IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 20 May 2023, accepted 8 June 2023, date of publication 20 June 2023, date of current version 14 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3287850

RESEARCH ARTICLE

Bridging the Performance Gap Between Two-Way and One-Way CSI-Based 5 GHz WiFi Ranging

SHERIEF HELWA[1], (Student Member, IEEE),
JAYSON P. VAN MARTER[1], (Student Member, IEEE),
SHAMMAN NOOR SHOUDHA[1], (Student Member, IEEE), MATAN BEN-SHACHAR[2],
YARON ALPERT[2], ANAND G. DABAK[2], (Fellow, IEEE),
MURAT TORLAK[1], (Senior Member, IEEE), AND NAOFAL AL-DHAHIR[1], (Fellow, IEEE)
[1]Department of Electrical and Computer Engineering, The University of Texas at Dallas, Richardson, TX 75080, USA
[2]Texas Instruments Inc., Dallas, TX 75243, USA

Corresponding author: Sherief Helwa (sherief.helwa@utdallas.edu)

This work was supported by Semiconductor Research Corporation under Grant 2810.076.

ABSTRACT Indoor Localization is gaining increased importance due to numerous location-based services in healthcare, logistics, and security, to name few, that are expected to be provided by next-generation wireless networks. Such services are characterized by stringent accuracy requirements, short response time, and lower cost which makes the localization problem more challenging and deserving of attention. A key element of the localization process is distance estimation (also known as ranging). In this paper, we design and analyze an efficient decimeter-level two-way ranging scheme for ubiquitous WiFi networks in the 5 GHz frequency band whose accuracy approaches ideal one-way ranging with no phase mismatches. We investigate the idea of channel frequency response (CFR) stitching across non-contiguous WiFi channels and how two-way CFR measurements help in achieving the CFR coherency necessary for accurate ranging. In addition, we quantify the decrease in ranging accuracy of two-way compared to one-way ranging due to SNR degradation, Line-of-Sight (LoS) component shrinkage, and doubling the multipath delay spread. Furthermore, We design a novel scheme to bridge the performance gap between two-way ranging and ideal one-way ranging which operates in three main steps: square-root of the two-way CFR, followed by phase unwrapping, and finally deep fade detection and phase errors correction. Our proposed scheme achieves significant performance gains over two-way ranging with only a slight performance gap from ideal one-way ranging. Moreover, our proposed scheme enjoys robustness as it preserves the ranging accuracy gains in various WiFi communication scenarios when operating at different SNR levels, different multipath channel models, and different CFR bandwidths, as well as operating under system impairments such as Sample Timing Offset (STO). The accuracy gains achieved by the proposed schemes are demonstrated using both simulations and an in-house WiFi testbed. Finally, we quantify the added complexity of our proposed scheme and show it to be insignificant compared to that of the MUSIC super-resolution ranging steps which confirms the practical viability of our proposed scheme.

INDEX TERMS Localization, WiFi, one-way ranging, two-way ranging, CFR Stitching, MUSIC super-resolution, PLL phase mismatches, sampling time offset.

I. INTRODUCTION

Channel State Information (CSI)-based WiFi ranging has received increased interest recently thanks to its performance gains over received signal strength information (RSSI)-based and time-stamp-based ranging, especially in multipath environments [1], [2], [3]. However, CSI-based ranging has its own challenges and limitations. One important factor that limits ranging accuracy is the CSI bandwidth [4], [5]. It is

The associate editor coordinating the review of this manuscript and approving it for publication was Li Zhang.

well known that wider bandwidth of the estimated CSI results in higher ranging accuracy since it facilitates resolving the channel's multipath components. Due to the scarce and typically discontiguous nature of the available radio frequency (RF) WiFi spectrum, bandwidth limitation has always been a key challenge for CSI-based WiFi ranging [6], [7]. Aside from spectrum limitations, wide bandwidth operation is also often not supported by many WiFi devices.

CSI stitching is a promising idea to address this bandwidth limitation where WiFi CSI is acquired over multiple WiFi channels, and for each channel, the Channel Frequency Response (CFR) is estimated across a new set of frequencies. Then, the individual CFR estimates are stitched together to form a unified CFR estimate of a much wider bandwidth than what can be supported in one WiFi transmission. Nonetheless, CSI stitching presents several challenges, the most important of which is the Transmitter (Tx) and Receiver's (Rx) phase-locked loop (PLL) phase mismatches [8], [9].

The issue with mismatched PLL phases at the Tx and Rx is not the mismatch itself as it only causes an overall constant phase across the bandwidth of the CFR. Instead, the problem arises from the changing phases of these PLLs while switching to a different carrier frequency to collect CFR estimates at a different set of frequencies (WiFi channel). This problem will cause sudden phase jumps between individual CFR estimates which will hinder the stitching process due to the lack of phase coherence. This issue was initially mitigated in the literature by using the two-way channel measurement approach which, at that time, used to work only with carrier phases; see e.g. [9]. In later works, it was extended to the whole CFR including magnitude response as well [10].

Sub-Sample Timing Offset (STO) is another serious issue that can degrade the ranging accuracy. This problem is caused by the lack of sub-sample-level time synchronization between two communicating devices. Although the receiver usually performs some packet-level synchronization using packet detection algorithms, a residual STO can still remain. This non-zero STO causes an error signal in the estimated CFR phase, hence, degrading the ranging accuracy. The significance of STO was highlighted in [11] and [12]. Another great advantage of two-way channel measurements is that they eliminate the STO problem [13].

The idea of two-way channel measurements is to estimate the CFR at each of the two communicating wireless nodes. Then, the two CFR estimates are multiplied together leading to the cancellation of any mismatched phase components. This idea is based on the fact that PLL phase mismatches as well as STO effects reciprocate when measured at the two devices of interest. The two-way channel measurement approach will be discussed in detail in Section III to highlight its pros and cons relative to one-way operation.

Unfortunately, multiplying the two CFR estimates (which essentially squares the CFR estimate due to channel reciprocity), doubles the multipath delay spread and degrades ranging accuracy. To mitigate this ranging accuracy degradation from two-way operation, we propose a novel square-root-based algorithm to transform two-way CSI measurements to one-way CSI. The main challenge in this transformation is the positive/negative sign ambiguity due to square-root operation. This causes extra π phase transitions that ruin the estimated CSI quality and degrade the ranging accuracy.With the aid of a special type of PLL that stays locked to the same phase as carrier frequency changes, the authors of [10] proposed a phase processing technique to mitigate this sign ambiguity problem. They make the strong assumption that by using those special PLLs, phase mismatches from one frequency band to the next one can be calculated and compensated for. In this paper, we do not assume any special type of PLL and therefore, we propose a phase transition detection and correction algorithm that mitigates the positive/negative sign ambiguities. Additionally, we propose an enhancement to our phase transition detection and correction algorithm that offers additional performance gain by dealing with the highly challenging cases of deep fading channels. Hence, our proposed schemes are distinct from state of the art techniques in the literature that either stick with two-way operation or assume special type PLLs to mitigate its issues. The main contributions of this paper are summarized as follows:

- We provide a detailed analysis of the two-way channel approach drawbacks including SNR degradation and its negative impact on the line-of-sight (LoS) to non-LoS components power ratio.
- We propose a novel square-root-based scheme for two-way to one-way CFR transformation that can bridge the ranging performance gap between the two approaches.
- We enhance our two-way to one-way CFR transformation scheme by proposing a novel phase correction algorithm capable of detecting phase errors resulting from deep wireless channel fades.
- We analyze the complexity of our proposed scheme and show the insignificance of its added complexity relative to the MUSIC ranging algorithm complexity.
- We quantify the significant performance gains achieved by our proposed approach using an accurate WiFi system simulator that incorporates various realistic wireless channel models adopted by WiFi standards.
- We develop a Universal Software Radio Peripheral (USRP) based WiFi testbed and use it to demonstrate the performance gains of our proposed scheme.

The rest of this paper is organized as follows. We start in Section II by describing the ranging system model including its two main steps: channel estimation and distance estimation using estimated CSI. This is followed by analyzing the pros and cons of one-way versus two-way CSI approaches in Section III. Section IV describes our proposed schemes for two-way to one-way CSI transformation, while Section V provides a detailed complexity analysis of those schemes. In Section VI, we present an overall system performance evaluation of our proposed schemes compared to benchmark schemes using both computer simulations and a USRP-based WiFi testbed. Finally, the paper is concluded in Section VII.

The key variables and acronyms frequently used in this paper are summarized in Tables 1 and 2, respectively.

TABLE 1. List of key variables used in the paper.

Variable	Notation	Description
Ideal one-way CFR	H	Assumed to have perfect phase coherency
Ideal two-way CFR	$\tilde{H}$	Achieves phase coherency through AP and STA one-way CFR multiplication
Est. two-way CFR	$\hat{\tilde{H}}$	An estimate of the two-way CFR
Sqrt of 2-way CFR	H_{sqrt}	Square-root of the 2-way CFR estimate
One-way CFR Est.	$\hat{H}$	Estimate of one-way CFR achieved by unwrapping the phase of H_{sqrt}
Enhanced one-way CFR Est.	$\hat{\hat{H}}$	A better estimate achieved by treating phase errors in $\hat{H}$
One-way CFR Est. at Node A	$\hat{H}_A$	The phase incoherent one-way estimate achieved at node A
One-way CFR Est. at Node B	$\hat{H}_B$	The phase incoherent one-way estimate achieved at node B

TABLE 2. List of key acronyms frequently used in the paper.

Acronym	Full Form
CSI	Channel State Information
CFR	Channel Frequency Response
CIR	Channel Impulse Response
PLL	Phase Locked Loop
AP	Access Point
STA	STAtion
LoS	Line-of-Sight
ToF	Time-of-Flight
PPDU	Physical Packet Data Unit
WiFi HE	WiFi High Efficiency
MUSIC	MUltiple SIgnal Classification
EVD	EigenValue Decomposition
LTF	Long Training Field
FLOP	FLoating-point OPeration
FIR	Finite Impulse Response

II. SYSTEM MODEL AND RANGING TECHNIQUES

The ranging method we consider in this paper is CSI-based where the Tx-Rx separation distance is inferred from CSI information. For single-path LoS transmission, the distance travelled by the transmitted signal introduces propagation delay which is reflected in the channel phase response as a linear phase increase. For a multi-path propagation environment, the channel response is composed of multiple delayed taps with different magnitudes. Therefore, the Channel Impulse Response (CIR) of a multipath channel is given by

$$h(t) = \sum_{l=0}^{L-1} \alpha_l \delta(t - \tau_l), \tag{1}$$

where l is the channel tap index, α_l represents channel tap amplitude and is generally complex ($\alpha_l \in \mathbb{C}$), while τ_l is the channel tap delay. For a multipath channel, the CSI-based ranging method's objective is to calculate the Time of Flight (ToF) by estimating τ_0 which is used to calculate the distance.

In this paper, we consider an 802.11ax WiFi system, also known as High Efficiency (HE) WiFi (or WiFi 6) which sends a preamble sequence at the beginning of each data packet. The preamble fields including training sequences known at the Rx are used to enable data detection. The Physical Packet Data Unit (PPDU) preamble is split into two parts. The first is the legacy preamble part, which is added for backward compatibility and is used for time and frequency synchronization. The second part is the HE preamble, which is added for channel estimation and to share signaling information essential for data decoding.

For ranging purposes, we only rely on the HE-Long Training Field (HE-LTF) which is used for channel estimation since our ranging method is CSI-based. The frequency-domain signal model of the received preamble is given by

$$Y_A[k] = X_p[k]H[k] + V_A[k], \tag{2}$$

where $X_p \in \{+1, -1\}$ is the pilot sequence constituting the HE-LTF, $H \in \mathbb{C}$ is the Channel Frequency Response (CFR), $V \in \mathbb{C}$ is additive white Gaussian noise (AWGN), and the index $k = \{0, 1, \ldots, N-1\}$ represents the frequency bin index. The channel coefficients in H have a Rayleigh fading magnitude since $H \sim \mathcal{CN}(0, \sigma_h^2)$ which leads to a non-zero probability of experiencing deep fades at some frequency subcarriers. The AWGN in (2) follows $V \sim \mathcal{CN}(0, \sigma_v{}^2)$. Finally, the subscript A refers to communication node A which receives the PPDU transmitted by node B.

For channel estimation, we apply a simple Least Squares (LS) channel estimation technique to the received signal Y_A in (2) and the estimated CFR is given by

$$\hat{H}_A[k] = X_p[k]^{-1}Y_A[k] = H[k] + \tilde{V}_A[k], \tag{3}$$

where $\tilde{V}_A[k] = X_p[k]^{-1}V_A[k]$ is the new noise term which has the same statistical characteristics as $V_A[k]$ since $X_p[k]$ is a Binary Phase Shift Keying (BPSK) sequence.

Once a CFR estimate is computed at the Rx, ranging techniques can be applied. One of these techniques is the simple approach of applying an Inverse Fast Fourier Transform (IFFT) to $\hat{H}_A$ to estimate the CIR and compute the delay of its first tap [14]. A direct conversion of the first tap delay to distance can then be applied to get the distance; $\hat{d} = c\hat{\tau}_0$.

Another common approach in the literature is the subspace-based super-resolution MUltiple SIgnal Classification (MUSIC) algorithm which was originally applied to the problem of multiple signal Angle of Arrival (AoA) estimation using linear receive antenna arrays [15]. This problem is analogous to the problem of channel tap delay estimation from CFR estimated at equi-spaced frequencies. Therefore, in this paper, the estimated CFR is the input to the MUSIC algorithm to estimate the first channel tap delay and then is converted to an equivalent distance estimate.

The MUSIC algorithm works by first estimating the CFR covariance matrix which is calculated as

$$\hat{\mathbf{R}} = \frac{1}{M}\mathbf{H}\mathbf{H}^H, \tag{4}$$

where $\mathbf{H}$ is an $N_{SC} \times M$ matrix whose columns are the CFR data estimated across N_{SC} sub-carriers from M time snapshots. To minimize the overhead of capturing multiple signal snapshots, the covariance matrix estimate $\hat{\mathbf{R}}$ can be realized using a Hankel matrix that is constructed from one CFR snapshot and spectral smoothing is applied as explained in [10] and [16]. To apply spectral smoothing, we replace (4) by $\hat{\mathbf{R}} = \bar{\mathbf{H}}\bar{\mathbf{H}}^H$, where $\bar{\mathbf{H}}$ is the Hankel matrix given by

$$\bar{\mathbf{H}} = \begin{bmatrix} \hat{H}_A[0] & \hat{H}_A[1] & \ldots & \hat{H}_A[N_{SC}-1-L_S] \\ \hat{H}_A[1] & \hat{H}_A[2] & \ldots & \hat{H}_A[N_{SC}-L_S] \\ \vdots & \vdots & \ddots & \vdots \\ \hat{H}_A[L_S-1] & \hat{H}_A[L_S] & \ldots & \hat{H}_A[N_{SC}-1] \end{bmatrix}, \tag{5}$$

and L_S is the smoothing length. An EigenValue Decomposition (EVD) of $\hat{\mathbf{R}}$ follows, where the signal and noise eigen-subspaces are separated as follows

$$\hat{\mathbf{R}} = \mathbf{U}\Lambda\mathbf{U}^H, \tag{6}$$

$$\mathbf{U} = \left[\mathbf{U}^s \ \mathbf{U}^n\right], \Lambda = \begin{bmatrix} \Lambda^s & 0 \\ 0 & \Lambda^n \end{bmatrix}. \tag{7}$$

The columns of the matrix $\mathbf{U}$ represent the eigenvectors of $\hat{\mathbf{R}}$ and are denoted by u_i, while the matrix Λ is a diagonal matrix with the eigenvalues λ_i placed along its diagonal elements. The signal subspace dimension is needed to know the number of signal eigenvalues and eigenvectors and separate them from the noise eigenvalues and eigenvectors as shown in (7). The signal subspace dimension is also equal to the number of channel paths. Hence, we apply a simple threshold-based algorithm to estimate the number of channel paths based on the idea that the signal eigenvalues should exhibit higher magnitudes than those of the noise.

Next, we compute the MUSIC pseudo spectrum $J(\tau)$ where we exploit orthogonality between the signal and noise subspaces, in addition to the fact that the signal steering vector $\phi(\tau) = \left[1, e^{-j2\pi\Delta f\tau}, e^{-j2\pi 2\Delta f\tau}, \ldots, e^{-j2\pi(N-1)\Delta f\tau}\right]$ is in the signal subspace for any delay τ value that matches the delay of any of the channel paths. Hence, we calculate the steering vectors for all possible delays and substitute them in the following MUSIC pseudo spectrum expression

$$J(\tau) = \frac{1}{\phi^H(\tau)\mathbf{U}^n\mathbf{U}^{nH}\phi(\tau)}. \tag{8}$$

For the ease of implementation, $\phi(\tau)$ is calculated for different τ values and concatenated in a unified matrix Φ to get the entire MUSIC pseudo spectrum vector in one step as follows:

$$J = \frac{1}{\Phi^H\mathbf{U}^n\mathbf{U}^{nH}\Phi} = \frac{1}{||\Phi^H\mathbf{U}^n||^2}. \tag{9}$$

Finally, the largest peaks of J are identified, where the first peak delay represents $\hat{\tau}_0$. For a detailed explanation of the MUSIC algorithm, the reader is referred to [17], [18], [19], and [20].

III. TWO-WAY CHANNEL MEASUREMENTS

As mentioned in Section I, CFR bandwidth is the most critical factor affecting ranging accuracy. Nevertheless, wide bandwidth CFR estimates are not always achievable due to several practical limitations, such as the inability of most low-power IoT devices to support wide bandwidth operation. To overcome the end device operation bandwidth limitation, CFR estimates can be collected at different WiFi channels each having a relatively smaller bandwidth. Individual CFR estimates are then stitched together to form an aggregate unified CFR estimate whose bandwidth is sufficiently large to satisfy ranging accuracy requirements. In this paper, we focus on operating in the WiFi 5 GHz frequency band where we have access to a much wider bandwidth.

A. PHASE ERRORS

For individual CFR estimates (collected at WiFi channels $i = 0, 1, \ldots, B-1$) to be successfully stitched together, they must have coherent phase. Unfortunately, due to the PLL operation at both the Tx and the Rx, it settles on a new random phase every time it switches frequency. This ruins the phase coherency between CFR estimates collected at different channels. Denote the PLL phase at the Tx (device B) and Rx (device A) at WiFi channel i by θ_i^B and θ_i^A, respectively. Then, the overall phase offset of the CFR at channel i will be $\theta_i^B - \theta_i^A$. Thus, the effect of these phase mismatches on the estimated CFR in channel i is

$$\hat{H}_A^i[k] = H^i[k]e^{j(\theta_i^B - \theta_i^A)}, \tag{10}$$

where, H^i, and $\hat{H}_A^i$ are the clean and contaminated-phase CFRs of channel i, respectively, $k = 0, 1, \ldots, N-1$ is the frequency index, and N is the total number of frequency samples [8]. Note that noise is neglected in this model.

To restore coherence and thus enable CFR stitching, the two-way approach can be applied [9]. This approach involves two nodes; the initiator and the reflector nodes, which exchange single-tone carrier signals and measure their phases. By combining the measured phases at both nodes, the PLL mismatched phase terms cancel out and yield coherent measurements collected at different channels [14], [21], [22]. This approach has been further extended to include the channel magnitude response in addition to its phase to get what we refer to as two-way CSI measurements. The two-way CSI measurement approach is adopted in the literature for mitigating CFR incoherence in Bluetooth [13] and WiFi [8] systems. To match the two-way CSI measurement concept with the notation used in Equations (2) and (3), we denote the reflector and initiator by nodes A, and B, respectively, throughout the rest of this paper.

Unlike the phase-based two-way transmission approach which only sends unmodulated carrier signals, the two-way CSI-based approach executes the CFR estimation process twice; once at node A and another time at node B. CFR estimates collected at both nodes are then multiplied yielding the two-way CFR estimate $\hat{\hat{H}}$. Thanks to the channel reciprocity property, any carrier phase mismatch gets cancelled after this CFR multiplication. We note that dealing with the two-way CFR estimate $\hat{\hat{H}}$ instead of the one-way CFR estimate $\hat{H}$ is equivalent to convolving the CIR with itself ($\hat{\hat{h}} = \hat{h} * \hat{h}$) which will double the multipath delay spread. Consequently, it will double the delay of the first tap and therefore the final distance estimate has to be divided by two.

Another issue that is not related to CFR stitching but affects the estimated CFR phase quality is Sub-sample Timing Offset (STO) which is present when there is no time synchronization between nodes A and B on a sub-sample level. The term sub-sample synchronization refers to a finer level of time synchronization that aligns signal time samples taken at the two communicating nodes, and not just packet-level synchronization. STO, if not corrected, will add a linear phase signal to the estimated CFR phase. By adding STO effects to PLL phase mismatches included in (10), we get

$$\hat{H}_A^i[k] = H^i[k]e^{j(\theta_i^B-\theta_i^A)-j2\pi\tilde{\tau}_A k/N}, \tag{11}$$

where $\tilde{\tau}_A$ is the STO value normalized to the sample interval and seen by node A. To cancel STO effects, the two-way CFR approach can be applied which exploits the reciprocity property. In other words, since $\tilde{\tau}_B = 1 - \tilde{\tau}_A$, the STO value will be canceled out in the two-way CFR as follows:

$$\hat{H}_B^i[k] = H^i[k]e^{j(\theta_i^A-\theta_i^B)-j2\pi(1-\tilde{\tau}_A)k/N}, \tag{12}$$

$$\hat{\hat{H}}[k] = \hat{H}_A^i[k]\hat{H}_B^i[k] = H^{i^2}[k]e^{-j2\pi k/N}. \tag{13}$$

We emphasize that $\tilde{\tau}_B$ is not just equal to $-\tilde{\tau}_A$ because STO can not be negative. The resulting extra factor $e^{-j2\pi k/N}$ in (13) is known and can be pre-compensated for at the packet detection stage or later after the two-way CFR $\hat{\hat{H}}$ is calculated.

B. PERFORMANCE DRAWBACKS OF THE TWO-WAY APPROACH

Although the two-way approach is effective in mitigating PLL phase mismatches and STO linear phase, it yields an effective CIR that is equal to the convolution of the actual CIR with itself which has the following drawbacks on the ranging performance

- CFR multiplication degrades the SNR level.
- The convolution operation doubles the width of each channel tap which significantly increases the probability of interference between consecutive taps.
- It weakens the first channel tap, which represents the LoS path, relative to other channel paths. This significantly complicates the first tap detection to estimate its delay and degrades the ranging accuracy.
- It doubles the multipath effects as the convolution operation yields double the number of channel taps making it more challenging to resolve these paths. Moreover, distributing the channel power over more taps will affect their magnitudes and some could be undetectable.

To demonstrate how two-way CFR measurements degrade the SNR, we start from (3) which describes the one-way CFR estimate at each node. To get the two-way CFR estimate, the two one-way estimates collected at nodes A and B are multiplied as follows

$$\begin{aligned}\hat{\hat{H}}[k] &= \hat{H}_A[k]\hat{H}_B[k]\\ &= (H[k]e^{j\theta_{BA}} + \tilde{V}_A[k])(H[k]e^{j\theta_{AB}} + \tilde{V}_B[k]),\end{aligned} \tag{14}$$

where the two phase parameters θ_{AB} and θ_{BA} represent the overall phase mismatches between the two nodes seen by nodes B and A, respectively. As explained before, $\theta_{AB} = -\theta_{BA}$ and will cancel out. The final two-way CFR estimate is given by

$$\begin{aligned}\hat{\hat{H}}[k] = H^2[k] &+ H[k]e^{j\theta_{BA}}\tilde{V}_B[k]\\ &+ H[k]e^{j\theta_{AB}}\tilde{V}_A[k] + \tilde{V}_A[k]\tilde{V}_B[k],\end{aligned} \tag{15}$$

where it can be seen that the first term is the desired term and the other three terms combined represent the new noise term for the two-way CFR estimate.

Now, we derive the SNR expressions needed to compare both approaches. The one-way SNR expression is straightforward to derive from (3) and is given by

$$SNR_{1way} = \frac{\mathbb{E}[H^*H]}{\mathbb{E}[\tilde{V}^*\tilde{V}]} = \frac{\sigma_h^2}{\sigma_{\tilde{v}}^2} = \rho, \tag{16}$$

where we also refer to the ratio $\sigma_h^2/\sigma_{\tilde{v}}^2$ as the input SNR and denote it by ρ. On the other hand, (15) is used to derive the two-way SNR expression as follows

$$\begin{aligned}&SNR_{2way}\\ &= \frac{\mathbb{E}[H^{2*}H^2]}{\mathbb{E}[(H\tilde{V}_B + H\tilde{V}_A + \tilde{V}_A\tilde{V}_B)^*(H\tilde{V}_B + H\tilde{V}_A + \tilde{V}_A\tilde{V}_B)]},\\ &= \frac{2\sigma_h^4}{2\sigma_h^2\sigma_{\tilde{v}}^2 + \sigma_{\tilde{v}}^4} = \frac{2\rho^2}{2\rho + 1},\end{aligned} \tag{17}$$

where the details of the second-order moment calculation of H^2 are included in Appendix A. In addition, to simplify notation, the phase terms were dropped as they will not affect the power of the noise terms. From the expressions in (16) and (17), we have

$$\frac{SNR_{1way}}{SNR_{2Way}} = \frac{2\rho^2 + \rho}{2\rho^2} = 1 + \frac{1}{2\rho}, \tag{18}$$

It is clear that the SNRs of the two approaches will only converge at high input SNR. Figure 1 demonstrates that the SNR loss exhibited by the two-way approach keeps decreasing with increasing input SNR until reaching a value of less

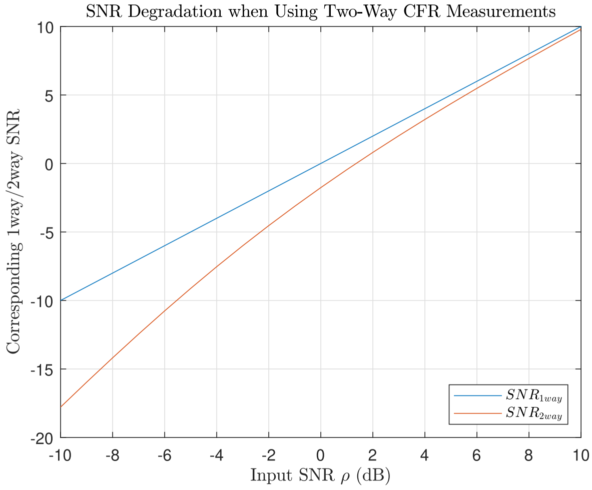

FIGURE 1. One-way vs. two-way SNR.

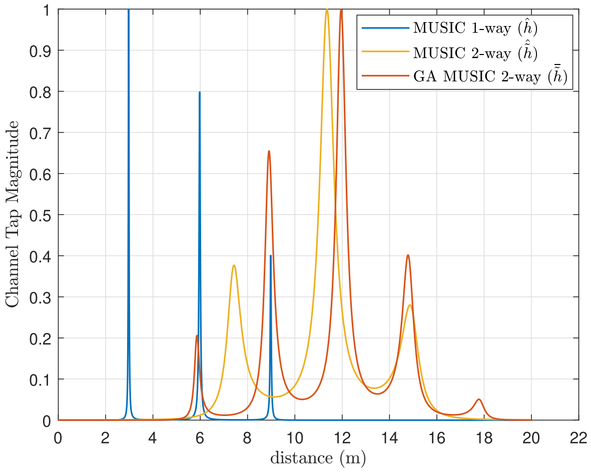

FIGURE 2. One-way vs. two-way ideal CIR and their MUSIC estimates.

than 1 dB when the input SNR exceeds 5 dB. On the other hand, the SNR loss increases at lower input SNR.

The other three drawbacks of using two-way channel measurements are demonstrated in Figure 2 which shows different variants of the estimated CIR of a 3-tap multipath channel that has tap delays of 10ns, 20ns, and 30ns. These delays are equivalent to distances of 3m, 6m, and 9m, respectively. The equivalent channel tap magnitudes are 0 dB, -1 dB, -3 dB, respectively. The three CIR estimates depicted in the figure correspond to: one-way MUSIC estimate $\hat{h}$, two-way MUSIC estimate $\hat{\hat{h}}$, and Genie-Aided (GA) two-way MUSIC estimate $\bar{\bar{h}}$ which assumes knowledge of the correct number of channel paths. The total CFR bandwidth assumed when computing these MUSIC estimates is 160 MHz, and the distance between the Tx and Rx is assumed to be 3 meters.

By comparing the three MUSIC CIR estimates in Figure 2, it can be seen that one-way MUSIC estimation yields sharp peaks located very close to the distances equivalent to the true delays of the channel taps. Notice that all the impulse-like peaks are shifted by 3 meters. On the other hand, two-way MUSIC estimation, which assumes no prior knowledge of the number of channel paths, failed to generate a number of peaks that reflects the true number of channel paths. Recall that for two-way channel measurements, the true number of paths should be 5 while we see 3 peaks only because the two-way operation weakened the power of some of the signal eigenvalues to be below the detectable range. Therefore, the two-way CIR estimate is not accurate and the first peak will lead to an erroneous distance estimate.

In addition to one-way and two-way MUSIC estimation, the GA two-way MUSIC is added to the comparison to demonstrate the other two drawbacks without including the effect of an incorrect number of CIR paths estimation. Hence, by comparing the GA two-way MUSIC estimate of the CIR and one-way MUSIC estimation, we observe two main differences. First, the width of each detected peak is much wider than the width of those peaks in one-way estimation. This increases the probability of blending the first and second peaks together. Second, the first peak is the second weakest peak compared to being the strongest in one-way estimation. This is analogous to transforming the LoS scenario to a non-LoS one where the first path is not the strongest. These two problems might not be very significant here in this relaxed scenario where the channel paths are well separated and the bandwidth is sufficiently large. However, in scenarios where the channel paths are closer or the bandwidth is more limited, the first peak can be indistinguishable from the second one.

The reduction of the first channel tap power can be demonstrated mathematically by considering a simple 2-tap channel model. Denoting the one-way channel taps by h_0 and h_1, then the equivalent two-way 3 channel taps will be h_0^2, $2h_0h_1$, and h_1^2. Hence, the first-to-second tap power ratio for both the one-way and two-way channels are given by

$$\left(\frac{P_0}{P_1}\right)_{1way} = \frac{|h_0|^2}{|h_1|^2}, \tag{19}$$

$$\left(\frac{P_0}{P_1}\right)_{2way} = \frac{|h_0^2|^2}{4|h_0h_1|^2} = \frac{|h_0|^2}{4|h_1|^2}, \tag{20}$$

$$\Rightarrow \left(\frac{P_0}{P_1}\right)_{2way} = \frac{1}{4}\left(\frac{P_0}{P_1}\right)_{1way}. \tag{21}$$

This result demonstrates that correctly distinguishing the first tap from the second one is much more challenging while operating with two-way channels. In addition, the result in (21) holds regardless of the number of channel taps since the first and second taps of the two-way channel will always be h_0^2, and $2h_0h_1$, respectively. Moreover, the first-to-second tap power is most important since it affects the first tap location estimation and, in turn, ranging accuracy.

C. ONE-WAY VS TWO-WAY RANGING ACCURACY

After gaining some insights on how MUSIC operates with two-way channel measurements, it is also important to compare the overall ranging accuracy using one-way and two-way

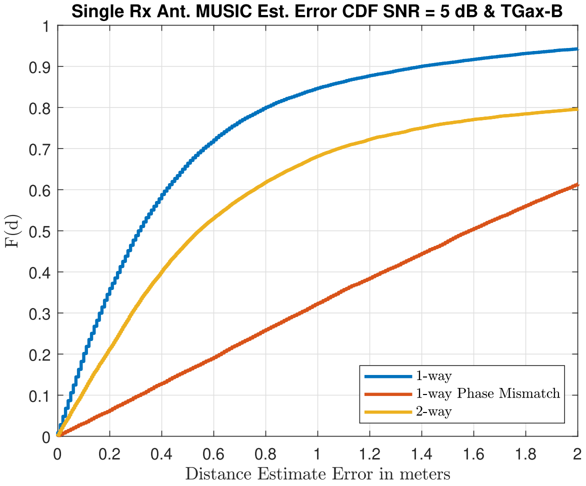

FIGURE 3. One-way vs. two-way distance estimation error CDF curves.

Algorithm 1 2-Way to 1-Way Channel Transformation

```
**Input:** $\hat{\tilde{H}} \rightarrow (N_{SC}^{tot} \times 1), \hat{H}_A \rightarrow (N_{SC}^{ch} \times B)$
**Output:** $\hat{H} \rightarrow (N_{SC}^{tot} \times 1), \hat{\hat{H}} \rightarrow (N_{SC}^{tot} \times 1)$
**initialization:**
    $signFlipMarker = zeros(N_{SC}^{tot})$
    $\phi_{Th} = \pi/2$
**procedure**
  $H_{sqrt} = \sqrt{\hat{\tilde{H}}}$
  $\left(|H_{sqrt}| = \sqrt{|\hat{\tilde{H}}|}\right)$
  $\left(\angle H_{sqrt} = \angle\hat{\tilde{H}}/2\right)$
    $\phi = \angle(H_{sqrt})$
    $\hat{H} = H_{sqrt}$
  **for** $i_{SC} = 1 : N_{SC}^{tot} - 1$ **do**
    **if** $|\phi^{i_{SC}} - \phi^{i_{SC}-1}| > \phi_{Th}$ **then**
      $signFlipMarker(i_{SC}) = 1$
    **end if**
  **end for**
  **for** $i_{SC} = 1 : N_{SC}^{tot} - 1$ **do**
    **if** $signFlipMarker(i_{SC}) == 1$ **then**
      $\hat{H}[i_{SC} : end] = -\hat{H}[i_{SC} : end]$
    **end if**
  **end for**
  $\hat{\hat{H}} = df\_det\_corr(\hat{H}, \hat{H}_A)$
**end procedure**
**return** $\hat{H}, \hat{\hat{H}}$
```

channels under practical operating conditions. To do this, we developed an 802.11ax WiFi simulator which models the PLL phase mismatches in addition to the WiFi preamble transmission and channel estimation process. The CFR estimates computed by the simulator are fed to the MUSIC algorithm that also incorporates the spectral smoothing method. For this one-way versus two-way comparison, we use 8 of the 12 20-MHz channels available in the UNII-2c sub-band of the 5GHz WiFi frequency band [23]. The estimated CFR at the 8 20-MHz channels are then stitched together to form a unified CFR estimate with 160 MHz total bandwidth. This is done once using the two-way approach where all phase errors are mitigated, and a second time using the one-way approach where phase mismatches are not mitigated. In addition, we compare with the ideal case of 1-way without phase mismatches which represents a performance upper bound added to understand how much ranging accuracy we lose when using the two-way approach. The operating SNR is set to 5 dB and we use the TGax Type-B channel model described in [24].

The distance estimation error cumulative distribution function (CDF) curves for the three approaches are plotted in Figure 3, where the performance gap can be clearly seen between the ideal one-way with no phase mismatches and the two-way curves. This corroborates our earlier discussion about the four drawbacks of two-way operation. On the other hand, one-way operation which suffers from uncompensated phase mismatches achieves the worst performance and is not considered any further in this paper.

IV. TWO-WAY TO ONE-WAY CHANNEL TRANSFORMATION

As we demonstrated in the previous section, despite the benefits of two-way channel measurements in mitigating phase mismatches, ranging accuracy is degraded significantly compared to ideal one-way channels. Therefore, in this section, we propose a novel scheme to estimate the one-way channel from the two-way channel. Our scheme operates on the two-way channel measurements after mitigating phase mismatches that hinder CSI stitching. Hence, there is no compromise on the quality of CSI stitching because of our proposed two-way to one-way channel transformation.

A. RESOLVING THE SIGN AMBIGUITY

For two-way to one-way channel transformation, a simple idea that first comes to mind is to take the square root of the two-way CFR. However, taking the square root results in a sign ambiguity. More specifically, taking the square root of a complex CFR sample transforms its phase from ranging between $-\pi$ to π to prematurely wrapping around between $-\frac{\pi}{2}$ to $\frac{\pi}{2}$. This distorts the CFR and renders it useless for ranging because of the extra phase transitions taking place every time the phase hits $-\frac{\pi}{2}$ or $\frac{\pi}{2}$.

The first step in our two-way to one-way channel transformation is to deal with the limited phase range resulting from taking the square root. Hence, in Algorithm 1, we provide our pseudo code to unwrap the phase and return it to its natural $-\pi$ to π range. Our idea is to approach the square root channel in a differential manner, where we compare the phase of each sample with that of the preceding sample. Whenever we measure a phase change that is greater than $\frac{\pi}{2}$, a phase wrapping point is detected and a negative sign should be applied starting from this sample to the end of the CFR vector.

Algorithm 2 $df\_det\_corr(\hat{H}, \hat{H}_A)$ Funcion Logic

```
**Input:** $\hat{H} \rightarrow (N_{SC}^{tot} \times 1)$, $\hat{H}_A \rightarrow (N_{SC}^{ch} \times B)$
**Output:** $\hat{\hat{H}} \rightarrow (N_{SC}^{tot} \times 1)$ (The enhanced version)
**initialization:**
    $\hat{\hat{H}} = \hat{H}$
    $deepFade_{Th} = 0.20$
    $N_{df} = 0$ (Number of detected deep fades)
    $dfGroups = \phi$ (Deep fade indices grouped)
**procedure**
    $H_{sqrt} = H_{sqrt}/\text{mean}(|H_{sqrt}|)$
    $dfScIndices = |H_{sqrt}| < deepFade_{Th}$
    $[dfScGroups, N_{df}] = group(dfScIndices)$
    (Group adjacent indices into groups)

    **for** $i_{df} = 1 : N_{df}$ **do**
        **if** $dfScGroups\{i_{df}\} \notin \{gapScIndices\}$ **then**
            $i = dfScGroups\{i_{df}\} \in \{chan_{start}^{i} : chan_{end}^{i}\}$
            $\psi = \angle(\hat{\hat{H}}[chan_{start}^{i} : chan_{end}^{i}])$
                $-\angle(\hat{H}_A[:, i])$
            $\psi = \psi - \psi[0]$
            $i_{filpSign} = \Delta\psi > \pi/2$
            $\hat{\hat{H}}[i_{filpSign}] = -\hat{\hat{H}}[i_{filpSign}]$
        **else**
            $\psi = \angle\big(movAvg(\hat{H}_A, L_{FIR})\big)$
            $\psi' = \Delta\psi$
            $i = dfScGroups\{i_{df}\} \in \{gapScIndices\}$
            **if** $\psi'^{i}[end] > 0$ **or** $\psi'^{i+1}[0] > 0$ **then**
                **if** $\angle(\hat{\hat{H}}[chan_{end}^{i}]) > \angle(\hat{\hat{H}}[chan_{start}^{i+1}])$**then**
                    $\hat{\hat{H}}[chan_{start}^{i+1} : end] = -\hat{\hat{H}}[chan_{start}^{i+1} : end]$
                **end if**
            **else**
                **if** $\angle(\hat{\hat{H}}[chan_{end}^{i}]) < \angle(\hat{\hat{H}}[chan_{start}^{i+1}])$**then**
                    $\hat{\hat{H}}[chan_{start}^{i+1} : end] = -\hat{\hat{H}}[chan_{start}^{i+1} : end]$
                **end if**
            **end if**
        **end if**
    **end for**
**return** $\hat{\hat{H}}$
```

We chose the phase jump threshold to be $\frac{\pi}{2}$ as it represents the midpoint in any $-\frac{\pi}{2}$ to $\frac{\pi}{2}$ transition.

We emphasize that if a negative sign is applied once a phase wrap is detected, it will have a vertical shifting effect on the remaining CFR samples. This ruins the phase wrap detection criterion by invalidating the threshold value applied for detection. Therefore, the phase wrap detection and correction steps have to be separated as shown in Algorithm 1. The algorithm ends by calling Alg. 2 which provides some enhancements to be discussed in the next subsection.

B. DEEP FADE CASES

While testing our proposed phase unwrapping scheme, we noticed that its accuracy decreases under severe multipath conditions due to more frequent deep fades. The significance of these deep fades is that they are typically accompanied by sharp transitions in the channel phase response. These phase transitions can confuse our phase unwrapping algorithm since it operates by detecting transitions to undo them. In addition, at deep fade frequencies the CFR magnitude is so weak and the CFR estimates are very noisy making the problem even worse. In Appendix B, we demonstrate the relationship between the CFR fading magnitude and its equivalent phase response sudden changes.

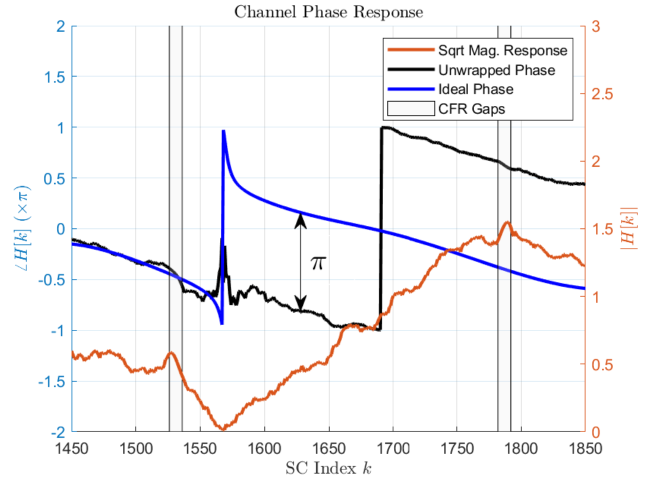

FIGURE 4. Channel phase response at deep fade frequencies.

The effect of deep fades on the estimated channel phase response is illustrated in Figure 4. As depicted in the figure, the steep drop of the ideal phase response taking place around the deep fade went undetected in the unwrapped phase response. This took place because the transition was too steep and therefore, with $[-\frac{\pi}{2}, \frac{\pi}{2}]$ phase wrapping it appeared as if the phase continued decreasing in an almost linear fashion. It can also be seen from the figure how degraded the phase estimate quality is around the deep fading frequency. The end result of these inaccuracies is having a phase mismatch of π between the ideal and estimated phases in all samples succeeding the fading frequency. In some other cases, phase transitions around fading frequencies can be misinterpreted by the unwrapping algorithm and get mistakenly modified. This takes place since the unwrapping algorithm cannot differentiate between real phase transitions due to deep fades and phase artifacts due to the square root operation.

C. ALGORITHM ENHANCEMENTS ADDRESSING DEEP FADE PROBLEMS

The solution we propose to deal with the deep fade problem is based on the availability of the initial one-way CFR estimates. Although this initial one-way CFR estimate suffers from phase transitions between channel estimates over different WiFi frequency channels (due to PLL phase mismatches) and linear phase caused by STO, it can still be beneficial in detecting and correcting the deep fade problem effects. Our idea is to locate the deep fade frequency and match it with the overlapping WiFi channel. Since the initial one-way CFR is coherent within each WiFi channel, it can be used as a phase correction reference for the unwrapped phase. Nevertheless, due to the linear phase imposed on the one-way CFR because of STO, it cannot be directly used as a reference, but we solve this problem by adding a differentiation step to get rid of that linear function. The unwrapped phases of one-way CFR $\hat{H}_A$, and the one-way CFR estimate $\hat{H}$ from Alg. 1, respectively, are given by

$$\psi_{\hat{H}_A}[k] = f[k] + \tau_0 k + \tilde{\tau}_A k + n_1, \tag{22}$$

$$\psi_{\hat{H}}[k] = f[k] + \tau_0 k + e[k] + n_2, \tag{23}$$

where $f[k]$ is a phase function depending on the channel structure, $e[k]$ is the phase error signal representing the erroneous phase transitions of value π, and n_1 and n_2 are two noise terms. The term $\tau_0 k$ in both equations represents the linear phase due to propagation delay, while $\tilde{\tau}_A$ represents the linear phase due to STO. By calculating the difference ψ between the two phases in (22) and (23) and then calculating the difference $\Delta\psi$, we can eliminate the STO linear phase and locate the frequency bins where phase errors of π took place. The steps of the proposed phase correction technique are listed in Algorithm 2.

Unfortunately, the WiFi channel structure in the 5 GHz band might render this proposed solution inapplicable in some cases because of the non-overlapping nature of the 5 GHz band WiFi channels which results in some CFR gaps between each WiFi channel and the next one. Consequently, whenever a deep fade lies within one of these gaps, the phase correction algorithm cannot be applied. Therefore, in Algorithm 2, we first identify the location of the deep fades. If they are located within one of the available CFR ranges, then we apply our idea of using one-way CFR as a correction reference. However, phase correction when deep fades take place within CFR gaps is much more challenging due to the lack of any coherent reference.

To deal with this second challenging scenario, we propose an approach based on phase slope estimation followed by applying the logic in Algorithm 2. Our phase slope-based technique is illustrated in Figures 5, and 6, where we differentiate between two cases: deep fades resulting from zeros inside or outside the unit circle. As depicted in the Figures, the first case exhibits a phase increase, while we observe a phase decrease in the second case. Therefore, by calculating the derivative of the estimated CFR phase and determining its sign around the gap, we can predict the phase trend within the gap which aids us in determining the correct phase. In Figure 5, it is clear that the phase slope is positive right before and after the gap. Therefore, we decide that the phase slope is positive within the gap. Consequently, observing any phase values that belong to the "Mismatched Phase" group shown in the figure will imply a phase error that should be corrected. Similarly, negative phase slopes before and after the gap can guide us to correct the phase as shown in Figure 6.

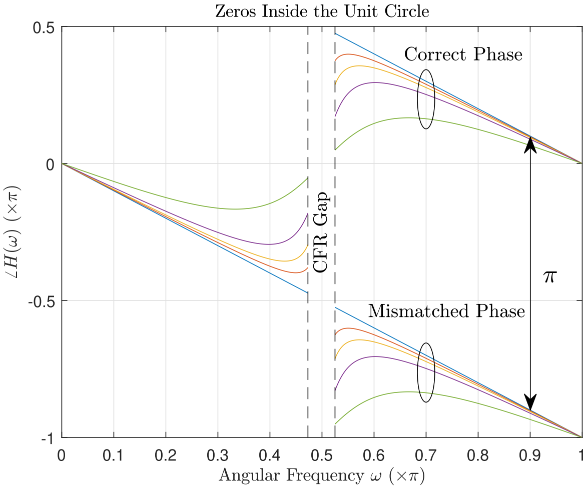

FIGURE 5. Phase errors of value π caused by channel deep fades taking place within CFR gaps when the CIR zeros are inside the unit circle.

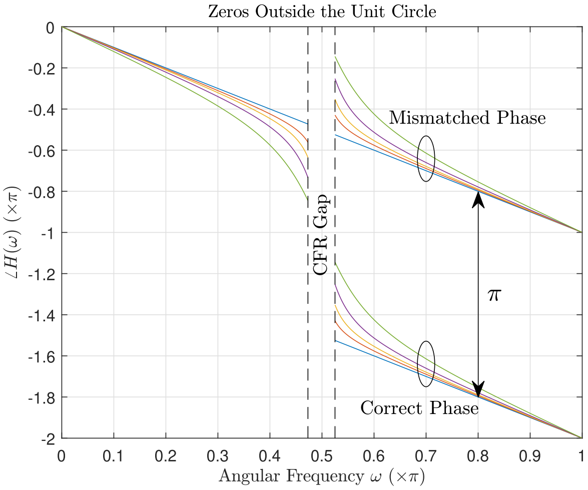

FIGURE 6. Phase errors of value π caused by channel deep fades taking place within CFR gaps when the CIR zeros are outside the unit circle.

D. SIGNIFICANCE OF THE DEEP FADE PROBLEM

As shown in Alg. 2, we propose two techniques to deal with CFR deep fades based on their locations. For deep fades within the available CFR frequencies, we follow the simple approach of comparing with one-way CFR. On the other hand, the other case where deep fades take place within CFR gaps is more challenging. To justify the extra processing needed for the second case, we calculate its frequency of occurrence. Therefore, we derive the probability of its occurrence in different channel environments. We consider three channel models that belong to the TGax channel model family described in the IEEE 802.11 standard documents [24]. The description of these channel models is in Table 3.

After deciding on the channel models of interest and based on our knowledge of the CFR gaps locations, we can now calculate the probability of overlap between CFR gaps and the channel deep fades. Depending on the total CFR bandwidth, the number of gaps and the total number of sub-carriers will change. In all of our investigated scenarios, we assume transmission of a number of 20 MHz WiFi channels that are to be stitched later. For instance, by sending 10 of these 20 MHz channels, we have a total bandwidth of 200 MHz, 2560 sub-carriers (including gaps), and 9 CFR gaps each consisting of 11 sub-carriers. Therefore, the probabilities of the first, second, and the n$^{\text{th}}$ deep fade to overlap with a CFR gap are given by

$$P(1^{st}DF \cap Gap) = \frac{N_{SC}^{G}(B-1)}{N_{SC}^{tot}B}, \tag{24}$$

$$P(2^{nd}DF \cap Gap|1^{st}DF \cap Gap = \phi) = \frac{N_{SC}^{G}(B-1)}{N_{SC}^{tot}B - S}, \tag{25}$$

$$\begin{aligned} P\Big(n^{th}DF \cap Gap|\big(1^{st}DF \cap Gap = \phi\big) \cap \ldots \\ \cap \big((n-1)^{th}DF \cap Gap = \phi\big)\Big) = \frac{N_{SC}^{G}(B-1)}{N_{SC}^{tot}B - (n-1)S}, \end{aligned} \tag{26}$$

where, N_{SC}^{G}, N_{SC}^{ch}, and B represent the number of sub-carriers per CFR gap, the number of sub-carriers per channel, and the number of channels, respectively. These three parameters are system configuration parameters, while S is an algorithm parameter and represents the assumed minimum separation between consecutive deep fades in sub-carriers. Denoting the probabilities in (24), (25), and (26) by p_1, p_2, and p_n, respectively, then the probability of at least one deep fade to overlap with a CFR gap can be expressed as follows

$$P(anyDF \cap Gap) = \sum_{n=1}^{N_{DF}} p_n, \tag{27}$$

where N_{DF} is the average total number of deep fades for a specific channel model. Simulations were run for the three TGax channel models under study and we found that the average total number of deep fades for models Type-B, Type-C, and Type-D is 3.25, 5.42, and 6.94, respectively, in a total bandwidth of 240 MHz. By rounding these numbers to the nearest integer and substituting back in (27), we get probabilities of having an overlap between at least one deep fade and a gap of 0.12, 0.2, and 0.29 for Type-B, Type-C, and Type-D TGax channel models, respectively. This analysis confirms the importance of executing the additional algorithm steps that deal with cases where deep fades are located within CFR gaps.

E. MULTIPLE SNAPSHOTS FOR SNR ENHANCEMENT

The success of our proposed schemes is dependent on the quality of the estimated CFR. The schemes involve phase comparisons with finely-tuned thresholds, unwrapped channel phase response comparison with the estimated one-way channel phase response which acts as a reference, and also phase response slope estimation. These are all intricate operations whose accuracy depends on the phase response estimate quality. The lower the SNR operating level is, the lower the quality of these phase estimates will be and therefore, the worse the proposed schemes will perform.

TABLE 3. TGax channel models description [24].

Model	Delay Spread	# of Clusters	Taps/ Cluster	Propagation Scenario	Usage Model
B	15ns	2	5,7	Indoor residential	Intra-room, room to room
C	30ns	2	10,8	Small office	Conference, classrooms
D	50ns	3	16,7,4	Indoor typical office	Open areas, large classrooms

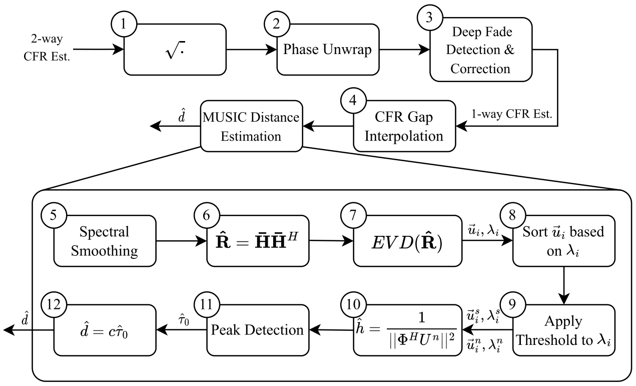
2-way
CFR Est.
1
$\sqrt{\cdot}$
2
Phase Unwrap
3
Deep Fade Detection & Correction
1-way CFR Est.
4
CFR Gap Interpolation
MUSIC Distance Estimation
$\hat{d}$
5
Spectral Smoothing
6
$\hat{\mathbf{R}} = \bar{\mathbf{H}}\bar{\mathbf{H}}^H$
7
$EVD(\hat{\mathbf{R}})$
$\vec{u}_i, \lambda_i$
8
Sort $\vec{u}_i$ based on λ_i
9
Apply Threshold to λ_i
$\vec{u}_i^s, \lambda_i^s$
$\vec{u}_i^n, \lambda_i^n$
10
$\hat{h} = \frac{1}{||\Phi^H U^n||^2}$
11
Peak Detection
$\hat{\tau}_0$
12
$\hat{d} = c\hat{\tau}_0$
$\hat{d}$

FIGURE 7. Ranging algorithm steps.

To address this challenge, we propose an extension of our scheme that utilizes multiple snapshots. Since this challenge is limited to low operating SNR scenarios, we can mitigate it by sending multiple HE-LTF fields within the WiFi PPDU so that channel estimation can be done multiple times yielding multiple CFR estimates that can be averaged to boost the SNR level. This approach is fully compatible with the WiFi 802.11ax standard which allows up to 8 LTF fields in the HE portion of the preamble [25], [26]. In Section IV, we will present performance results for a low operating SNR scenario where we exploit multiple HE-LTF fields to boost the SNR and enhance the proposed schemes performance levels.

V. COMPLEXITY ANALYSIS

In this section, we study the computational complexity of our proposed scheme in its two versions. The entire WiFi ranging scheme is broken down into steps as depicted in the block diagram in Figure 7. Steps 1 and 2 represent the first version of our proposed scheme for one-way CFR estimation from two-way CFR (Alg. 1). Adding the third step, we get the second and more advanced version of the proposed scheme (Alg. 1 plus Alg. 2). Steps 4 to 12 represent the smoothed MUSIC CSI-based ranging technique, which can be applied directly to the input two-way CFR estimate or to any of the one-way CFR estimates we get at the outputs of Step 2 and 3. The detailed explanation of the MUSIC Distance Estimation Block operation (steps 5 to 12) was provided in Section II.

To assess the added computational complexity of our proposed schemes, we calculate the FLoating-point OPeration (FLOP) count of each block. Although the MUSIC distance estimation steps are common among all investigated schemes, we still include it in our FLOP count. To get a FLOP count estimate for any algorithm, some assumptions must be made about the basic arithmetic operations cost. It is assumed in [27] that addition, subtraction, multiplication, division, and square-root can all be counted as one FLOP. The justification provided for equating the division and square-root FLOP count to that of addition, subtraction, and multiplication despite of their extra complexity, is their rarity. However, our proposed schemes heavily utilize the square-root operation and such assumption does not hold. Moreover, in our proposed schemes, we convert the CFR samples from Cartesian to polar forms and back which requires estimating the computational complexity of trignometric functions.

In our complexity analysis, we rely on the bench-marking study in [28]. Flop count values of 1, 1, 1, 4, 6, 14, 14, and 23 will be used for the addition, subtraction, multiplication, division, square-root, sin(.), cos(.), and arctan(.) operations, respectively. In addition, to simplify the complexity analysis for algorithms that involve complex number arithmetic operations, it is suggested in [29] to use complex FLOP counts instead of breaking them into real FLOP counts which is the approach we will follow. We emphasize that any computational complexity assessment should be viewed as an approximate measure of complexity and interpreted in a relative sense when comparing different algorithms due to varying processor architectures and different memory handling techniques [30].

In Table 4, we summarize the total FLOP counts of the main ranging algorithm steps. The first entry shows the combined FLOP count of Steps 1 and 2 shown in Figure 7. Similarly, the second entry of the table shows the FLOP count of Step 3 which represents the algorithms enhancements of our proposed scheme for deep fade scenarios. It can be seen that Step 3 entails more complexity than Steps 1 and 2 combined as it is of the order $O({N_{SC}}^2)$ compared to $O(N_{SC})$ for Steps 1 and 2. However, this quadratic complexity level of the proposed scheme will diminish in comparison to the complexity of Steps 4 to 12 that represent the conventional MUSIC distance estimation algorithm. It is also worth noting that the complexity of Steps 4 to 12 is dominated by that of Steps 6, 7, and 10 which involve costly complex matrix multiplications and EVD.[1] As shown in the table, Steps 4 to 12 have cubic complexity of $O({N_{SC}^{tot}}^3)$, where N_{SC} and N_{SC}^{tot} represent the total number of sub-carriers before and after adding the gap sub-carriers, respectively. The two quantities are proportional and therefore, the change of variables will not affect the calculated complexity orders

$$N_{SC}^{tot} = N_{SC} + 11(B - 1). \tag{28}$$

TABLE 4. Complex FLOP count for the most significant Algorithm steps.

Alg. Step	FLOP Count [2]
① + ②	$49 N_{SC}$
③	$\frac{\gamma}{\kappa} {N_{SC}}^2 + (\frac{N_{SC}^{ch}(L_{FIR}+35)}{\kappa} + 21) N_{SC}$
④ → ⑫	$\sim {N_{SC}^{tot}}^3 + \frac{10}{3} \mu {N_{SC}^{tot}}^2 - 10 \mu M_s N_{SC}^{tot}$

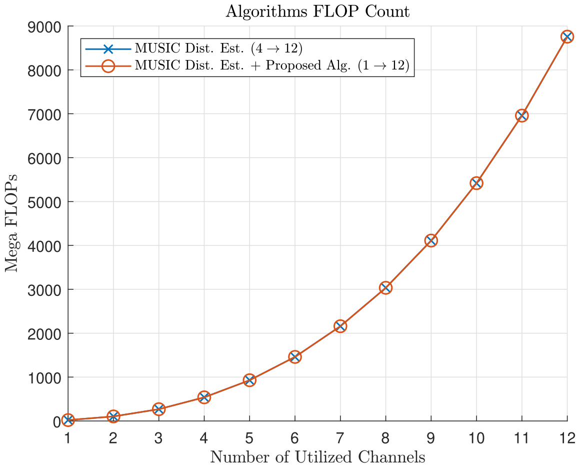

FIGURE 8. Ranging algorithm complexity with and without our proposed schemes.

The number 11 above represents the fixed guard band size between any two consecutive 20-MHz channels in the 5 GHz WiFi band, while B is the number of 20-MHz channels used.

This is further clarified by referring to Figure 8 which compares the total FLOP counts for the ranging algorithm with and without utilizing our proposed scheme. As it can be seen from the figure, there is no noticeable difference between the two curves which highlights the fact that the added complexity of our proposed algorithms is negligible compared to the MUSIC distance estimation algorithm complexity. Hence, performance gains reported in the next section are achieved at negligible additional complexity.

VI. NUMERICAL RESULTS

In this section, we split our performance results into to two parts: simulation-based results and Universal Software Radio Peripheral (USRP) testbed results. However, before presenting the performance results, the following remarks related to practical issues regarding Alg. 1 and 2 are in order.

- **The Deep Fade Magnitude Threshold:** First, it is important to emphasize that the CFR estimate is normalized with respect to its average magnitude and not the

[1] The number of FLOPs used for the EVD step takes into consideration the Hermitian structure of the estimated CFR covariance matrix.

[2] The variables γ, κ, L_{FIR}, μ and M_s represent the size of deep fade regions in sub-carriers, the ratio between the number of sub-carriers and the number of deep fades taking place in that range, the length of the moving average filter in Alg. 2, the reciprocal of the distance calculation resolution in centimeters, and the number of estimated channel taps, respectively.

maximum. We found this choice to enhance robustness since the maximum can dramatically change from one channel realization to another. Second, the deep fade magnitude threshold used in Algorithm 2 was chosen to be 20% of the average CFR magnitude. This value was chosen to achieve a good compromise between deep fades miss detection and false alarms. In our problem, both are harmful to the ranging performance. Miss detection simply means that phase transitions due to deep fades will be overlooked causing phase errors. On the other hand, false alarms mean that the correct phase will be mistakenly modified which will leave us with an erroneous phase response as well.

- **Phase Slope Estimation:** In Algorithm 2, there is a phase slope estimation step where the estimated slope is used to extrapolate the phase behavior within CFR gaps. The accuracy of this phase slope estimate is highly dependent on the CFR estimate quality. Therefore, we apply moving average smoothing to the estimated CFR to eliminate any high frequency variations that might alter slope estimation around the gaps since slope estimation is vulnerable to high frequency small changes.
- **CFR Interpolation:** As highlighted in Section IV-C, the 5 GHz WiFi channel structure leaves us with some CFR gaps after CFR stitching. These gaps have to be filled before the CFR is passed to the MUSIC distance estimation algorithm. In our WiFi simulator, we apply cubic spline interpolation to fill in the gaps after all the phase correction steps are completed [31].

A. COMPUTER SIMULATION RESULTS

To evaluate the overall WiFi ranging performance, we use distance estimation error CDF as our metric. In addition, we report the median error value and the percentage of time a 50 cm of distance error or less is achieved. Figures 9, 10, and 11 show these CDF curves for the three TGax channel models B, C, and D, respectively. The figures compare four approaches: square-root phase unwrapping, square-root phase unwrapping with deep fade detection and correction, in addition to the plain two-way and ideal one-way approaches. Note that for the ideal one-way, the PLL and all other phase mismatches are disabled to coherently stitch individual CFR estimates collected from different WiFi channels. All of the results presented in this section are generated for a total bandwidth of 240 MHz unless stated otherwise.

It can be seen from Figure 9 that the two proposed schemes for square-root phase processing offer a significant gain over the plain two-way approach. For this scenario, our enhanced proposed algorithm achieves almost identical performance to that of the ideal one-way approach. The median error values achieved for the ideal one-way, square-root phase unwrapping with deep fade detection and correction, square-root phase unwrapping, and plain two-way approaches are 13 cm, 14 cm, 16 cm, and 30 cm, respectively. In addition, 50 cm of distance error or less was achieved 85%, 83%, 78%, and 63% of the time by the four approaches, respectively.

TABLE 5. Ranging performance for three TGax channel model types.

Scheme	Metric	TGax Type-B	TGax Type-C	TGax Type-D
1-way	Median	13 cm	19 cm	16 cm
	<50 cm	85%	76%	82%
Unwrap	Median	16 cm	31 cm	41 cm
	<50 cm	78%	61%	54%
DF Det. & Corr.	Median	14 cm	23 cm	25 cm
	<50 cm	83%	70%	66%
2-way	Median	30 cm	59 cm	84 cm
	<50 cm	63%	45%	41%

Switching to the TGax Type-C results presented in Figure 10, it can be seen that the performance of our proposed schemes is not as close to the ideal one-way approach as in the previous case of the TGax Type-B. However, ranging accuracy gains over the plain two-way approach are still evident and even more significant than in the previous case. In this scenario, 19 cm, 23 cm, 31 cm, and 59 cm median errors were achieved by the four schemes, respectively, while the 50 cm mark was achieved 76%, 70%, 61%, and 45% of the time, respectively. Similarly, as depicted in Figure 11, we observe bigger gaps between the two proposed schemes and the ideal one-way approach while still achieving significant gains over the two-way approach. Finally, for this scenario, median error values of 16 cm, 25 cm, 41 cm, and 84 cm were achieved by the four approaches, respectively, while 50 cm of error or less was achieved 82%, 66%, 54%, and 41% of the time, respectively. The numerical results for these three channel model scenarios are summarized in Table 5. The key conclusion from these results is the robustness of the ranging accuracy gains of our proposed schemes over plain 2-way transmission across different channel models.

It is also interesting to observe how the one-way and two-way performances vary across different channel models with varying multipath severity. Specifically, for the ideal one-way approach, the ranging accuracy degradation from the Type-B to Type-C channel models, then to Type-D is much less significant than the degradation experienced by the plain two-way approach. This again corroborates the assertions we made in Section III about the sensitivity of the plain two-way approach to multipath.

In Figure 12, we showcase the resilience of our proposed schemes to low operating SNR scenarios. Here, we compare 4 sets of CDF curves, one representing each of the 4 approaches under test. Nevertheless, this time for each approach, we consider a CFR estimate obtained by averaging 1, 2, 4, and 8 CFR estimates obtained from multiple HE-LTF fields. For the one-way and two-way approaches, performance did not change using SNR-enhanced CFR

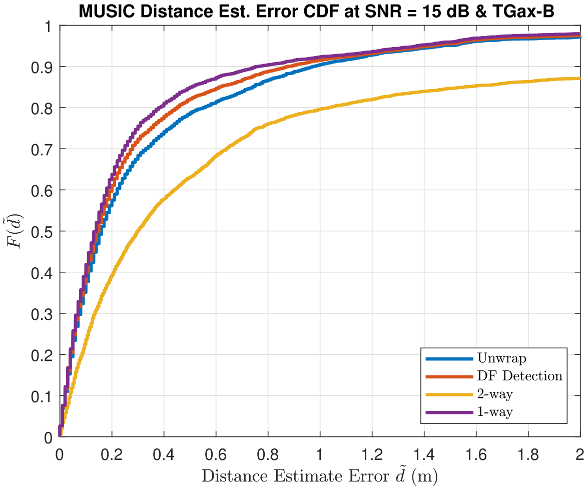

FIGURE 9. **Distance estimation error CDF curve for TGax Type-B channel model.**

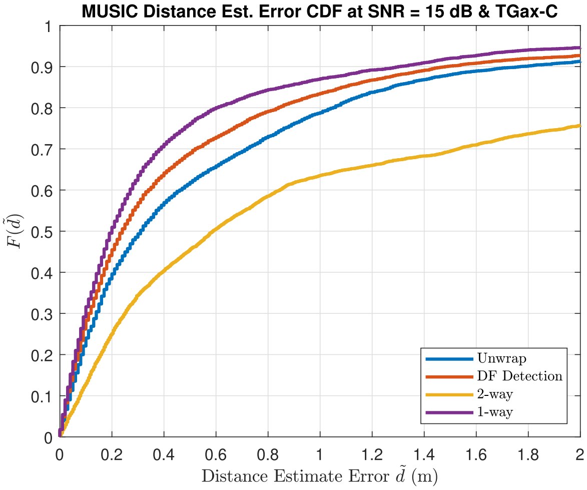

FIGURE 10. **Distance estimation error CDF curve for TGax Type-C channel model.**

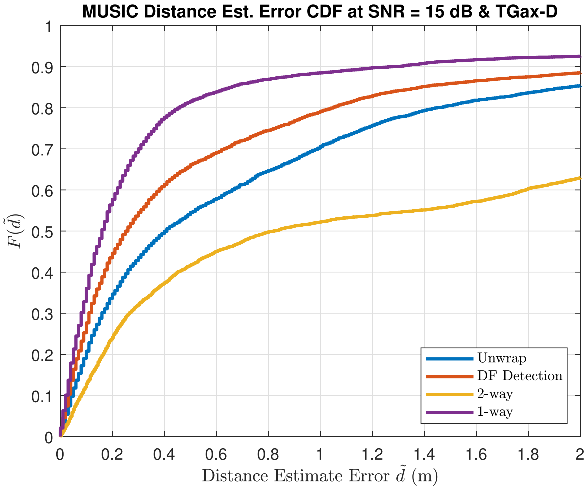

FIGURE 11. **Distance estimation error CDF curve for TGax Type-D channel model.**

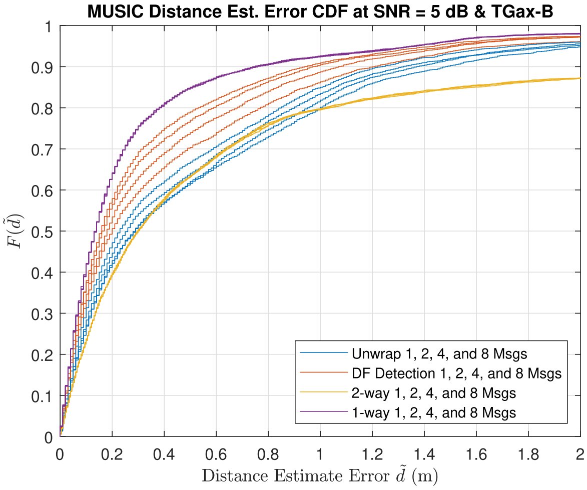

FIGURE 12. **Distance estimation error CDF curves for TGax Type-B channel model operating at SNR = 5 dB and using multiple messages.**

estimates. This suggests that the assumed SNR of 5 dB is high enough for ranging accuracy to be already multipath limited and not noise limited. On the other hand, the ranging accuracy gain of our proposed schemes from using SNR-enhanced CFR estimates is evident. This gain is due to the enhanced estimated channel phase response quality which enables us to execute the proposed algorithms steps with better accuracy leading to significant ranging accuracy gains as mentioned in Subsection IV-E and seen in Figure 12. It is also worth mentioning that if multiple CFR estimates are not used to boost the SNR, then the first version of our proposed scheme (only square-root and phase unwrapping) will have a crossover with the two-way approach as seen in the figure. This is due to accuracy effects low SNR operation have on the proposed schemes that are mitigated using multiple CFR estimates.

Finally, we investigate the ranging accuracy gains of our proposed scheme with total bandwidth. In addition to the 240 MHz case studied earlier, we consider a total bandwidth of 80 MHz and 160 MHz and the resulting CDF curves are shown in Figure 13. To simplify the presentation, only the enhanced version of our proposed algorithm is compared to the plain two-way and ideal one-way approaches. As depicted in the figure, the performance gap between our proposed scheme and ideal one-way is negligible for both bandwidths. The numerical results for these cases are summarized in Table 6.

B. USRP TESTBED RESULTS

To demonstrate the performance enhancements our proposed schemes can achieve in practical scenarios, we built a USRP testbed that mimics 802.11ax Wi-Fi operation. This wireless system consists of two USRP devices acting as node A and B (initiator and reflector). Each device is set up with external amplifiers, switches, and calibrations required for successful Wi-Fi transmission and reception to obtain two-way CSI measurements for ranging. No external time

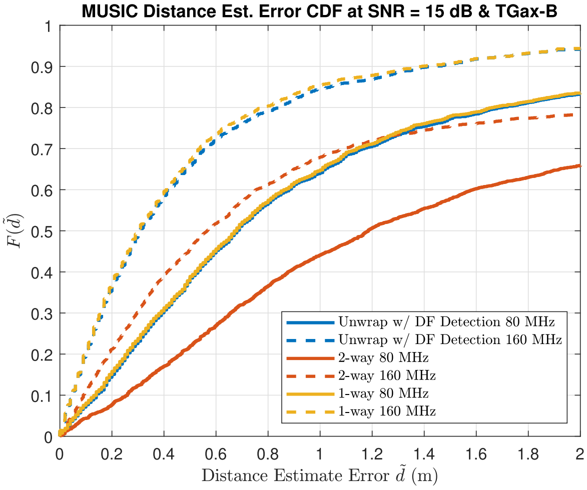

FIGURE 13. Distance estimation error CDF curve for TGax Type-B channel model at BW = 80 MHz and 160 MHz.

TABLE 6. Ranging performance for different total bandwidth.

Scheme	Metric	240 MHz	160 MHz	80 MHz
1-way	Median	13 cm	30 cm	67 cm
	<50 cm	85%	67%	39%
DF Det. & Corr.	Median	14 cm	31 cm	67 cm
	<50 cm	83%	66%	38%
2-way	Median	30 cm	57 cm	118.5 cm
	<50 cm	63%	46%	22%

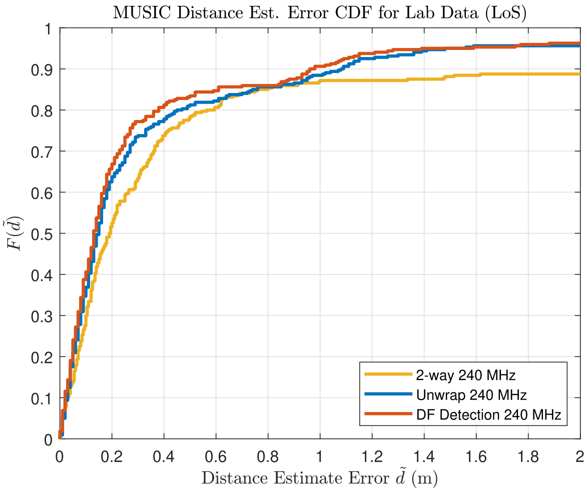

FIGURE 14. Distance estimation error CDF curves for WiFi testbed data collected in LoS scenarios.

or frequency synchronization is employed. With this testbed, measurements are taken across 12 20-MHz channels in the UNII-2c sub-band, and individual antenna pair measurements are utilized for evaluation.

All of our laboratory tests are performed in a room full of PCs, benches, and other miscellaneous hardware acting as signal scatterers and representing a multipath rich environment. The testbed data was collected in two main communication scenarios: i) Line-of-Sight (LoS), and ii) mainly Non-LoS. The distance estimation error CDF curves for these two scenarios are depicted in Figures 14 and 15, respectively. The results obtained for the two scenarios highly resemble the simulated results we obtained for the TGax Type-B and Type-D cases. This highlights the accuracy of our simulation models and the accuracy of our assumptions compared to realistic scenarios.

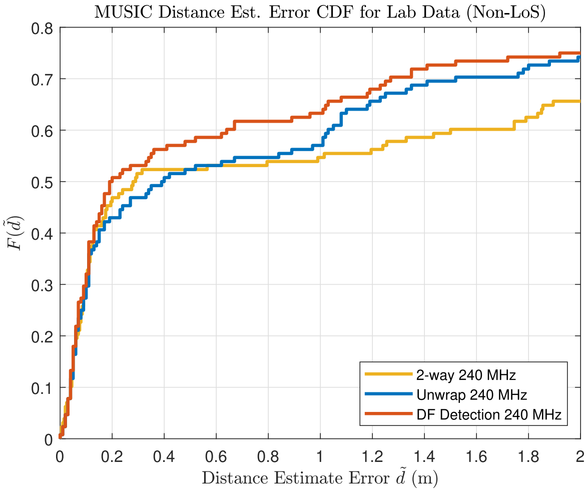

FIGURE 15. Distance estimation error CDF curves for WiFi testbed data collected in Non-LoS scenarios.

TABLE 7. Ranging performance for WiFi testbed data.

Scheme	Metric	LoS	Non-LoS
DF Det. & Corr.	Median	13 cm	19 cm
	<50 cm	83%	59%
2-way	Median	20 cm	29 cm
	<50 cm	78%	52%

As seen in Figure 14 which represents the LoS scenario, both versions of our proposed algorithm achieve a significant gain over two-way operation. The median distance error achieved is only 13 cm while error values smaller than or equal to 50 cm were achieved 83% of the time. In addition, the 90th percentile is achieved at a sub-meter error level. On the other hand, the non-LoS data results depicted in Figure 15 which shows, as expected, that the overall performance is not as good as that achieved in a LoS scenario. Nevertheless, our proposed schemes still exhibit a performance gain that is even higher than that achieved in the LoS case since there is more room for improvement. In this non-LoS case, the median error achieved is 19 cm and the percentage at which error values smaller than or equal to 50 cm were achieved dropped to 59%. It is important to mention that the ideal one-way performance is not shown in any of the testbed results since it cannot be practically achieved in the testbed and was only added to the simulation results for comparison purposes (as a performance upper-bound). The testbed results achieved for our two performance metrics are summarized in Table 7.

VII. CONCLUSION

In this paper, we considered a practical WiFi ranging scenario, where large bandwidth is crucial for achieving decimeter-level ranging accuracy and is realized using CFR stitching. This, in turn, requires mitigation of PLL phase mismatches from one WiFi channel to the next, in addition to eliminating STO both of which can be achieved using two-way ranging. On the other hand, we also discussed in detail the ranging accuracy degradation of the two-way approach compared to the ideal one-way approach due to doubling the multipath delay spread. Consequently, we proposed two novel schemes addressing the two-way ranging accuracy degradation. We applied the square-root to transform two-way CFR measurements to their one-way form followed by processing the phase errors at two levels. The first level dealt with immature phase wrapping and yielded our first scheme while the second level operates on top of the first one to further enhance the performance by detecting and correcting any phase errors that accompany deep channel fades.

The two proposed phase processing techniques were shown to achieve significant performance gains over the plain two-way approach by means of simulated data as well as a USRP-based WiFi ranging testbed. This gain was demonstrated under different channel models (with varying multipath severity), SNR levels, and total bandwidth values. For all of the scenarios tested using simulations, our proposed algorithm achieved distance estimation errors that are less than 10 cm higher than those achieved by the ideal one-way performance bound. In some cases, differences of as low as 1 cm of median distance error were achieved. Additionally, the WiFi testbed data confirms the gains achieved by our proposed schemes over two-way operation. Not only does our proposed algorithm achieve high ranging accuracy, but its added complexity is negligible compared to the baseline MUSIC ranging.

APPENDIX A
SECOND ORDER MOMENT OF A COMPLEX SQUARED RV

We start by considering the complex number $z = x + jy$, where $z \sim \mathcal{CN}(0, \sigma_z^2)$. It follows that x and $y \sim \mathcal{N}(0, \sigma_z^2/2)$, where they are iid. Now assume that the Random Variable (RV) $q = z^2 = x^2 - y^2 + j2xy$. It is required to calculate the first and second moments of the RV q. The expression for the first moment is given by

$$\mathbb{E}[q] = \mathbb{E}[x^2] - \mathbb{E}[y^2] + j2\mathbb{E}[xy] = 0, \tag{29}$$

because x and y are independent with zero mean, and $\mathbb{E}[x^2] = \mathbb{E}[y^2]$. The second-order moment expression can be derived as follows

$$\begin{aligned}\mathbb{E}[qq^*] &= \mathbb{E}[z^2 z^{2*}],\\ &= \mathbb{E}[x^4] + 2\mathbb{E}[x^2]\mathbb{E}[y^2] + \mathbb{E}[y^4].\end{aligned} \tag{30}$$

It is well-known that the fourth-order moment of a real normal RV $\mathbb{E}[x^4] = 3\sigma_x^4$ [32]. In our case, $\sigma_x^2 = \sigma_z^2/2$ and therefore, $\mathbb{E}[x^4] = \frac{3\sigma_z^4}{4}$. We use this result to substitute back in (30) to get

$$\mathbb{E}[qq^*] = 2\sigma_z^2. \tag{31}$$

This result is directly applied to the SNR expression derivation in (17).

APPENDIX B
PHASE RESPONSE AROUND DEEP FADE FREQUENCIES

Wireless multipath channels can be accurately modeled as finite impulse response (FIR) filters. The connection between the channel phase variations and deep fade locations can be easily understood by examining the zeros locations of these FIR filters. To understand the phase behavior around the filter's zeros, we consider a 2-tap FIR filter having a pair of complex-conjugate zeros at π and $-\pi$. The filter response is given by

$$H(z) = 1 + a_2 z^{-2}, \tag{32}$$

where a_2 is the second tap used to control the location of the filter zeros on the imaginary axis. In our analysis, we will compare the filter response for two sets of zeros locations. One set includes locations inside the unit circle and the other including locations outside it. Within each set we will vary the closeness of the filter zero to the unit circle to see how it affects the phase response behavior for both cases.

For zero locations inside the unit circle, we use a value of $a_2 = a$, while for the outside locations we use $a_2 = 2 - a$ to ensure that for every value of a the two locations are at the same distance from the unit circle and will affect the filter magnitude response equally at the frequency of the zero. The value of the parameter a is varied in the range $[0.5, 1]$. By varying the value of a in this range and calculating equivalent values of a_2, we get the filter phase responses depicted in Figure 16.

It can be seen in the figure that the biggest change in the filter phase response values take place around the filter zeros. Depending on whether those zeros are located inside or outside the unit circle, the phase response will either exhibit positive or negative phase transitions, respectively. Also, the closer the filter zeros are to the unit circle, the sharper their equivalent phase transitions will be. Recall that the closer a filter zero to the unit circle is, the deeper the fade will be.

Maximum phase changes taking place around the filter zeros is a behavior that can be mathematically analyzed as well. For a generic value of the filter coefficient a_2, the filter frequency response is given by [33]

$$\begin{aligned}H(e^{j\omega}) &= 1 + a_2 e^{-j2\omega},\\ &= 1 + a_2 cos(2\omega) - ja_2 sin(2\omega),\end{aligned} \tag{33}$$

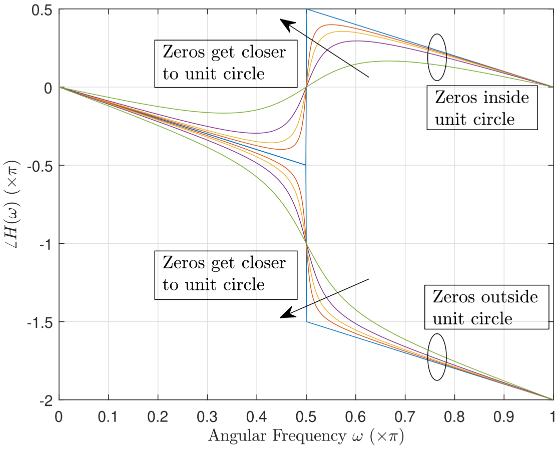

FIGURE 16. FIR filter phase response for different zeros locations.

where ω is the digital angular frequency. Hence, the phase response of this filter is given by

$$\angle H(e^{j\omega}) = -tan^{-1}\frac{a_2 sin(2\omega)}{1 + a_2 cos(2\omega)}. \quad (34)$$

To demonstrate that maximum phase changes take place at the frequencies of the zeros, the first and second derivatives of the phase expression in (34) are derived to get

$$\frac{d\angle H(e^{j\omega})}{d\omega} = \frac{2a_2\big(a_2 + cos(2\omega)\big)}{1 + a_2^2 + 2a_2 cos(2\omega)}, \quad (35)$$

$$\frac{d^2\angle H(e^{j\omega})}{d\omega^2} = \frac{4a_2 sin(2\omega)(1 - a_2^2)}{(1 + a_2^2)^2 + 4a_2(1 + a_2^2)cos(2\omega) + 4a_2^2 cos^2(2\omega)}. \quad (36)$$

Using (35) and (36), it can be easily shown that the maximum phase slope takes place at $\omega = \pi, -\pi$ which are the angular frequencies of the filter zeros. It can also be shown that values of a_2 that are closer to 1 will yield higher slope values and hence sharper phase transitions as depicted in Figure 16.

REFERENCES

[1] H. Liu, N. Xia, D. Guo, and P. Qing, "CSI-based indoor tracking with positioning-assisted," in *Proc. Ubiquitous Positioning, Indoor Navigat. Location-Based Services (UPINLBS)*, Mar. 2018, pp. 1–8.

[2] W. Liu, Q. Cheng, Z. Deng, H. Chen, X. Fu, X. Zheng, S. Zheng, C. Chen, and S. Wang, "Survey on CSI-based indoor positioning systems and recent advances," in *Proc. Int. Conf. Indoor Positioning Indoor Navigat. (IPIN)*, Sep. 2019, pp. 1–8.

[3] P. S. Farahsari, A. Farahzadi, J. Rezazadeh, and A. Bagheri, "A survey on indoor positioning systems for IoT-based applications," *IEEE Internet Things J.*, vol. 9, no. 10, pp. 7680–7699, May 2022.

[4] A. Quazi, "An overview on the time delay estimate in active and passive systems for target localization," *IEEE Trans. Acoust., Speech, Signal Process.*, vol. ASSP-29, no. 3, pp. 527–533, Jun. 1981.

[5] T. Redant and W. Dehaene, "High resolution time-of-arrival for a cm-precise super 10 meter 802.15. 3C-based 60 GHz OFDM positioning application," in *Proc. 2nd Int. Conf. Pervasive Embedded Comput. Commun. Syst.*, vol. 20. Setúbal, Portugal: SciTePress, 2012, pp. 271–277. [Online]. Available: http://www.scitepress.org

[6] Z. Yang, Z. Zhou, and Y. Liu, "From RSSI to CSI: Indoor localization via channel response," *ACM Comput. Surv.*, vol. 46, no. 2, pp. 1–32, Nov. 2013.

[7] J. Xiong, K. Sundaresan, and K. Jamieson, "Tonetrack: Leveraging frequency-agile radios for time-based indoor wireless localization," in *Proc. 21st Annu. Int. Conf. Mobile Comput. Netw.*, 2015, pp. 537–549.

[8] D. Vasisht, S. Kumar, and D. Katabi, "Decimeter-level localization with a single WiFi access point," in *Proc. 13th USENIX Symp. Netw. Syst. Design Implement. (NSDI)*, 2016, pp. 165–178.

[9] M. Pelka, C. Bollmeyer, and H. Hellbrück, "Accurate radio distance estimation by phase measurements with multiple frequencies," in *Proc. Int. Conf. Indoor Positioning Indoor Navigat. (IPIN)*, Oct. 2014, pp. 142–151.

[10] P. Boer, J. Romme, J. Govers, and G. Dolmans, "Performance of high-accuracy phase-based ranging in multipath environments," in *Proc. IEEE 91st Veh. Technol. Conf. (VTC-Spring)*, May 2020, pp. 1–5.

[11] S. Sen, B. Radunovic, R. R. Choudhury, and T. Minka, "You are facing the Mona Lisa: Spot localization using PHY layer information," in *Proc. 10th Int. Conf. Mobile Syst., Appl., Services*, Jun. 2012, pp. 183–196.

[12] M. Kotaru, K. Joshi, D. Bharadia, and S. Katti, "SpotFi: Decimeter level localization using WiFi," in *Proc. ACM Conf. Special Interest Group Data Commun.*, Aug. 2015, pp. 269–282.

[13] S. N. Shoudha, J. P. Van Marter, S. Helwa, A. G. Dabak, M. Torlak, and N. Al-Dhahir, "Reduced-complexity decimeter-level Bluetooth ranging in multipath environments," *IEEE Access*, vol. 10, pp. 38335–38350, 2022.

[14] Y. Schröder, D. Reimers, and L. Wolf, "Accurate and precise distance estimation from phase-based ranging data," in *Proc. Int. Conf. Indoor Positioning Indoor Navigat. (IPIN)*, Sep. 2018, pp. 1–8.

[15] H. Krim and M. Viberg, "Two decades of array signal processing research: The parametric approach," *IEEE Signal Process. Mag.*, vol. 13, no. 4, pp. 67–94, Jul. 1996.

[16] W. Liao and A. Fannjiang, "MUSIC for single-snapshot spectral estimation: Stability and super-resolution," *Appl. Comput. Harmon. Anal.*, vol. 40, no. 1, pp. 33–67, Jan. 2016.

[17] R. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE Trans. Antennas Propag.*, vol. AP-34, no. 3, pp. 276–280, Mar. 1986.

[18] P. Stoica and A. Nehorai, "MUSIC, maximum likelihood, and Cramer–Rao bound," *IEEE Trans. Acoust., Speech, Signal Process.*, vol. 37, no. 5, pp. 720–741, May 1989.

[19] H. L. Van Trees, *Optimum Array Processing: Part IV of Detection, Estimation, and Modulation Theory*. Hoboken, NJ, USA: Wiley, 2002.

[20] X. Li and K. Pahlavan, "Super-resolution TOA estimation with diversity for indoor geolocation," *IEEE Trans. Wireless Commun.*, vol. 3, no. 1, pp. 224–234, Jan. 2004.

[21] P. Zand, J. Romme, J. Govers, F. Pasveer, and G. Dolmans, "A high-accuracy phase-based ranging solution with Bluetooth low energy (BLE)," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–8.

[22] P. Zand, A. Duzen, J. Romme, J. Govers, C. Bachmann, and K. Philips, "A high-accuracy concurrent phase-based ranging for large-scale dense BLE network," in *Proc. IEEE 30th Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2019, pp. 1–7.

[23] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11-2020 (Revision of IEEE Standard 802.11-2016), 2021, pp. 1–4379.

[24] J. Liu, R. Porat, N. Jindal, V. Erceg, and S. Azizi, *IEEE 802.11ax Channel Model Document*, Standard IEEE 802.11ax, Wireless LANs, 2014.

[25] *IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks—Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN*, IEEE Standard 802.11ax-2021 (Amendment to IEEE Standard 802.11-2020), 2021, pp. 1–767.

[26] L. Ward, "802.11 ax technology introduction," Rohde & Schwarz, Munich, Germany, White Paper, Apr. 2020.

[27] L. N. Trefethen and D. Bau, III, *Numerical Linear Algebra*, vol. 50. Philadelphia, PA, USA: SIAM, 1997.

[28] L. Atkinson. *A Simple Benchmark of Various Math Operations*. Accessed: Jan. 26, 2023. [Online]. Available: https://latkin.org/blog/2014/11/09/a-simple-benchmark-of-various-math-operations/

[29] N. J. Higham, *Functions of Matrices: Theory and Computation*. Philadelphia, PA, USA: SIAM, 2008.

[30] C. F. Van Loan and G. Golub, *Matrix Computations* (Johns Hopkins Studies in Mathematical Sciences), vol. 53, 3rd ed. Baltimore, MD, USA: The Johns Hopkins Univ. Press, 1996.

[31] C. De Boor, *A Practical Guide to Splines*, vol. 27. New York, NY, USA: Springer-Verlag, 1978.

[32] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Upper Saddle River, NJ, USA: Prentice-Hall, 1993.

[33] J. G. Proakis and D. G. Manolakis, *Digital Signal Processing: Principles, Algorithms, and Applications*, 3rd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 1996.

SHERIEF HELWA (Student Member, IEEE) received the B.S. and M.S. degrees from Ain Shams University, Cairo, Egypt, in 2012 and 2017, respectively. He is currently pursuing the Ph.D. degree in electrical engineering with The University of Texas at Dallas, Richardson, TX, USA. From 2014 to 2015, he was a Research Engineer with Alcatel-Lucent under the Bell Labs org., where he worked on capacity dimensioning and RF planning algorithms and tools. From 2015 to 2018, he was developing signal processing algorithms and did wireless system design with Axxcelera Broadband Wireless, Cairo. In 2019, he joined the Connectivity Department, Facebook Inc., Menlo Park, CA, USA, as an Intern, where he worked on the ''Rural Access'' project. In 2020, he joined Qualcomm Corporation, San Diego, CA, USA, as an Intern and contributed to Qualcomm's 802.11ax access point design. His research interests include signal processing for digital communication systems and machine learning applications.

JAYSON P. VAN MARTER (Student Member, IEEE) received the B.S. degree (summa cum laude) in electrical engineering from The University of Texas at Dallas, Richardson, TX, USA, in 2020, where he is currently pursuing the Ph.D. degree with a focus on wireless information systems. In spring and summer 2020, he developed a USRP software-defined radio testbed engine as a TxACE Intern. His current research interests include real-time embedded systems, localization, millimeter wave radar, terahertz radar, and SAR imaging algorithms. He received the TxACE Promising Researcher Award, in May 2020, and the Jonsson School Excellence in Education Doctoral Fellowship, in August 2020.

SHAMMAN NOOR SHOUDHA (Student Member, IEEE) received the B.Sc. degree in electrical and electronics engineering from the Bangladesh University of Engineering and Technology, in 2017, and the M.Sc. degree in electrical engineering from The University of Texas at Dallas, in 2021, where he is currently pursuing the Ph.D. degree in electrical engineering. His current research interests include wireless localization and machine learning applications. He received the Louis Beecherl Jr. Graduate and Phil Ritter Endowed Fellowships, in 2021 and 2022, respectively.

MATAN BEN-SHACHAR was born in Israel, in 1977. He received the B.Sc. degree in electrical engineering from the Ben-Gurion University of the Negev, Beer-Sheva, Israel, in 2005. Since 2005, he has been a PHY-Layer Modem and System Engineer, specializing in WiFi, BLE, and NFC standards. His research interests include communication systems and education theory.

YARON ALPERT was born in Israel, in 1966. He received the B.Sc. degree in electrical engineering from the Technion—Israel Institute of Technology, Haifa, Israel, in 1993, and the M.Sc. degree (summa cum laude) in electrical engineering from Tel-Aviv University, Tel-Aviv, Israel, in 1999. Since 1999, he has been a Principal Communication System Architect, specializing in WiFi, BLE, and 3GPP standards. His research interests include wireless networks and communication theory. He is also an active member of the IEEE 802.11 Standard Committee and in the WiFi Alliance.

ANAND G. DABAK (Fellow, IEEE) received the bachelor's degree from IIT, Bombay, India, in 1987, and the master's and Ph.D. degrees in electrical engineering from Rice University, in 1989 and 1992, respectively. He joined the DSP Systems Research and Development Center, Texas Instruments Inc. (TI), as a member of Technical Staff working on wireless systems, in 1995. He worked on algorithms, standards, and systems issues related to communications, namely 3GPP, WCDMA, LTE, UWB, powerline communications (PLC), and modem development on TI processors, until 2011. From 2011 to 2019, he was with Kilby Labs on ultrasonic flow metering for residential water and gas metering. From 2019 to 2021, he developed localization solutions for Bluetooth low energy (BLE) systems using both angles of arrival (AoA) and employed super-resolution techniques for high-accuracy distance measurement (HADM) phase-based techniques. Since 2021, he has been with the Radar Group on applying signal processing techniques to radar applications. He has more than 250 patents in the areas of signal processing for wireless, PLC, and ultrasound applications to flow metering. He has been a TI Fellow, since 2007.

MURAT TORLAK (Senior Member, IEEE) received the M.S. and Ph.D. degrees in electrical engineering from The University of Texas at Austin, Austin, TX, USA, in 1995 and 1999, respectively. Since August 1999, he has been with the Department of Electrical and Computer Engineering, The University of Texas at Dallas, Richardson, TX, USA, where he has been promoted to the rank of a Full Professor. He is currently the Rotating Program Director of the U.S. National Science Foundation, Alexandria, VA, USA. His current research interests include experimental verification of wireless networking systems, cognitive radios, millimeter wave automotive radars, millimeter wave imaging systems, and interference mitigation in radio telescopes. He was the General Chair of the Symposium on Millimeter Wave Imaging and Communications, in 2013, and the IEEE GlobalSIP Conference. He was an Associate Editor of the IEEE Transactions on Wireless Communications, from 2008 to 2013. He was the Guest Co-Editor of the Special Issue on Recent Advances in Automotive Radar Signal Processing of IEEE Journal of Selected Topics in Signal Processing, in 2021.

NAOFAL AL-DHAHIR (Fellow, IEEE) received the Ph.D. degree from Stanford University. He was a Principal Member of Technical Staff with the GE Research Center and AT&T Shannon Laboratory, from 1994 to 2003. He is currently an Erik Jonsson Distinguished Professor and the ECE Department Associate Head with The University of Texas at Dallas. He is a co-inventor of 43 issued patents and the coauthor of about 460 articles. He is a fellow of the National Academy of Inventors. He was a co-recipient of four IEEE best paper awards. He received the 2019 IEEE SPCC Technical Recognition Award and the 2021 Qualcomm Faculty Award. He served as the Editor-in-Chief for IEEE Transactions on Communications, from January 2016 to December 2019.