The packet boundary detector (PBD) performs correlation between $s[n]$ and a pre-defined 802.11 preamble pattern to confirm an incoming packet. Once the preamble of a packet is detected, the signal central frequency is calibrated by the central frequency offset (CFO) corrector. The OFDM receiver estimates the CSI based on the calibrated $s[n]$ and the CSI is passed to the subsequent equalization module (not shown) to compensate errors prior to the packet decoding. Due to the hardware imperfection, the CSIs measured by NICs introduce the following errors.

Power control uncertainty. Limited by the hardware resolution, Automatic Gain Controller (AGC) cannot perfectly compensate the signal amplitude attenuation to the transmitted power level. The measured CSI amplitude equals to the compensated power level, which is mixed with the power control uncertainty error that has to be removed.

System nonlinearity. Due to hardware imperfection, the Wi-Fi receiver demonstrates nonlinearity which causes nonlinear phase error in the frequency domain.

Channel bonding. Wi-Fi achieves 40MHz channelization by combining two adjacent 20MHz sub-channels. The signal

3. Similar to Fig. 4, we use average amplitude of the two CSI traces to derive power delay profiles to avoid the impact from the amplitude.

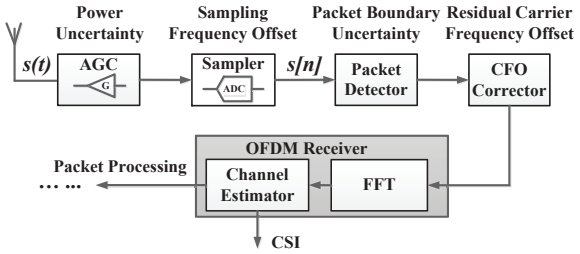


Fig. 6: Illustration of signal processing in 802.11.

received from two 20MHz sub-channels are not coherent with each other and demonstrate unmatched phase value.

Sampling frequency offset (SFO). The sampling frequencies of a transmission pair exhibit an offset due to non-synchronized clocks, which can cause frequency dependent phase error λ_o to received signals.

Packet boundary detection (PBD) shifts. The starting point of a packet estimated by the packet detector exhibit a time shift τ_b with the ground-truth, which will also cause frequency dependent phase error λ_b to received signals.

Central frequency offset (CFO). The central frequencies of the transceiver cannot be perfectly synchronized. The central frequency offset is compensated by the CFO corrector, but due to the hardware imperfection, the compensation is incomplete. Signal $s[n]$ still carries residual errors, which can cause the CSI phase offsets β.

Power control uncertainty introduce error to the measured CSI amplitude and the last five error sources cause error to the measured CSI. In the next section, we focus on demonstrating in detail how those error sources impact the measured CSI phase followed by our solutions to compensate above CSI phase errors. Our method to deal with error in measured CSI amplitude is presented in §3.4.

3.2 Phase error compensation

In this section, we demonstrate how the error impacts the CSI we measured, and we propose our method to compensate them. We observe that errors in CSI phase can be categorized into two types: linear and nonlinear. We begin with the introduction of nonlinear errors.

3.2.1 Nonlinear phase error

The end-to-end Wi-Fi transmission in theory is a linear system. The hardware imperfections, however, could introduce nonlinearity to the received signals. To verify this point, we conduct a controlled experiment by connecting the radio

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2860991, IEEE Transactions on Mobile Computing

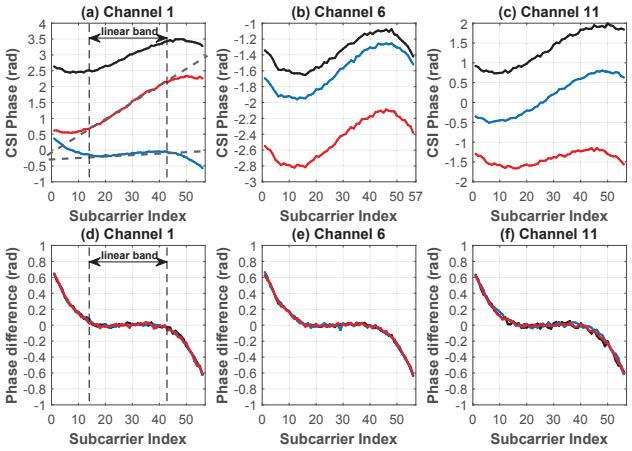


Fig. 7: The CSI phases measured from three non-overlapping channel: (a) 1, (b) 6 and (c) 11. The phase is not linear across the whole band. We use the linear band to predict the phase and calculate the nonlinearity for channels (d) 1, (e) 6 and (f) 11.

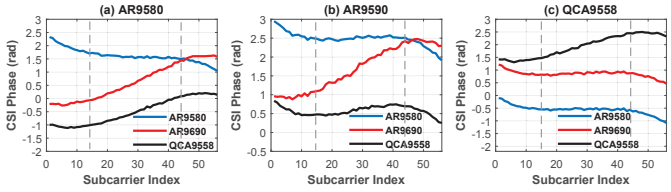


Fig. 8: The CSI phases measured from (a) AR9580, (b) AR9590 and (c) QCA9558 as receivers. For each receiver, we use other AR9580, AR9590 and QCA9558 devices as senders.

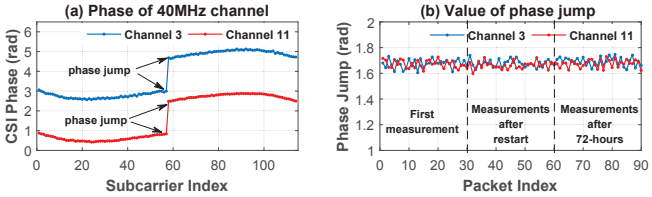


Fig. 9: Phase jump due to channel bonding. (a) Phase jumps in different channels. (b) The stability of phase jumps over time.

chains of two Wi-Fi devices via the coaxial cable to eliminate the multipath effect. According to [19], the phase of the received signal is determined by the cable length d, *i.e.*, $\phi = 2\pi f \frac{d}{c}$, where f and c is the frequency and speed of the signal. Therefore, the phase of subcarrier k with frequency $f = f_0 + k\Delta f$ can be represented as:

$$\phi_k = 2\pi(f_0 + k\Delta f)\frac{d}{c} = (2\pi\Delta f \frac{d}{c})k + 2\pi f_0 \frac{d}{c}, \quad (3)$$

where the bandwidth Δf of one Wi-Fi subcarrier. It equals $312.5kHz$. Eq. (3) indicates that the phase of subcarrier should change linearly with its frequency and the slope is determined by the propagation path length d. However, the experiments show that the measured CSI phases are not linear all the time. Fig. 7 (a), (b) and (c) depict the phases of three CSIs measured from channel 1, 6 and 11 at 2.4 GHz, respectively. From the results, we observe the central part (subcarrier 15 to 44) exhibits strong linearity, while the rest subcarriers exhibit strong nonlinearity.

To isolate the nonlinearity, we derive the theoretical phase of those non-linear subcarriers. In particular, we use a least square linear fitting with the central subcarriers (15 to 44) to estimate the slope $(2\pi\Delta f \frac{d}{c})$ and offset $2\pi f_0 \frac{d}{c}$ in Eq. (3), which is further used to predict the phase of non-linear subcarriers according to Eq. (3). We thus obtain the (predicted) linear CSI phases $\hat{\phi}_k$ for all 56 subcarriers.

The nonlinearity is then calculated as the difference between the theoretical linear phase $\hat{\phi}_k$ and the measured phase ϕ_k, which is plotted in Fig. 7 (d), (e) and (f). We observe that the nonlinearity caused by the Wi-Fi hardware is constant for each subcarrier, and the nonlinearity is very stable over time as the three CSIs are measured with 30 minute delay. We also experiment with different cable lengths, and find that the nonlinearity is always the same, implying it does not change with distance. We further examine the phase linearity and nonlinearity regions cross 3 different Atheros devices. Fig. 8 shows that the linearity regions are 10MHz wide across devices (subcarriers 15-44), while the phases are nonlinear outside this region. We also test for WARP software-define-radio and observe WARP has a wider linear region (about 30MHz for subcarriers 16-112).

As nonlinearity $\phi_k - \hat{\phi}_k$ is constant for one device, we thus measure the nonlinearity off-line and subtract it to retrieve the linear phase of each received CSI. Through the nonlinearity measure, we also know the exact width of a device's original linear band.

Channel bonding. Wi-Fi achieves 40MHz channelization by combining two adjacent 20MHz sub-channels. The phase of the signal received from two sub-channels is not coherent since they are processed separately and thus exhibits unmatched signal phases, which also break the linearity of the CSI phase. Fig. 9 (a) plots the phase of the raw CSI measured from two 40MHz channels. Specifically, the first 57 subcarriers are from first subchannel. We can observe a sudden jump between the phase from two subchannels, while the phase within each subchannel is smooth. Such a phase jump breaks the linearity of overall 40MHz channel.

To remove this phase jump, we conduct another experiment to measure its value in Fig. 9 (b). We then repeat this measure after we restart the device and further after 72 hours in Fig. 9 (b). We can see that the value of the phase jump is quite stable (variance is less than 0.001 radian). We thus treat it as a constant and remove its impact by subtracting this off-line measured value.

In summary, although the hardware imperfection could incur nonlinear phase errors, we find the nonlinearity is stable and constant. Thus, they can be well compensated by off-line training, which is only one-time effort for a device.

3.2.2 *Linear phase error*

After the removal of nonlinearity in measured CSI phase, the residual CSI errors are linear and can be modeled as follows. We denote S as the number of subcarriers in one WiFi band. Based on [20, 21], the reported CSI phase value ϕ_k from any sub-carrier k by WiFi NICs can be expressed:

$$\phi_k = \theta_k + k \cdot (\lambda_b + \lambda_o) + \beta, \quad (4)$$

where θ_k is the phase rotation of subcarrier k that is caused by the channel propagation, λ_b and λ_o are phase errors introduced by the packet boundary detection uncertainty

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2860991, IEEE Transactions on Mobile Computing

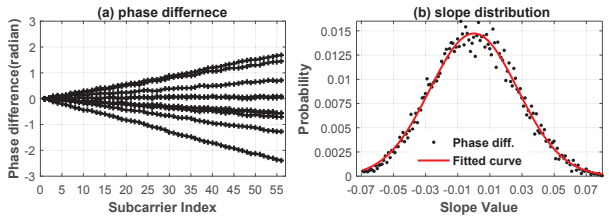


Fig. 10: Phase differences cross sub-carriers and the distribution of $\Delta\lambda_b$. (a) The phase differences $k \cdot \Delta\lambda_b$ of 8 randomly CSI pairs; (b) Distribution of slope $\Delta\lambda_b$ calculated from 180 CSIs.

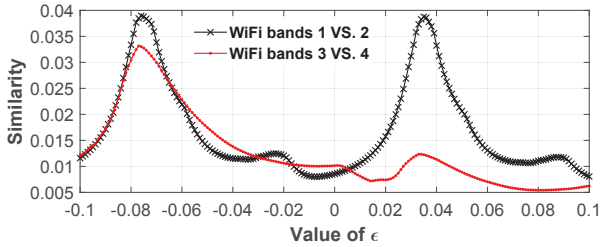


Fig. 11: The power delay profile similarities for two pairs of WiFi bands when ϵ varies from -0.1 to 0.1.

and the sampling frequency offset, respectively, β is the phase error caused by the central frequency offset, and $k = 1, 2, \ldots, S$. As $\lambda_b + \lambda_o$ is multiplied by the sub-carrier index k in Eq. (4), the phase errors cross different sub-carriers are diverse among different CSI measures as shown in Fig. 3. Our target is to obtain the phase value θ_k by eliminating the impact of other parameters, *i.e.*, the λ_b, the λ_o and the β. We focus on the removal of λ_b and λ_o from ϕ_k in the rest of this subsection, and introduce the removal of β when we splice the CSI phases in §3.3.

PBD phase error λ_b removal. Phase error λ_b is caused by the time shift τ_b from the packet boundary detection uncertainty. To investigate the effect of τ_b, we examine the discrete Fourier transform of the channel frequency response in Eq. (5):

$$h[k] = \sum_{n=0}^{N-1} f[n] \cdot e^{-j \cdot 2\pi \cdot k \cdot n/N}, \tag{5}$$

where $h[k]$ and $f[n]$ are the discrete versions of $h(f)$ in Eq. (1) and $f(t)$ in Eq. (2), respectively, and N is the IFFT length. With a time shift τ_b in $f[n]$, Eq. (5) can be rephrased:

$$h[k] \cdot e^{-j \cdot 2\pi \cdot k \cdot \tau_b/N} = \sum_{n=0}^{N-1} f[(n - \tau_b)_N] \cdot e^{-j \cdot 2\pi \cdot k \cdot n/N},$$

where the term $e^{-j \cdot 2\pi \cdot k \cdot \tau_b/N}$ indicates that the time shift τ_b can introduce a phase error, $2\pi \cdot k \cdot \tau_b/N$, in each sub-carrier k. Therefore, $\lambda_b = 2\pi \cdot \tau_b/N$.

To remove λ_b from each ϕ_k, we leverage an observation that the time shift τ_b follows a Gaussian distribution with the zero mean [20]. The error λ_b thus changes accordingly with τ_b and follows the same distribution $\lambda_b \sim N(0, \sigma^2)$, where σ is the standard deviation. According to the weak law of large numbers, λ_b can be removed by averaging over the measured CSI phases ϕ_k.

To validate this observation, we perform a trial of experiments in Fig. 10. In Eq. (4), λ_b is mixed with λ_o, β, and θ_k in the CSI phase ϕ_k, and we cannot directly investigate its distribution. Therefore, for the collected CSIs from the same WiFi band, we calculate the mutual phase differences of those CSIs and obtain a set of $\Delta\theta_k + k \cdot (\Delta\lambda_b + \Delta\lambda_o) + \Delta\beta = k \cdot \Delta\lambda_b + a$ for each sub-carrier k[4]. The mutual phase difference is a straight line with slope of $\Delta\lambda_b$ and y-intercept of a. We thus examine the distribution of $\Delta\lambda_b$, because if $\lambda_b \sim N(0, \sigma^2)$, $\Delta\lambda_b$ should be a Gaussian with the zero mean as well. We collect 180 CSIs from a 20MHz channel within a short time interval when the environment is stable.

4. λ_o is a constant that can be removed by the deduction, which is detailed in the SFO phase error removal.

Fig. 10 (a) plots the $k \cdot \Delta\lambda_b$ value versus the sub-carrier index k for 8 randomly selected CSI pairs. Fig. 10 (a) shows each line is a straight line and the slopes of those lines are different. The result indicates that λ_b is a constant to each sub-carrier in each individual measure, but varies cross different measures, and a is also a constant (but we do not need to know its value). To further examine its distribution, in Fig. 10 (b), we divide the range $[-0.075, 0.075]$ into 100 bins on the x-axis and plot the frequency of $\Delta\lambda_b$ falling into each bin on the y-axis. After the curve fitting, we find that $\Delta\lambda_b$ indeed follows a Gaussian distribution with the zero mean.

According to the distribution of λ_b, we can remove its impact by averaging over the measured CSI phases ϕ_k. In principle, more measurements lead to a better error removal, but it will prolong the latency to scan each single band. In §3.5, we will determine an optimal number of CSIs collected from each band to balance this trade-off subjected to the stringent channel coherence time. Given the optimal amount $\dot{n}_i$ for any band i, we calculate:

$$\overline{\phi}_k^i = \sum_{i=1}^{\dot{n}_i} \phi_k^i(j)/\dot{n}_i, \tag{6}$$

where $\phi_k^i(j)$ stands for the j-th CSI measure from band i. After λ_b is removed, $\overline{\phi}_k^i = \theta_k^i + k \cdot \lambda_o + \beta$. In the next subsection, we introduce how to remove λ_o from $\overline{\phi}_k^i$.

SFO phase error λ_o removal. Phase error λ_o is caused by the offset of the sampling frequencies of the sender and the receiver, f_s and f_r. We denote $\zeta = \frac{f_s}{f_r} - 1$ as the fractional difference in sampling frequency, and the effect of the sampling frequency offset is to introduce a term, $e^{j \cdot \zeta' \cdot k}$, to the channel frequency response: $h'[k] = h[k] \cdot e^{j \cdot \zeta' \cdot k}$, where ζ' stands for ζ multiplied with a constant and $h[k]$ is the channel frequency response without the sampling frequency offset (Eq. (5)). Hence, $\lambda_o = \zeta'$. As the fractional frequency difference keeps stable in the order of minutes [22], λ_o is a constant during the process of the CSI splicing.

To remove λ_o from $\overline{\phi}_k^i = \theta_k^i + k \cdot \lambda_o + \beta$, obtained from Eq. (6), we leverage an observation that the power delay profiles derived from different WiFi bands should be the same after λ_o is removed (we will show in §3.3 that the phase offest β has no impact on the derived power delay profile), since they characterize the same multipath channel. For any WiFi band i, the CSI phases $\overline{\phi}_k^i$s from all S sub-carriers form a vector $\overline{\Phi}^i = [\overline{\phi}_1^i, \overline{\phi}_2^i, \ldots, \overline{\phi}_S^i]^T$. Therefore, we propose to gradually "rotate" two distinct $\overline{\Phi}^i$ and $\overline{\Phi}^j$ in the

Algorithm 1: SFO Phase Error Compensation

1 **for** *each WiFi band pair c* **do**
2 Record the top-two local maximal similarity values and the corresponding ϵ: $< \epsilon_1^c, \rho_1^c >$ and $< \epsilon_2^c, \rho_2^c >$.
3 Clustering on ϵ and find the cluster with the maximal similarity sum.
4 Return the cluster center as the final ϵ value.

frequency domain[5] and stop when the two derived power delay profiles best match each other. We repeat this process for different pairs of WiFi bands to improve the accuracy. To quantify the likelihood of two power delay profiles, *e.g.*, P_1 and P_2, we define their similarity as:

$$\rho(P_1, P_2) = \frac{1}{||P_1 - P_2||_2}, \quad (7)$$

where the dominator essentially measures the power level differences of each multipath component in the two power delay profiles. A large $\rho(P_1, P_2)$ value indicates that P_1 and P_2 are more similar.

To illustrate this solution, we measure four different 20MHz WiFi bands, and compute the similarities for two channel pairs in Fig. 11. We compensate λ_o by $\lambda_o - \epsilon$ and search for the optimal ϵ for both positive and negative directions. For the first pair, we observe four local maximum points, and for the second pair, we observe three local maximum points when ϵ varies in $[-0.1, 0.1]$. According to Algorithm 1, we can determine the final ϵ as the average of ϵ_1 and ϵ_2 in Fig. 11. With the optimal ϵ obtained from Algorithm 1, for each $\overline{\Phi}^i$ after the PBD phase error λ_b removal, we can further remove λ_o by $\widetilde{\Phi}^i = \overline{\Phi}^i - [\epsilon, 2\epsilon, \ldots, S\epsilon]^T$, where S is the number of subcarriers.

Although the ϵ searching introduces extra computational delays, Algorithm 1 does not need to be executed parallel to the CSI sampling in real-time. As a matter of fact, once sufficient CSIs can be obtained subjected to the stringent channel coherence time (§3.5), the latency of Algorithm 1 only impacts the frequency to generate power delay profiles to the upper-layer applications. We evaluate the computational efficiency in §5.

CSI phase offset β removal. Fig. 12 plots the corrected CSI phases at this stage for the three 20MHz channels in Fig. 3 (b). From the result, we observe that after the phase error removals of λ_b and λ_o, the shapes of the overlapped sub-carrier phases from different WiFi bands now become similar and consistent. The only barrier that remains is the offsets. In this subsection, we target to removing offsets to finally enable the phase splicing.

Phase offset β is caused by the central frequency offset of the transmission pair. Through our study, we find that for individual WiFi bands, phase offset β has no impact on the derived power delay profile, *i.e.*, given a pair of CSI amplitude (ω) and phase (θ), the power delay profile derived by ω and θ is identical to the one derived by ω and $\theta + \beta$. The reason is that offsets are frequency independent. After IFFT, the error will result in a constant phase rotation term in each α_l of Eq. (2). We do not need to derive such an phase rotation since it causes no change to the norm operation result. Hence the power level of each multipath component keeps unchanged. According to this observation, we can use the phase measured from any band as a reference and compensate β by calibrating the phases measured from other bands with respect to the reference.

5. We rotate the phase by multiplying $\overline{\Phi}^i$ and $\overline{\Phi}^j$ with $e^{j\cdot\epsilon\cdot k}$, and gradually vary ϵ.

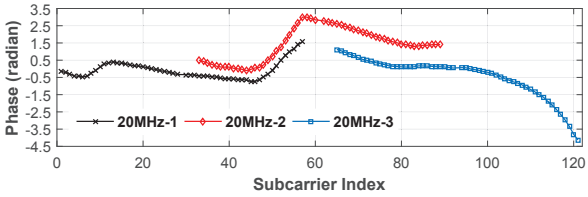


Fig. 12: CSI phases after the removal of λ_s and λ_o. We can see obvious offset between phases of CSI from different channels.

Unused subcarriers. Subcarriers of one Wi-Fi channel are not fully utilized and some of them are reserved to be empty, *i.e.* the central/DC subcarrier is empty to prevent DC offset and edge subcarriers serve as a guard band to avoid interference from neighboring channels [23]. Wi-Fi devices do not report CSI for empty subcarriers and set them to null. Deriving power delay profile using IFFT, however, requires continuous CSI report in frequency domain [24].

In communication theories, the coherence bandwidth B_c is used to describe the frequency interval over which two frequencies of a signal are likely to experience correlated fading (correlation level larger than 0.9). Thus, the channel responses at two frequencies f_0 and f_1 are strongly correlated with each other if their frequency difference $|f_0 - f_1|$ is smaller than B_c. Prior measurements show that B_c for a typical indoor channel is larger than $10MHz$. In other words, the CSI value of nearby subcarriers are strongly correlated, and their amplitude and phase curves exhibit smoothness. Based on the smoothness, we use curve fitting to recover empty subcarriers. We first find the curve that best fits the measured CSI. We then recover the DC subcarrier in the center, with the fitted curve of that channel. CSIs of the edge subcarriers are retrieved by averaging the recovering results using the fitted curves of two neighboring channels.

3.3 CSI phase splicing

So far, the CSI phases measured from different channels can be spliced already. However, we find that the CSI phase accuracy can be further improved by leveraging the primarily spliced result. In the SFO phase error λ_o removal, we rely on the similarity of the derived power delay profile to compensate λ_o, but the derived power delay profiles are based on the CSI from single WiFi bands with limited bandwidth. The phase error λ_o thus cannot get fully corrected using low-resolution power delay profiles. To refine the phase information, in the phase splicer, we further manually divide the spliced channel bandwidth into multiple windows illustrated in Fig. 13. Each window has a much wider bandwidth, denoted as l, than each single WiFi band. We slide the window and obtain a set of l-wide phase pieces. For each phase pair, we call Algorithm 1 to estimate

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2860991, IEEE Transactions on Mobile Computing

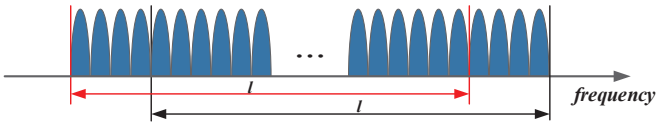


Fig. 13: Spliced CSI phase refinement.

the SFO phase error compensator ϵ, and use their average value to further compensate the spliced CSI phase.

In Fig. 13, the window size l balances a trade-off. A larger l will lead to a higher-resolution power delay profile, which potentially can better compensate the phase error λ_o. However, with a large l, the channel information carried by each divided CSI piece will be highly redundant (more overlapped sub-carriers). Two such power delay profiles will produce a large body of local maximal points in Fig. 11, which are dominated by the channel information redundancy, instead of the removal of the phase error λ_o. It thus prevents to find the optimal ϵ to compensate λ_o. Therefore, the length l needs to be carefully selected. In Fig. 14, we investigate this trade-off. The experimental setting is detailed in §5, where we use ranging accuracy as the metric for the evaluation. We set the window size l as a fraction of the total bandwidth that the spliced CSI covers. Initially, when we increase the window size, the ranging accuracy improves because λ_o is better compensated by higher-resolution power delay profiles. However, when l is excessive large, *e.g.*, close to 0.95, the accuracy decreases due to the unreliability in the optimal ϵ search. According to Fig. 14, we set l to be $\frac{3}{4}$ of the total bandwidth that the spliced CSI covers as default in Splicer.

3.4 CSI amplitude splicing

In Fig. 2, we have shown that the amplitudes of raw CSIs also exhibit significant offsets. The reason is that the power control uncertainty [25, 26], which also follow a Gaussian distribution. However, different from the CSI phases, the power uncertainty is frequency band independent, *i.e.*, the amplitudes measured from different bands follow the same distribution. Thus, for CSI amplitudes, there is no need to average them for individual WiFi bands. Instead, we can average the amplitudes after we collect all CSIs for the splicing. The total number of CSIs to collect for splicing is determined by the channel coherence time, which will be discussed and given in the next subsection.

3.5 Battle the coherence time constraint

Wireless channels are time-varying, which enforce a stringent time budget for each round of CSI splicing, since the spliced CSI is valid only when the channel condition is relatively stable [27]. In this subsection, we first estimate the minimum number of CSIs to collect from each individual band that can fully compensate phase errors, and then propose an efficient CSI sampling scheduler to balance the trade-off between the error compensation quality in each individual band and the total bandwidth that can be afforded for the CSI splicing within the time budget.

Stringent time budget. The channel coherence time T_c can be expressed as $T_c \approx \frac{1}{2 \cdot f_d}$, where f_d stands for the Doppler

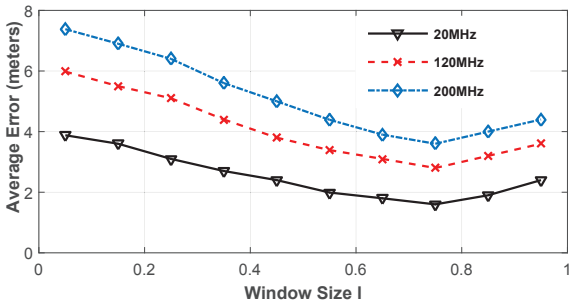


Fig. 14: Empirical investigation of window size l.

shift. Previous works [15] have studied the Doppler shifts caused in typical mobile environments. For instance, when people are walking, the Doppler shifts are usually less than 12Hz, which can be translated into $T_c = 40ms$ with 2.4GHz WiFi. In Splicer, the transmission delay of each packet (with minimum payload) is around $0.2ms$, *e.g.*, approximately 200 CSIs can be collected within the time budget. In our current design, we reply on the empirical results from the literature to set T_c. We leave the cooperation with advanced channel coherence time measurement schemes [28] in Splicer as the future work of this study.

CSI measurements for each band. As aforementioned in §3.2, for each WiFi band, we need to collect sufficient CSI measures to fully compensate phase error λ_b, which is caused by the signal boundary detection uncertainty and follows a Gaussian distribution. According to the weak law of large numbers, more CSIs lead to a better compensation. However, we have a stringent time budget T_c to scan the entire WiFi band, which on the other hand limits the number of CSI collected from each WiFi band. To deal with this trade-off, we first investigate the minimum number of CSIs for each band that can achieve a given confidence level.

When we collect n CSIs from one band, for any sub-carrier k, we can calculate the average phase value $\overline{\phi}_k$ by Eq. (6). According to [29], we can define a confidence range $(\overline{\phi}_k - \frac{\sigma}{\sqrt{n}} z_{\alpha/2}, \overline{\phi}_k + \frac{\sigma}{\sqrt{n}} z_{\alpha/2})$, where σ is the standard deviation of λ_b, α is an error rate, and z_j is a normal distribution related parameter that can be obtained from a table [29]. When n increases, the range shrinks, *i.e.*, the confidence increases. The theory in [29] proves that the probability that $E[\phi_k]$ falls into this range is greater than $1 - \alpha$. Therefore, given α and the confidence range length r, the minimal number of CSIs to collect, $\dot{n}$, can be determined when $\frac{\sigma}{\sqrt{\dot{n}}} z_{\alpha/2} \leq r/2$.

We note that although the CSI phase value ϕ_k consists of several variables λ_b, λ_o and β, and only λ_b directly follows the Gaussian distribution, the estimation above can still work with the following processing. In §3.2, we know λ_o is a constant. So $\lambda_o + \lambda_b$ is Gaussian. On the other hand, we may not be aware β's exact distribution, but is a constant for one CSI measurement across different subcarriers. Hence, if we look at the phase difference of subcarriers with index $k = 0$ of two CSI phase ϕ_1 and ϕ_2, we have

$$\phi_{dif} = \phi_1 - \phi_2 = \beta_1 - \beta_2, \quad (8)$$

where β_1 and β_2 are the phase error β contained in two CSIs. From Eq. (8), we obtain the difference of two β contained in two different CSIs. Then we can use the first CSI with β_1

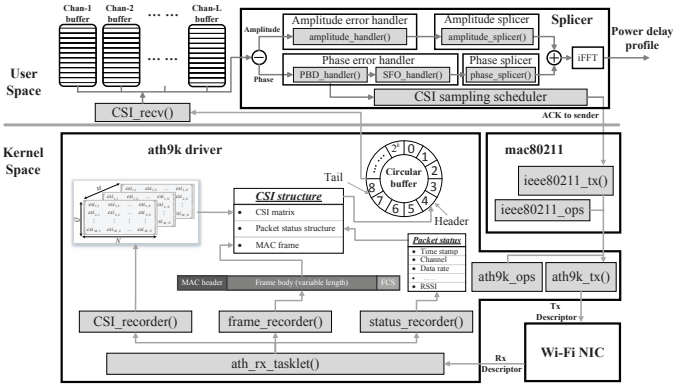


Fig. 15: Architecture of Splicer implemented on Linux systems.

as the reference and add the ϕ_{dif} to the second CSI with β_2. Thus, the β added to every subcarrier of the second CSI is given by $\beta_2 + \phi_{dif} = \beta_1$, which is the same as the reference. Afterwards, the phase value ϕ follows a Gaussian distribution and we can apply above estimation design.

To cover the entire WiFi band, we need to scan multiple (*e.g.*, C) individual WiFi bands, *e.g.*, $C = 5$ for 802.11n at 2.4GHz. However, due to the stringent time budget, it could be infeasible to collect all $C \times \dot{n}$ CSIs within T_c. Therefore, we propose to balance the trade-off between the error compensation quality in each individual band and the total bandwidth that can be afforded for the CSI splicing. Through our study, we observe that for any three consecutive WiFi bands, if the CSI phases in the first and the third channels are well compensated, they can serve as two anchors to further calibrate the CSI phase from the second band if its phase error is not fully corrected. In particular, we can rotate the CSI phase from the second band and stop when its phase differences for the overlapped sub-carriers with other two bands are minimized. With this observation, the scheduling of the CSI measurement for each band is as follows. We have three constraints:

- Collecting $\dot{n}$ CSIs from a set of WiFi bands whose indices are odd. They form anchors.
- For each even-indexed band in between, we set a lower bound that the number of CSIs collected from those even-indexed bands is greater than this bound.
- All CSIs are collected within the time budget T_c.

The scheduling objective is to maximize the total number of bands, both odd and even, that can be used for the CSI splicing. After solving this optimization problem, we can determine the optimal CSI collection assignment. When enough CSIs are collected from each band, the CSI sampling scheduler informs the physical layer to send an ACK such that the sender and the receiver switch to the next band synchronously. As a contingency plan, the sender and receiver will switch back to the first channel if no packets received for a given time-out duration.

Early termination. Due to the wireless channel dynamics, the time budget we adopt from the literature may not always precisely capture the channel coherence time. It is possible that the wireless channel changes dramatically in the middle of CSI collection so that the CSIs from rest WiFi bands will become useless for splicing. To address this issue, we propose an early termination strategy to detect such a case in real time, which leverages the following observation. If the channel is stable, θ_k for any sub-carrier k of a WiFi band in Eq. (4) keeps unchanged. When we collect multiple CSIs from this band and compute their phase differences, we can obtain a set of straight lines as shown in Fig. 10. Later when channel condition is changed, if we collect another CSI trace from the new channel and compare the phase difference with the CSI from the previous channel, the result demonstrates not a straight line. To quantify this distortion, we apply the linear fitting on the phase difference and calculate R^2 to measure the *goodness-of-fit* [30] and empirically set 0.9 as threshold, *i.e.* when $R^2 < 0.9$, the splicing terminates.

4 Implementation

We implement Splicer on various hardware platforms, *e.g.* Wi-Fi routers, Arduino boards and Laptops. All those devices are equipped with Atheros Wi-Fi NIC and run various Linux based OS, *i.e.*, OpenWRT for router, Linino for Arduino and Ubuntu for laptops.

Figure 15 illustrates the architecture of Splicer, which is implemented on Linux systems. In the kernel space, Splicer receives CSI from Wi-Fi NIC and stores it into a circular buffer. In the user space, Splicer retrieves CSI from the kernel and stores them into L buffers according to their channel. Received CSIs are divided into phase and amplitude. Splicer corrects the errors in both amplitude and phase and splicing them together to derive high-resolution power delay profile. Since CSI is widely used for localization and RF sensing in many mobile systems and applications, we have released the source codes for extracting CSI from Atheros Wi-Fi NICs as Athero-CSI-Tool [31] to facilitate the research in this area. The source codes (OpenWRT and Ubuntu version) are available on Github [32].

CSI collection. To ensure that the CSI is calculated for every packet, Splicer disables the 802.11 frame aggregation when collecting CSI, to make sure that every packet has a PHY layer preamble for CSI calculation. Splicer also adopts the minimum payload size for each frame to guarantee minimum air time of a single packet to collect CSIs.

Channel switching. To enable rapid channel switching, devices works in monitor mode (without the association). Transmitter first transmits packets in the default channel, and the receiver keeps listening and collects the CSIs. When enough CSIs are collected, the receiver launches the switching to the next channel, by sending an ACK frame to inform the transmitter. After receiving the ACK, transmitter switches the channel accordingly and starts transmitting at the new channel. As there is no association process, the switching latency is mainly determined by the delay between receiving last packet and transmitting the short ACK, which is only around $10\mu s$ to $20\mu s$.

5 Evaluation

In this section, we conduct testbed-based experiments to evaluate the performance of Splicer. We introduce our experimental setting in §5.1, evaluate the efficacy of Splicer in §5.2, and report the end-to-end system performance of Splicer-enhanced CUPID in §5.3, which is one of the state-of-the-art indoor localization designs [6].

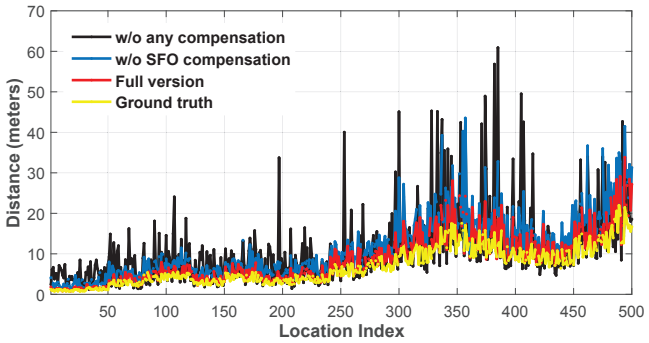


Fig. 16: Ranging results at 500 different locations by different versions of Splicer in a single WiFi band.

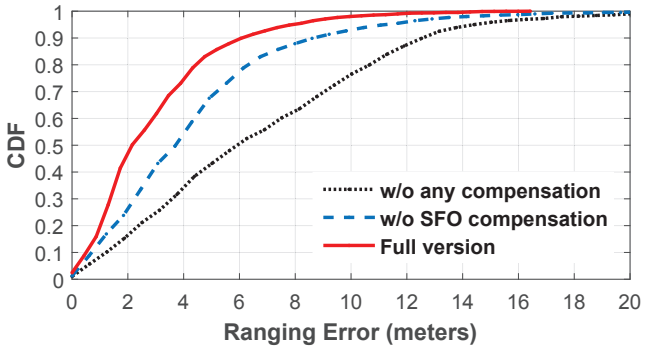


Fig. 17: CDF of ranging errors using CSI of a single band but with different levels of phase error corrected.

5.1 Experimental setup

We conduct experiments in a laboratory, with natural dynamics introduced by 10 occupants. We install five APs at five known locations. Each AP is a Wi-Fi router (TP-Link WDR4300), which is equipped with Atheros 9580 NIC. The five APs are configured in monitor mode as receivers. We select 500 different locations in the laboratory and place another AP, which is set to the RootAP mode as sender, at each of these locations sequentially. At each location, the AP sender conducts multiple rounds of CSI splicing with the five AP receivers. Specifically, for each round of CSI splicing, the sender transmits packets in multiple channels and five receiver receives the packets simultaneously. The received CSIs are spliced at each receiver. The spliced CSIs are sent to a server for further processing, *e.g.* ranging or localization.

To examine the accuracy of the power delay profiles derived by Splicer, we first evaluate the accuracy of the power level measured from the Line-of-Sight (LoS) path. To this end, we measure the distance between the sender and each of the receivers at all 500 different locations as the ground truth. At each location, we compare the derived distance from the power delay profile with the ground truth for evaluation. In addition to the LoS path, we also evaluate the quality of the derived power delay profiles using the power level stability for Non-Line-of-Sight (NLoS) paths.

We first provides a detailed performance analysis of Splicer in §5.2, we disable the sampling scheduler (described in §3.5), and manually control the number of scanned channels. From each channel, we collect 30 CSI traces. After that, in §5.3, we enable the sampling scheduler and evaluate the end-to-end performance with the full-version Splicer in a localization application.

5.2 Results

Phase error correction. To investigate the effectiveness of the CSI error correction designs in Splicer, we first evaluate the ranging performance to estimate the LoS path length d in each single 20MHz WiFi band without using CSI splicing. We evaluate Splicer for three different versions to investigate where the performance gains Splicer achieves come from: the full version with both λ_b and λ_o compensations, as well as two degraded versions — without λ_b compensation and without any phase error compensation. We compare the three versions against the measured ground truth to one randomly selected receiver of one AP in Fig. 16. In the figure, the x-axis presents different locations and the y-axis illustrates the ranging results of each Splicer version (as well as the ground truth). Each reported accuracy value is the average from 10 measurements. From the result, we observe that without any phase error correction, the ranging performance is highly unreliable. After the phase error λ_b removal, the ranging accuracy Splicer achieves has been dramatically improved, but it is still far away from the ground truth. After the compensations of λ_b and λ_o, we find that the accuracy is very close to the true distance value between the sender and the receiver at different locations. Similar results are observed for other four APs.

In Fig. 17, we provide detailed statistical results for the performance achieved by different Splicer versions of five APs. From the result, we see that when the raw CSI phases are used, the ranging error is $10.7m$ for 80% of the measurements. The median and the maximum errors are $6.1m$ and $24m$, respectively, compared with the ground truth. After the compensation of phase error λ_b, the ranging error is reduced to $6.3m$ for 80% measurements. After the removal of both λ_b and λ_o, the ranging error is less than $4.3m$ for 80% of cases. The improvement is as high as $4.8m$ on average compared with the traditional ranging performance using the raw phase information.

CSI splicing. In Fig. 18, we evaluate the ranging performance of Splicer With CSI splicing enabled. As the power delay profile resolution is determined by the channel bandwidth, we select two representative bandwidths after splicing, 200MHz that is the total bandwidth allocated to 802.11n and 120MHz that is in between the entire WiFi band and each single WiFi band. We select all spliced CSIs with these two selected bandwidths to report the performance. As a benchmark, we also include the performance of the full version Splicer in 20MHz for comparison. We also compare the ranging performance with CSI without conducting the phase refinement (§3.3) to understand its performance gain.

Fig. 18 plots CDF of the ranging errors from those three approaches. From the result, we find that the performance of Splicer using merely a single WiFi band is still limited, even with the CSI error correction. In general, the wider the bandwidth Splicer uses, the smaller error the ranging can achieve. The performance gain stems from more accurate power level measurement of the LoS path. According to the statistics, on average Splicer-120MHz and Splicer-200MHz

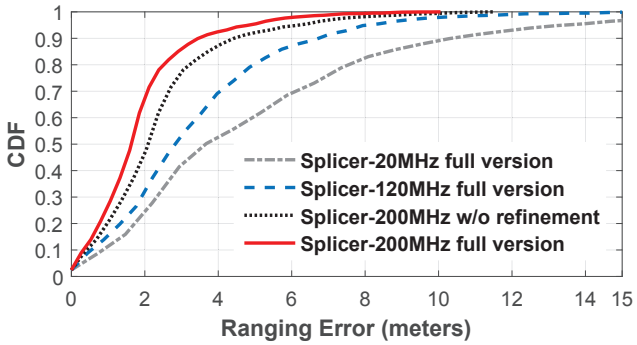


Fig. 18: CDF of ranging errors with CSI splicing. The error reduces when using wider band.

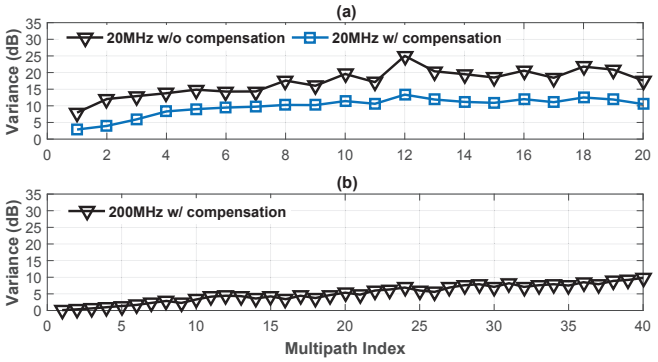


Fig. 19: Measured power level variance for NLoS path components in the derived power delay profiles. (a) In 20MHz WiFi band; (b) In 200MHz WiFi band.

can outperform Splicer-20MHz by 22.7% and 55.5%, respectively. The performance gain of Splicer stems from both the CSI splicing as well as the CSI phase refinement (§3.3). In Fig. 18, we also show the performance gain the phase refinement provides. From the result, we see that the CSI phase refinement can reduce ranging error by about $0.42m$. On the other hand, Fig. 18 also implies that Splicer with 802.11n can achieve comparable performance as the new protocol 802.11ac, as they both cover up to 200MHz bandwidth.

Non-line-of-sight paths. In Fig.s 16 to 18, we have evaluated estimation accuracy of the LoS path power in the derived power delay profiles. In this experiment, we investigate the quality of the derived power delay profiles for all other NLoS paths. In practice, the absolute power level of a NLoS path is not directly useful in applications. Instead, the relative change of the power level of each NLoS path indicates the multipath channel dynamics, which has been used for activity or gesture recognitions [2, 18]. To this end, we randomly select 10 locations in the laboratory. At each location, the transmission pair performs multiple rounds of CSI splicing. We evaluate the stability of the measured power levels for all the NLoS paths in Fig. 19.

Fig. 19 (a) shows the NLoS path power level stability using a single 20MHz WiFi channel. However, we observe that without the phase error compensation, the power variance is high, *e.g.*, around 16 dB, even the pair of transmitters are static at their locations. Our CSI error compensation designs can reduce the variance to be less than 10 dB on average for single WiFi bands. In Fig. 19 (b), due to the CSI splicing, we can derive higher-resolution power delay profiles. Hence, the measured power level for each multipath component is aggregated from fewer non-distinguishable multipaths (§2), which should suffer from even less uncertainty. The result in Fig. 19 (b) is consistent to our analysis, which shows that the power level variance for NLos paths in the derived power delay profiles using 200MHz spliced bandwidth is less than 5.2dB in our experiment.

5.3 Case study: indoor localization

In §5.2, we have evaluated the accuracy of the derived power delay profiles. With high resolution power delay profiles, the performance of a plethora of upper-layer applications, *e.g.*, localization, object tracking, gesture recognition, etc., can be significantly improved. We take localization as a vehicle to demonstrate this capability of Splicer.

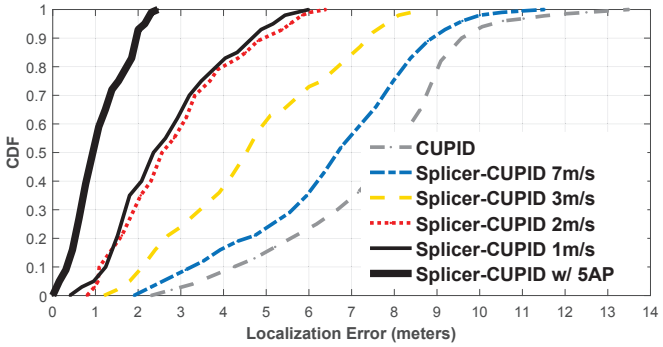


Fig. 20: CDF of localization errors using the original CUPID and the enhanced CUPID by Splicer.

5.3.1 Case study overview

We integrate Splicer into the recent single-AP location approach CUPID [6]. In CUPID, a mobile device can locate its location as follows. The device transmits a packet to an AP with known location. The AP extracts the CSI upon receiving this packet and derives the power delay profile. According to the power level of the LoS path, the AP can estimate this path length. On the other hand, the AP further apply the MUSIC algorithm on the CSI to compute its pseudo spectrum, which can approximate the signal arrival direction from the LoS path. According to the path length and the signal arrival direction, the AP can locate the mobile user and send the localization result back to the user.

To enhance CUPID, we replace the spliced wideband CSI as the system input and keep the rest of the CUPID design unchanged. To evaluate the performance, we install one AP in the laboratory with known location and deploy one AP on a robot. The robot is programmed to move along a predefined trajectory with a known speed. Based on the timestamps of each packet reported by NIC, we can calculate and log the instant location of the robot when the mobile AP transmits this packet. To evaluate the end-to-end performance, we enable the sampling scheduler in Splicer.

5.3.2 Results

Localization accuracy. In Fig. 20 (a), we compare the performance of the original CUPID and the enhanced CUPID by Splicer, denoted as Splicer-CUPID. We vary the moving speeds of the robot in the experiment. Since the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2860991, IEEE Transactions on Mobile Computing

localization in the original CUPID depends on a single CSI measurement, the localization performance of CUPID is not impacted by the moving speed of the robot. For Splicer-CUPID, a higher moving speed leads to a shorter channel coherence time. As a consequence, fewer WiFi bands can be included in each round of CSI splicing and the localization accuracy will decrease. From Fig. 20, we find that in general, the localization accuracy of CUPID is not quite accurate, *e.g.*, around $8m$ for 80% of localizations, which is consistent to the performance reported in [6]. For Splicer-CUPID, with a normal moving speed of a person ($< 2m/s$), the accuracy can be dramatically improved, *e.g.*, the median localization error is $2.3m$ and $2.5m$ when the speed is $1m/s$ and $2m/s$, respectively. The localization error is less than $6.4m$ throughout the experiment. With a higher moving speed, *e.g.*, $7m/s$, Splicer-CUPID still outperforms CUPID.

In [6], the authors propose an AP selection scheme to further improve the localization accuracy by harnessing a dense AP deployment. According to the experiment results in [6], the localization accuracy of Splicer-CUPID using a single AP achieves comparable performance to CUPID with 5 APs, which can significantly improve the usefulness of indoor localizations. In Fig. 20, we also leverage such an improvement opportunity. The result shows that the gain from Splicer-CUPID is significant. Localization errors are reduced to $1.75m$ for 80% cases and the median error is $0.95m$ when 5 APs are used. Although more APs may improve the localization performance, if the ranging accuracy is not high at the first place, improvement with more APs is limited.

Impact of moving speeds. In Fig. 21 (left y-axis), we investigate the total bandwidth that can be spliced with respect to different moving speeds of transmitters. In general, a higher speed leads to a shorter channel coherence time. As a result, CSI traces are spliced from fewer WiFi channels and the power delay profile resolution is lower. From Fig. 21, we see that Splicer can make full use of the 200MHz available WiFi frequency band, when the speed is smaller than $2m/s$. The small localization errors observed in this case in Fig. 20 is compatible with such an observation. When we accelerate the moving speed from $3m/s$ to $6m/s$, the utilized bandwidth drops from 130MHz to 60MHz, which, however, is still wider than a single WiFi channel, *i.e.* 20MHz or 40MHz. Further more, the bandwidth will drop to 45.5MHz when the speed increases to $7m/s$, which is comparable to one single 40MHz channel. Nevertheless, Splicer-CUPID still improve the localization performance since Splicer compensates the CSI measurement errors.

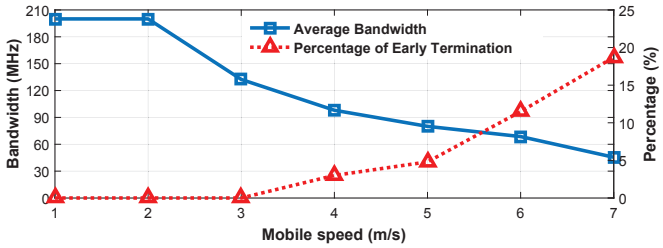


Fig. 21: Bandwidth used for localization under different speeds. (Left) Spliced bandwidth; (right) Early termination percentage.

We further examine the percentages of early terminations (§3.5) occurred in our experiment, in Fig. 21 (right y-axis). From the result, we see that the early termination strategy can discover 4.8% to 18.7% rapid channel varying within the channel coherence time budget.

6 Related Work

Channel sounding. Measuring the wideband channel frequency response requires high-end hardware with high sampling frequencies [33, 34]. The authors in [35, 36] develop systems to measure channel frequency responses from a group of narrow bands to approximate a wideband channel. In [37], the receiver only listens to a few harmonics of a wideband signal each time and then can reconstruct the wideband frequency response. Such a design does not require the modification at the sender. In addition, CSI-SF proposed in [38] can estimate the channel state information for multi-streams using the single stream measurement result. Some ToA-based localization approaches [19, 39] also propose to increase the resolution using the channel combination, which, however, only works with Software-Defined-Radio. Although Splicer shares a similar principle with those existing works, most of them require tight synchronization between the sender and receiver, *e.g.* devices are connected by the same clock or use GPS and atomic clocks. In this work, however, we meet and address particular challenges due to the hardware imperfection and stringent channel coherence delay constraint, which do not exist in any of existing works. In addition, Splicer can be integrated into commodity NICs without any hardware modification.

CSI phase calibration. Prior works also notice that the CSI traces reported by WiFi NICs contain phase errors introduced by hardware [40, 41]. ArrayPhaser [42] enables the phased array signal processing on commodity WiFi devices. However, ArrayPhaser does not correct any of those phase errors, instead they just treat the phase values measured from one NIC as the reference to calibrate the phase values of other NICs. Hence, they cannot truthfully remove the phase values to derive precise power delay profiles. Prior works [6, 43] try to synchronize the phases from two consecutive received CSIs via a linear transform. After the transformation, if the two measurements are from the same multipath channel, even the collected CSIs are different due to hardware noises, the transformation on these two CSIs leads to the same result, which could be used as fingerprint for localization. Some recent works aim to explicitly correct CSI phase errors, *e.g.*, MegaMIMO [44]. However, MegaMIMO requires both nanosecond-level synchronization and the access to the raw signal at PHY layer, which are not available on commodity NICs. In summary, existing works cannot directly remove measurement errors from CSIs reported by commodity WiFi NICs, and hence cannot address the challenges we met in Splicer.

Power delay profile based applications. At different locations, the received power delay profiles will be different, which can makes them a good choice for the fingerprint-based localization design [45, 46]. On the other hand, the Line-of-Sight information can be directly inferred from the power delay profile [43]. The power level of the LoS path can also be used to ranging between a pair of transmitters [1, 6]. Indoor localization based on the ranging results requires no dense AP deployments, no manual fingerprinting

site survey, and no sophisticated AP hardware [1, 6, 9, 47, 48]. In these applications, super-resolution algorithms can also be used to further improve localization or ranging accuracy. However, as the super-resolution algorithms do not provide the power information [19, 39], they cannot benefit the quality of power delay profile itself, which essentially dominated by the received signal bandwidth. For activity recognition, although the detailed relation between the multipath channel variance and the different activities is unknown, recent works propose to learn the inner relation. For example, to detect the existence of human beings [5], to count the number of people moving around [4], to detect human falling down in [3] and recognize different human activities [2, 49, 50, 51]. Splicer can benefit these applications as we can obtain a wider CSI containing more frequency band information to derive a higher-resolution power delay profile, which more precisely describes multipath channels.

7 Conclusion

This paper presents Splicer to derive precise power delay profiles on commodity WiFi devices. The Splicer design leverages the CSIs measured from multiple WiFi bands and splicing them to obtain a CSI of an equivalent wider WiFi band. We propose a set of key techniques to correct CSI error introduced by the hardware of Wi-Fi transceiver and derive accurate, high resolution power delay profile. Experiments show that our enhanced power delay profile can improve the performance of indoor localization significantly. A preliminary version of this work has been presented in [10].

Acknowledgement

This work is supported by Singapore MOE Tier 1 grant RG125/17, Tier 2 grant MOE2016-T2-2-023, and NTU CoE grant M4081879.. This work is also partially supported by the ECS grant from Research Grants Council of Hong Kong (Project No. CityU 21203516), and the GRF grant from Research Grants Council of Hong Kong (Project No. CityU 11217817).

References

[1] K. Wu, J. Xiao, Y. Yi, M. Gao, and L. Ni, "FILA: Fine-grained indoor localization," in *Proc. of IEEE INFOCOM*, 2012.

[2] Y. Wang, J. Liu, Y. Chen, M. Gruteser, J. Yang, and H. Liu, "E-eyes: Device-free location-oriented activity identification using fine-grained WiFi signatures," in *Proc. of ACM MobiCom*, 2014.

[3] C. Han, K. Wu, Y. Wang, and L. Ni, "WiFall: Device-free fall detection by wireless networks," in *Proc. of IEEE INFOCOM*, 2014.

[4] W. Xi, J. Zhao, X.-Y. Li, K. Zhao, S. Tang, X. Liu, and Z. Jiang, "Electronic frog eye: Counting crowd using WiFi," in *Proc. of IEEE INFOCOM*, 2014.

[5] Z. Zhou, Z. Yang, C. Wu, L. Shangguan, and Y. Liu, "Omnidirectional coverage for device-free passive human detection," *IEEE Transactions on Parallel and Distributed Systems*, 2014.

[6] S. Sen, J. Lee, K.-H. Kim, and P. Congdon, "Avoiding multipath to revive inbuilding WiFi localization," in *Proc. of ACM MobiSys*, 2013.

[7] S. Sen, R. R. Choudhury, and S. Nelakuditi, "Spinloc: Spin once to know your location," in *Proc. of ACM HotMobile*, 2012.

[8] H. Liu, Y. Gan, J. Yang, S. Sidhom, Y. Wang, Y. Chen, and F. Ye, "Push the limit of wifi based localization for smartphones," in *Proc. of ACM MobiCom*, 2012.

[9] D. Vasisht, S. Kumar, and D. Katabi, "Decimeter-level localization with a single wifi access point," in *Proc. of Usenix NSDI*, 2016.

[10] Y. Xie, Z. Li, and M. Li, "Precise power delay profiling with commodity wifi," in *Proc. of MobiCom*, 2015.

[11] J. Han, C. Qian, X. Wang, D. Ma, J. Zhao, W. Xi, Z. Jiang, and Z. Wang, "Twins: Device-free object tracking using passive tags," *IEEE/ACM Transactions on Networking*, 2016.

[12] L. Wang, Y. He, Y. Liu, W. Liu, J. Wang, and N. Jing, "It is not just a matter of time: oscillation-free emergency navigation with sensor networks," in *Proc. of IEEE RTSS*, 2012.

[13] J. Parsons, D. Demery, and A. Turkmani, "Sounding techniques for wideband mobile radio channels: a review," *Communications, Speech and Vision, IEE Proceedings I*, 1991.

[14] T. S. Rappaport *et al.*, *Wireless communications: principles and practice*. prentice hall PTR New Jersey, 1996.

[15] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.

[16] "IEEE Standard for Information Technology—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications," Mar. 2012.

[17] L. Zhang, K. Liu, Y. Jiang, X.-Y. Li, Y. Liu, P. Yang, and Z. Li, "Montage: Combine frames with movement continuity for realtime multi-user tracking," *IEEE Transactions on Mobile Computing*, 2017.

[18] G. Wang, Y. Zou, Z. Zhou, K. Wu, and L. M. Ni, "We can hear you with Wi-Fi!" in *Proc. of ACM MobiCom*, 2014.

[19] J. Xiong, K. Sundaresan, and K. Jamieson, "Tonetrack: Overcoming bandwidth constraints for indoor wireless localization," in *Proc. of ACM MobiCom*, 2015.

[20] M. Speth, S. Fechtel, G. Fock, and H. Meyr, "Optimum receiver design for wireless broad-band systems using OFDM. i," *IEEE Transactions on Communications*, 1999.

[21] J. K. Tan, "An adaptive orthogonal frequency division multiplexing baseband modem for wideband wireless channels," Master's thesis, Massachusetts Institute of Technology, 2006.

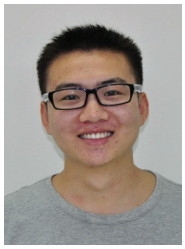
[22] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," in *Proc. of ACM MobiCom*, 2008.

[23] B. Razavi, "Design considerations for direct-conversion receivers," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, 1997.

[24] X. Li and K. Pahlavan, "Super-resolution toa estimation with diversity for indoor geolocation," *IEEE Transactions on Wireless Communications*, 2004.

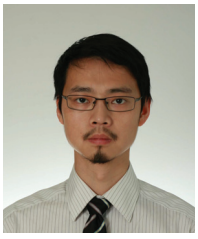
[25] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Predictable 802.11 packet delivery from wireless channel

measurements," in *Proc. of ACM SIGCOMM*, 2010.
[26] V. Jimenez, M. Fernandez-Getino Garcia, F. Serrano, and A. Armada, "Design and implementation of synchronization and agc for ofdm-based wlan receivers," *IEEE Transactions on Consumer Electronics*, 2004.
[27] X. Ji, Y. He, J. Wang, K. Wu, D. Liu, K. Yi, and Y. Liu, "On improving wireless channel utilization: A collision tolerance-based approach," *IEEE Transactions on Mobile Computing*, 2017.
[28] M. Khalid, Y. Wang, I. Butun, H.-j. Kim, I.-h. Ra, and R. Sankar, "Coherence time-based cooperative mac protocol 1 for wireless ad hoc networks," in *EURASIP Journal on Wireless Communications and Networking*, 2011.
[29] A. Azzalini, "A class of distributions which includes the normal ones," *Scandinavian journal of statistics*, 1985.
[30] P. M. Bentler and D. G. Bonett, "Significance tests and goodness of fit in the analysis of covariance structures." *Psychological bulletin*, 1980.
[31] Tool for extraction CSI on Atheros Wi-Fi NIC, url = http://wands.sg/AtherosCSI/.
[32] Github of Atheros CSI extraction tool., url = https://github.com/xieyaxiongfly/Atheros-CSI-Tool.
[33] T. Felhauer, P. Baier, W. Konig, and W. Mohr, "Optimum spread spectrum signals for wideband channel sounding," *Electronics Letters*, 1993.
[34] A. Molina, P. Fannin, and J. Timoney, "Generation of optimum excitation waveforms for mobile radio channel sounding," *IEEE Transactions on Vehicular Technology*, 1995.
[35] D. Molkdar and P. Matthews, "Measurements and characterization of the UHF mobile radio channel. part 1: Measurements over the band 853-885 MHz," *Electronic and Radio Engineers, Journal of the Institution of*, 1988.
[36] K. Pahlavan and A. H. Levesque, *Wireless information networks*. John Wiley & Sons, 2005.
[37] B. Kempke, P. Pannuto, and P. Dutta, "Harmonia: Wideband spreading for accurate indoor rf localization," in *Proc. of ACM HotWireless*, 2014.
[38] R. Crepaldi, J. Lee, R. Etkin, S.-J. Lee, and R. Kravets, "CSI-SF: Estimating wireless channel state using CSI sampling and fusion," in *Proc. of IEEE INFOCOM*, 2012.
[39] J. Xiong, K. Jamieson, and K. Sundaresan, "Synchronicity: Pushing the envelope of fine-grained localization with distributed mimo," in *Proc. of ACM HotWireless*, 2014.
[40] J. Xiong and K. Jamieson, "Arraytrack: A fine-grained indoor location system," in *Proc. of USENIX NSDI*, 2013.
[41] L. Yang, Y. Chen, X.-Y. Li, C. Xiao, M. Li, and Y. Liu, "Tagoram: Real-time tracking of mobile rfid tags to high precision using cots devices," in *Proc. of ACM MobiCom*, 2014.
[42] J. Gjengset, G. McPhillips, and K. Jamieson, "Arrayphaser: Enabling signal processing on WiFi access points," *Proc. of ACM MobiCom*, 2014.
[43] C. Wu, Z. Yang, Z. Zhou, K. Qian, Y. Liu, and M. Liu, "Phaseu: Real-time LOS identification with wifi," in *Proc. of IEEE INFOCOM*, 2014.
[44] H. S. Rahul, S. Kumar, and D. Katabi, "Jmb: Scaling wireless capacity with user demands," in *Proc. of ACM SIGCOMM*, 2014.
[45] J. Xiao, K. Wu, Y. Yi, and L. Ni, "FIFS: Fine-grained indoor fingerprinting system," in *Proc. of IEEE ICCCN*, 2012.
[46] S. Sen, B. Radunovic, R. R. Choudhury, and T. Minka, "You are facing the mona lisa: Spot localization using PHY layer information," in *Proc. of ACM MobiSys*, 2012.
[47] M. Kotaru, K. Joshi, D. Bharadia, and S. Katti, "Spotfi: Decimeter level localization using wifi," in *Proc. of ACM SIGCOMM*, 2015.
[48] J. Wang, H. Jiang, J. Xiong, K. Jamieson, X. Chen, D. Fang, and B. Xie, "Lifs: Low human-effort, device-free localization with fine-grained subcarrier information," in *Proc. of ACM MobiCom*, 2016.
[49] L. Shangguan, Z. Yang, A. X. Liu, Z. Zhou, and Y. Liu, "Relative localization of rfid tags using spatial-temporal phase profiling," in *Proc. of USENIX NSDI*, 2015.
[50] F. Adib, Z. Kabelac, D. Katabi, and R. C. Miller, "3d tracking via body radio reflections," in *Proc. of USENIX NSDI*, 2014.
[51] X. Zheng, J. Wang, L. Shangguan, Z. Zhou, and Y. Liu, "Design and implementation of a csi-based ubiquitous smoking detection system," *IEEE/ACM Transactions on Networking*, 2017.



Yaxiong Xie received the B.E. degree in automation from University of Science and Technology of China, Hefei, China, in 2012 and the Ph.D. degree in computer science and engineering from Nanyang Technological Unviersity, Singapore, in 2017. He is currently an Postdoc Research Fellow in School of Computer Science and Engineering, Nanyang Technological Unviersity, Singapore. His research interests include wireless systems, internet of things, cyber physical system and mobile computing.

Zhenjiang Li received the B.E. degree in computer science and technology from Xi'an Jiaotong University, Xi'an, China, in 2007 and the M.Phil. degree in electronic and computer engineering and the Ph.D. degree in computer science and engineering from The Hong Kong University of Science and Technology, Hong Kong, in 2009 and 2012, respectively. He is currently an Assistant Professor of the computer science department at City University of Hong Kong, Hong Kong. His research interests include wearable and mobile sensing, deep learning and distributed computing.



Mo Li received the B.S. degree in computer science and technology from Tsinghua University, Beijing, China, in 2004 and the Ph.D. degree in computer science and engineering from The Hong Kong University of Science and Technology, Hong Kong, in 2009. He is currently an Associate Professor with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research interests include networked and distributed sensing, wireless and mobile, cyber-physical systems, smart city, and urban computing.