Identifying Non-linear CSI Phase Measurement Errors with Commodity WiFi Devices

Yiwei Zhuo, Hongzi Zhu, Hua Xue
Department of Computer Science and Engineering
Shanghai Jiao Tong University
Shanghai, China
{zyw081285, hongzi, howardsid}@sjtu.edu.cn

***Abstract*—WiFi technology has gained a wide prevalence for not only wireless communication but also pervasive sensing. A wide variety of emerging applications leverage accurate measurements of the Channel State Information (CSI) information exposed by commodity WiFi devices. Due to hardware imperfection of commodity WiFi devices, the frequency response of internal signal processing circuit is mixed with the real channel frequency response in passband, which makes deriving accurate channel frequency response or CSI measurements a challenging task. In this paper, we conduct an extensive empirical studies on CSI measurements and identify a non-negligible non-linear CSI phase error, which cannot be compensated by existing calibration strategies targeted at linear CSI phase errors. We conduct intensive analysis on the properties of such non-linear CSI phase errors and find that such errors are prevalent among various WiFi devices. Furthermore, they are stable along time and for different time-of-flight but sensitive to the received signal strength indication (RSSI) of the received signal, the band frequency and the specific radios used between a transmission pair. Based on these key observations, we infer that the IQ imbalance issue in the direct-down-conversion architecture of commodity WiFi devices is the root source of the non-linear CSI phase errors. Our findings are essential to CSI-based applications and call for new practical strategies to remedy non-linear phase errors.**

Keywords—Channel State Information (CSI); measurements; non-linear phase errors; empirical study

I. INTRODUCTION

Ubiquitous WiFi technology has fostered a broad range of applications beyond a vehicle for communication. In recent years, fast conceptualization and continuous revolution of myriad emerging applications, e.g., seeing through-walls [1], gesture recognition [2, 19], line-of-sight (LOS) identification [3, 14], indoor localization [4, 5, 8, 10, 15], detecting movements of an object [11, 15, 37], secure communication [10, 17], continuously revolutionize the horizon [6]. Such applications rely heavily on accurate measurements of the Channel State Information (CSI), which refers to the channel properties of a communication link in any frequency band. This information describes how a signal propagates from the transmitter to the receiver and represents the combined effect of, for example, scattering, fading, and power decay with distance. In addition, the frequency domain CSI can also be transformed to the time domain Power Delay Profile (PDP) through Inverse Fast Fourier Transform (IFFT) without loss of information. A PDP fully characterizes a multipath channel, and has been recently used in various motion- or location-based applications. As a result, accurate CSI measurements are of great significance to tremendous applications.

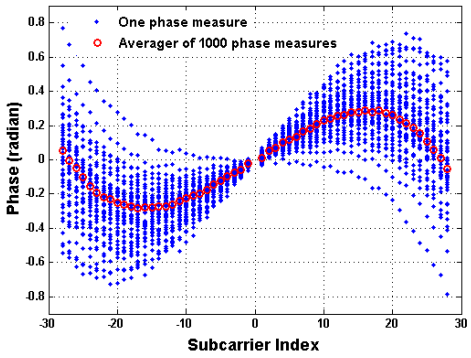

Fig. 1. 100 CSI phase measurements in a 20MHz WiFi channel at the 2.4GHz frequency band between a transmission pair obtained in a stable channel condition, with the mean of each measurement removed to zero.

To obtain a CSI, commodity WiFi network interface cards (NICs) such as Intel 5300 and Atheors AR9380 can be easily used. Deriving accurate CSIs directly from such NIC readings, however, is challenging as the obtained CSI measurements describe not only channel properties in passband but also the signal processing circuit properties in baseband. Previous studies [3,7,8,9,10] have pointed out the following sources of CSI measurement errors due to hardware imperfection in the wireless signal processing, including power control uncertainty, packet detection delay, sampling frequency offset (SFO), carrier frequency offset (CFO), random initial phase offset, and phase ambiguity. The impacts of above error sources to CSI measurements are three-fold: (1) power control uncertainty causes a CSI amplitude offset; (2) packet detection delay and SFO, essentially equivalent to a time delay, cause CSI phase rotation errors; (3) the rest would respectively cause an identical CSI phase offset error on each measured sub-carriers. As a result, the measured CSI phase in one WiFi band is *linearly* distorted with a phase error measured on each sub-carrier expressed as a rotation error proportional to the sub-carrier index plus an offset.

According to previous work [12], the CSI amplitude offsets in individual bands can be easily removed by averaging the sufficient number of CSI measurements obtained within the channel coherence time. As for CSI phase linear errors, several

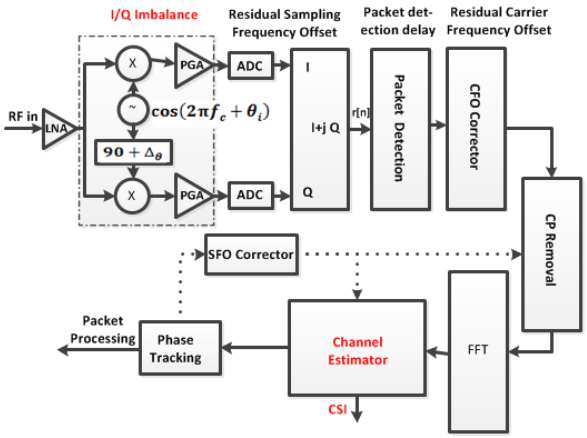

Fig. 2. Illustration of signal processing in 802.11n.

state-of-the-art strategies have been proposed. For example, a linear transform on the raw CSI phase can be conducted [13, 14], in the way that the mean of phases on all sub-carriers is forced to zero, and the phase slope between the first subcarrier and last subcarrier is forced to zero too. Another example is to search a linear fitting [4, 15] and subtract the fitted linear function from the raw CSI phase. Most recent work [9] obtains CSIs from different frequency bands, averages raw CSI phase measures from the same individual frequency band to eliminate the rotation error due to the packet detection delay, and search an identical rotation among individual frequency bands to compensate the rotation error due to SFO. All strategies above are based on an assumption that all the notable phase errors except measurement noise are linear. In contrast, Figure 1 illustrates 100 CSI phase measurements in a stable 20MHz WiFi channel at the 2.4GHz frequency band between two Atheors AR9380 nodes. It is obvious that phases measured on sub-carriers especially for those at both ends of the channel are severely distorted in a non-linear way. As a result, there exists an unknown source of non-linear CSI phase errors.

In this paper, we first conduct extensive empirical study on CSI measurements using commodity WiFi NICs. In addition to verifying those error sources mentioned above, we find *non-linear* CSI phase errors among all sub-carriers in a WiFi band. We then analyze the key properties of the non-linear CSI phase errors and have the following observations: 1) non-linear CSI phase errors are prevalent among various WiFi NICs; 2) the non-linear CSI phase errors introduced by the same WiFi receiver are rather stable along time; 3) the non-linear CSI phase errors has nothing to do with time-of-flight; 4) such non-linear CSI phase errors are closely related to the received signal strength indication (RSSI) of the received signal, the band frequency and the specific radios used between a transmission pair. We also point out that the IQ imbalance issue in the direct-down-conversion architecture of commodity WiFi devices is the root source of the non-linear CSI phase errors.

In the remainder of this paper, we first introduce some preliminary knowledge about the channel frequency response, the current signal processing design used in commodity WiFi devices and the reported CSI measurement error sources in Section II. Section III elaborates our empirical studies on CSI measurements, where non-linear CSI phase errors are identified and analyzed. We then discuss the root source of the identified non-linear phase errors in Section IV. Section V presents related work and we conclude in Section Vi.

II. PRELIMINARIES

A. Theoretical Foundation

According to [21, 22], the channel frequency response $h(f)$ can be expressed as:

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

where N is the total number of multipaths, α_l and τ_l represent the attenuation and the propagation delay of the signal through path l, respectively. Channel frequency response is reported in the form of CSI in 802.11 WiFi, with each sample containing amplitude and phase information. For two sub-carriers f_m and f_n, since they undergo the same time-of-flight along a path l, the phase difference between f_m and f_n can be expressed as:

$$\Delta_{m,n} = -2\pi \cdot (f_m - f_n) \cdot \tau_l \mod 2\pi \quad (2)$$

B. Signal Processing at an 802.11 Receiver

A typical WiFi 2.4GHz receiver with direct down conversion architecture is shown in Figure 2. An incoming radio frequency (RF) signal is first amplified by a low noise amplifier (LNA), then mixed with a pair of quadrature sinusoidal signals to perform the so-called quadrature down conversion in order to get the in-phase (I) and the quadrature (Q) baseband signals. After that, a programmable gain filter/amplifiers (PGA) and an Analog-to-Digital convertor (ADC) are applied to the parallel I and Q branches. After sampling, the discrete time domain signal $r[n]$ is passed through the packet detector, which performs correlation between $s[n]$ and a pre-defined 802.11 preamble pattern to confirm an incoming packet. Because the existence of CFO will seriously degrade the performance of OFDM, once the packet is detected, the CFO is estimated and corrected to minimize the effects of ICI in the later stages. The channel estimator estimates the instantaneous CSI and the subsequent equalization module (not shown) acts as channel corrector to compensate attenuation and phase errors prior to the packet decoding. Note that, the extracted CSI characterizes not only the frequency response of the external wireless channel in passband, but also the frequency response of the inner circuit mainly in baseband.

C. Reported CSI Measurement Error Sources

Since we aim to sense the external environment with CSIs extracted from commodity WiFi NICs, in this paper, all frequency responses of the inner signal processing circuit are regarded as errors. Besides measurement noise, previous studies [4, 7, 8, 9, 10, 14] have reported the sources of CSI measurement errors as follows.

Power amplifier uncertainty (PAU). Due to the resolution limitation of hardware, for example, 0.5dB for Atheros 9380, the total gain achieved from LNA and PGA cannot perfectly compensate the signal amplitude attenuation to the transmitted power level. The measured CSI amplitude equals to the compensated power level, mixed with a power amplifier uncertainty error, which causes a CSI amplitude offset.

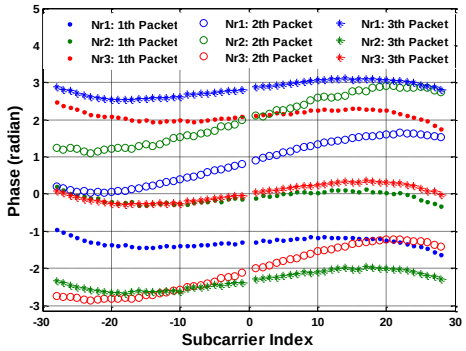

Fig. 3(a). Three groups of unwrapped CSI phases measures for three consecutive packets from strong LOS scenario with Atheros AR9380, with Nr1, Nr2, and Nr3 denoting the first, the second, and the third antenna of the receiver.

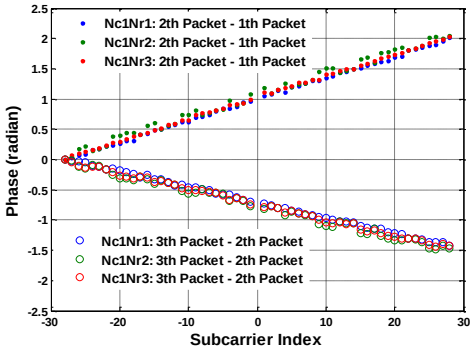

Fig. 3(b). The CSI phase differences of each transmission pair between two consecutive packets, with Nc1Nr1, Nc1Nr2, and Nc1Nr3 denoting transmitting pairs between the first antenna of the transmitter and the first, the second and the third antenna of the receiver, respectively.

Carrier Frequency Offset (CFO). The central frequencies of a transmission pair cannot be perfectly synchronized. The carrier frequency offset is compensated by the CFO corrector of the receiver, but due to the hardware imperfection, the compensation is incomplete. Signal still carries residual errors, which leads to a time-varying CSI phase offset across sub-carriers.

Sampling frequency offset (SFO). The sampling frequencies of the transmitter and the receiver exhibit an offset due to non-synchronized clocks, which can cause the received signal after ADC a time shift with respect to the transmitted signal. Similarly, the sampling frequency offset can be compensated by the SFO corrector of the receiver, but the compensation is incomplete, introducing errors to the CSI phases measured from different sub-carriers. Because clock offsets are relatively stable within a short time (e.g., in the order of minutes [16]), such phase rotation errors are nearly constant. For a large scale of time, time-varying SFO also leads to time-varying phase rotation errors.

Packet detection delay (PDD). Packet detection delay stems from energy detection or correlation detection which occurs in digital processing after down convert and ADC sampling. Packet detection introduces another time shift with respect to the transmitted signal [17, 18], which leads to packet-varying phase rotation error.

PLL Phase Offset (PPO). The phase-locked loop (PLL) is responsible for generating the center frequency for the transmitter and the receiver, starting at random initial phase [8]. As a result, the CSI phase measurement at the receiver is corrupted by an additional phase offset.

Phase ambiguity (PA). When examining the phase difference between two receiving antennas, recent work [10] validates a so called four-way phase ambiguity existence in Intel 5300 when working on 2.4GHz. Generally speaking, if the phase difference between the first receiving antenna and the second antenna should be $\theta \in (0, \pi/2)$, the four-way phase ambiguity can lead the phase difference to be θ, $\theta + \pi/2$, $\theta - \pi/2$ or $\theta - \pi$. As for Atheros 9380, we similarly discover a two-way phase ambiguity. As a result, phase ambiguity will lead to another phase offset.

According to [38], when the channel is stable, CSI amplitude offsets caused by CFO can be largely removed by averaging sufficient number of CSIs in the same band. In this paper, we focus on examine CSI phase errors. From above discussion, the measured CSI phases are distorted with various phase ration errors and/or phase offset errors. For a transmission pair, the phase measurement $\emptyset_{i,k}$ for sub-carrier k in channel i can be expressed as

$$\emptyset_{i,k} = \theta_{i,k} - 2\pi \cdot k \cdot f_s \cdot \delta + \beta + Z \qquad (3)$$

where k ranges from -28 to 28 (index 0 is reserved for carrier frequency) in IEEE 802.11n for 20MHz band width, $\theta_{i,k}$ denotes the true phase, δ is the time offset at the receiver, including time shift due to PDD and SFO, f_s is the sub-carrier spacing between two adjacent sub-carriers (i.e. 312.5KHz), β is the total phase offset, and Z is the additive white Gauss measurement noise. Note that, except for Z, other reported phase errors are linear errors.

III. Empirical Studies on CSI Phase Measurements

In this section, we first briefly describe our experiment testbed. Then we present our observation of obvious non-linear CSI phase measurement errors in real-world LOS indoor environments. Finally, we describe the intensive analysis on the characteristics of the non-linear CSI phase errors.

A. *Experiment Testbed*

Thanks to 802.11n, which defines a channel sounding mechanism where a transmitter can trigger CSI estimation at a receiver by setting an appropriate flag in the transmitted packet [25, 26]. We adopt Atheros AR9380 NICs, which support 802.11n with 20MHz/40MHz channels at the 2.4GHz/5GHz frequency bands and have three antennas on each NIC. In specific, we setup two HP desktops running Linux OS with each installed with an Atheros AR9380 NIC. With the help of an open source software *hostapd*, we configure one Atheros node to acts as AP, denoted as *Nc*, for transmitting packets and the other one as the receiver, denoted as *Nr*, to extract CSI measurements. We also modify the driver of Atheros 9380 so that the receiver can report an estimated CSI to the user space once receiving a packet. Packets in all experiments have the minimum payload (to ensure

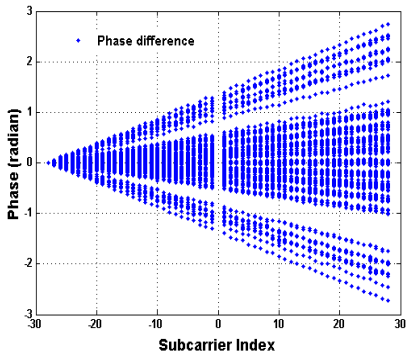

Fig. 4. The phase differences of 100 phase measures, after removing a special phase offset respectively.

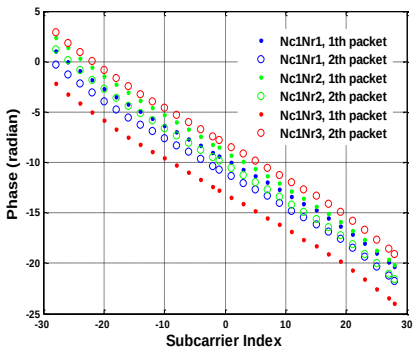

Fig. 5(a). Two groups of unwrapped CSI phase measures for two consecutive packets with 30cm cable between the transmission pair with Intel 5300.

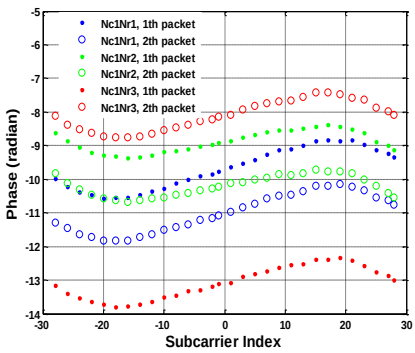

Fig. 5(b). The phase measures after compensating another phase rotation corresponding to a time shift of 200ns .

a short transmission delay, i.e., about 0.2ms in our experiment). When working in a 20MHz band, there are 56 complex numbers in one CSI measurement between one transmission pair, standing for the frequency responses of 56 nonzero sub-carriers out of the 64 available sub-carriers.

B. Identifying Nonliear CSI Phase Errors

We conduct experiments in a typical indoor environment with length and width of the room 12meters and 10meters, respectively. We arrange the transmitter and the receiver in strong line-of-sight (LOS) condition with their distance less than one meter, and make the transmitter to transmit with its first antenna with a fixed transmitting power of 5dBm and the receiver to receive with all of its three antennas. We collect CSIs when the environment is stable.

Figure 3(a) illustrates three groups of unwrapped CSI phase measurements for three consecutive packets, with each group having three CSI measurements obtained from three antennas, respectively. Intuitively, in such strong LOS scenarios, the direct path component rather than multipath components is dominant in the total power of the received signal. According to (2), since the time-of-flight is the same for different sub-carriers and the sub-carrier spacing is fixed at 312.5KHz, the ideal phase on each sub-carrier should be almost linear along with the subcarrier index. Although various CSI phase error sources described above may introduce addictive phase errors, the combined CSI phases should still be linear. We observe, however, obvious non-linear distortions in all unwrapped phase measurements. We repeat such experiment in other indoor environments and get similar results.

To exclude unexpected errors in measuring CSIs, we carefully check whether the environments are stable. According to previous work [3, 9], if the wireless channel is stable, the unwrapped phase differences of two consecutive packets for the same transmission pair are almost linear with the sub-carrier index given the existence of linear errors. After removing the phase offset at sub-carrier -28 from each CSI phase measurement, we calculate the CSI phase differences of each transmission pair between any two consecutive packets using the same CSI measurements used in Figure 3(a) and plot the results in Figure 3(b). It can be clearly seen that the unwrapped phase differences of two consecutive packets for the same transmission pair are almost linear with the sub-carrier index, indicating that the environment is quite stable. In addition, it also suggests that the non-linear CSI phase errors seem to be constant between different measurements. We thus, in this paper, try to answer the following two questions: 1) whether this non-linear CSI phase error is a system error or a random error? 2) what is the key factor that causes such errors?

C. Understanding Properties of Non-linear CSI Phase Errors

To get a deep understanding about the found non-linear CSI phase errors, we conduct a rich set of cable experiments, where the transmitter and the receiver is directly connected via coaxial cables, making a clean, stable and interference-free direct path between the transmission pair.

Non-linear CSI phase errors are non-negligible. In our first experiment (referred to as the basic experiment), we conduct more intensive measurements similar to the experiment present in above subsection to verify that the found non-linear CSI phase errors are not random. In specific, we use a cable of 30cm and an attenuator of 50dB to connect the first radio chains of both the transmitter and the receiver. The transmitter sends 1,000 packets within three seconds each time with a fixed transmission power of 15dBm in a 20MHz band with a central frequency of 2,412MHz. We random select 100 CSI measurements, remove the mean from each CSI phase measurement, and plot the unwrapped CSI phases and the phase differences for any two consecutive phase measures in Figure 1 and Figure 4, respectively.

We can see that the results are similar as in real-world indoor LOS environments, which state that: 1) the envelopes of unwrapped phases are not linear but symmetrical and analogous to some form of trigonometric function; 2) the phase differences of consecutive packets are linear with subcarrier index, which makes one envelope easy to rotate to another. It's reasonable to regard that only one single direct path exists in such scenario. Given that the length of cable is 0.3m, the time-of-flight is about 1ns. With the subcarrier spacing being 312.5KHz, according to (3), the phase slope $\Delta\varphi$, i.e., the phase difference between two adjacent sub-carriers, would be $\Delta\varphi = 2\pi \cdot 312.5/1000000 = 0.0020$rad. If only linear errors across sub-carriers are accumulated, the measured phases would still be linear, which contradicts with our observation. As a result, the default assumption that only notable linear phase error exists cannot

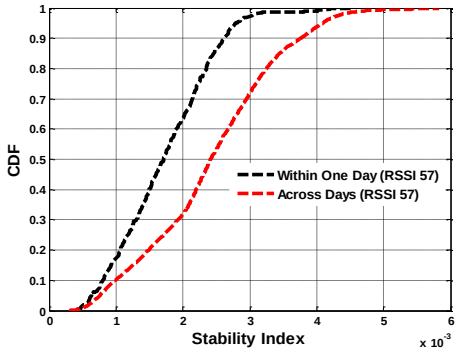

Fig. 6. CDFs of stability index on CSI phase measurments obtained across minutes and across days, respectively.

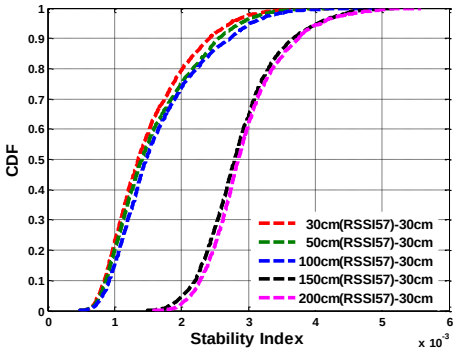

Fig. 7. CDF of stability index with different time-of-flight configurations.

hold and an unrevealed non-linear phase error exists, which cannot be mitigated through existing methods. To make matter worse, obviously this non-linear error is orders-of-magnitude higher than the ground truth phase and thus non-negligible. For example, in Figure 1, the measured CSI phases especially at such sub-carriers near both ends of the channel are severely distorted from the ground truth even after compensating all linear errors. We augment the CSI phase error model as

$$\emptyset_{i,k} = \theta_{i,k} + \varphi_{i,k} - 2\pi \cdot k \cdot f_s \cdot \delta + \beta + Z \qquad (4)$$

where $\varphi_{i,k}$ denotes the non-linear error as a function of the sub-carrier index *k* in channel *i*, with other parameters the same as in (3).

Non-linear CSI phase errors are prevalent among commodity WiFi devices. In this experiment, we examine whether the revealed non-linear CSI phase errors are common among different WiFi devices. We have verified that this non-linear phase error does exist in Atheros 9380/9580 NICs. Moreover, we examine whether the non-linear phase exists in Intel WiFi NIC family. We repeat the basic experiment except that we change the WiFi NICs to Intel 5300 and draw the unwrapped CSI phase measures of two packets in Figure 5(a). At the first glance, it seems that the CSI phases are pretty linear with sub-carrier indexes. According to previous work [27], the packet detection delay can span hundreds of nanoseconds for Intel 5300. After compensating 4 sampling periods, i.e., 200 *ns*, corresponding to the slope of 0.3928, we plot the corrected CSI phases in Figure 5(b). Note that, the phases are still added with residual linear errors. It can be seen that the envelopes of phase measures are similar to Figure 3 (a) and Figure 1.

Non-linear CSI phase errors are temporally stable. From above experiments, it can be seen that the non-linear CSI phase errors are rather stable during a short period time. Furthermore, we observe the unwrapped phase differences between CSIs are almost linear across sub-carriers. On one hand, this implies that the channel condition is stable; on the other hand, it also suggests that the non-linear CSI phase errors across different CSI measurements are also stable so that they can be canceled in the unwrapped phase differences between CSIs. To better quantitatively characterize how stable the non-linear CSI phase errors are, we design a metric, called *stability index* $\mathcal{S}$ between two CSI measurements j_1 and j_2, defined as

$$\mathcal{S}(j_1, j_2) = \left(\sum_{k=-28}^{28} (\Delta\emptyset_{i,k} - \psi_{i,k})^2\right)/56 \qquad (7)$$

where $\Delta\emptyset_{i,k}$ denotes the phase difference between j_1 and j_2 for subcarrier k in channel i, $\psi_{i,k}$ denotes the fitted value corresponding to $\Delta\emptyset_{i,k}$ after conducting a LS linear fitting with all $\Delta\emptyset_{i,k}$. The design of this metric fully utilizes the key insight that, in one single direct path environment, except for the non-linear error, the ground-truth phases and all other phase errors are linear with sub-carrier index. Essentially, the stability index characterizes how well the unwrapped phase differences between CSIs can fit a straight line, with the instinct that a small stability index value reflects a good linear fitting and thus constant non-linear phase errors.

Note that each CSI phase measurement also includes measurement noise, which empirically follows additive Gauss distribution with mean of zero. In order to mitigate the effect of noise, we take the average of 1,000 unwrapped CSI measurements to get one smooth CSI phase measurements. We thereafter use averaged CSI measurements in the following experiments.

In this experiment, we extend the time scale to check whether the non-linear CSI phase errors are stable in a large scale of time in terms of minutes and days with other configuration unchanged. In specific, we conduct the basic experiment and collect CSI measurements for 20 days (including one week after a deliberate reboot of both computers). On each day, we collect trace for 50 groups with each group lasting for 10 minutes. In order to study the stability of non-linear phase errors at minute level, we randomly select two averaged CSIs from the same group in the same day, calculate the stability index between this pair CSIs. We repeat the process for 1,000 times and plot the cumulative distribution functions (CDFs) of stability index values in Figure 6. Similarly, for day level, we randomly select two averaged CSIs from different groups in different days to calculate the stability index, repeat the process for 1,000 times, and plot the cumulative distribution function (CDF) in Figure 6.

It can be seen that the upper-bound variances for minute level and day level are around 0.0044rad and 0.0057rad, respectively, indicating the non-linear CSI phase error is pretty stable at a large scale of time.

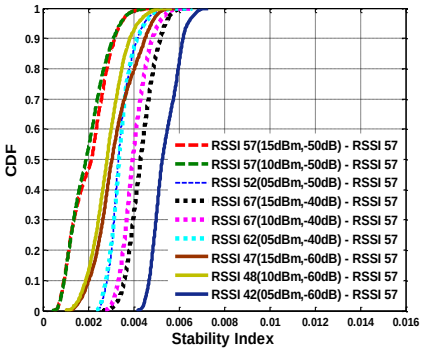

Fig. 8. CDF of stability index for different values of RSSI.

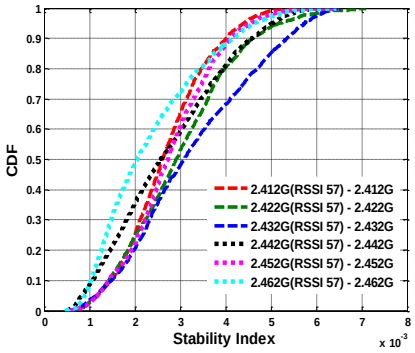

Fig. 9(a). CDF of stability index in the same center frequency.

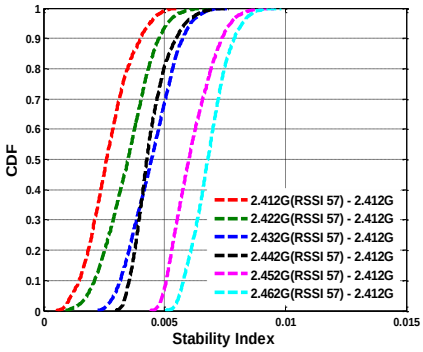

Fig. 9(b). CDF of variances across different center frequencies.

Non-linear CSI phase errors are independent of time-of-flight. Time-of-flight and PDD or SFO all lead to a phase rotation, but they occur at different stages of a signal's lifetime. Specifically, SFO and packet detection delay occurs in digital processing in baseband, introducing unexpected phase rotation errors. In contrast, time-of-flight occurs while the signal is transmitted in passband, leading to expected phase rotation.

In this experiment, we examine the impact of time-of-flight to the non-linear CSI phase errors. We configure the length of cable to be 0.3m, 0.5m, 1m, 1.5m and 2m, respectively and keep other configurations the same as in the basic experiment. As we have RF cables of three lengths, i.e., 0.3m, 0.5m, and 1m, we use a SMA adaptor to connect two short cables to get a cable of 1.5m and 2m, respectively. For each cable length, we conduct the experiment and collect CSI measurements for ten minutes. We randomly select an averaged CSI from the trace of 0.3m and another averaged CSI from the trace of 0.3m, 0.5m, 1m, 1.5m and 2m, respectively to calculate the stability index. For each cable length, we repeat 1,000 times and plot the CDFs of stability index values in Figure 7.

It is clear to see that, despite various time-of-flight values, the distributions of non-linear CSI phase errors are very similar, indicating that non-linear CSI phase errors are independent of time-of-flight. It should also be noted that the CDFs of combined cables are separated from those of original cables. We find that SMA adaptors introduce additional attenuations to the channel, which leads to distinct non-linear CSI phase errors.

Non-linear CSI phase errors are sensitive to the received RSSI. Inspired by the above experiment, in this experiment, we examine whether different RSSI values would affect the non-linear CSI phase errors. We combine different transmission power of 5/10/15dBm and different attenuators of 40/50/60dB connected to a 0.3m cable and conduct the basic experiment. For each combination, we collect a CSI trace for ten minutes. We randomly select an averaged CSI from the trace with 15dBm transmission power and a 50dB attenuator and another averaged CSI from another trace to calculate the stability index. For each power and attenuation combination, we repeat 1,000 times and plot the CDFs of stability index values in Figure 8.

It can be seen that CDFs with close RSSI configurations are very similar, though different combinations of transmission power and attenuation are used. We find that the stability of non-linear error is strongly related to the absolute value of RSSI contained in CSI entry.

Non-linear CSI phase errors are sensitive to the channel center frequency. In order to study whether the non-linear error is dependent with band center frequency, we configure the center frequency to be 2,412MHz, 2,422MHz, 2,432MHz, 2,442MHz, 2,452MHz and 2,462MHz, respectively, and keep other configurations the same as in the basic experiment. For each channel, we collect a CSI trace for ten minutes. We randomly select two averaged CSIs from the same trace to calculate the stability index, repeat this procedure for 1,000 times, and plot the CDFs in Figure 9(a). Moreover, we calculate the stability index values between the 2,412MHz channel and other channels and plot the CDFs in Figure 9(b).

There are two main observations. First, given the same channel center frequency, the non-linear CSI phase errors are constant. Second, non-linear CSI phase errors in different channels are also distinctive. In addition, it seems that the larger the difference between two channel center frequencies is, the less similar between the non-linear CSI phase errors produced in those channels. In conclusion, the non-linear error is sensitive to the channel center frequencies.

Non-linear CSI phase errors are sensitive to the channel center frequency. There are three radio chains for both the transmitter and the receiver. In order to study whether the non-linear phase error is related with a particular transmission pair, we conduct this experiment to collect CSI measurements using different transmission pairs. For Atheros 9380, selecting the second or the third radio chain to work alone is not allowed by the default strategy. However, after the authentication and connection with three working radio chains, Atheros 9380 can change to transmit or receive with any one radio chain for several seconds. For each combination between any of the three transmitter radios and any of the three receiver radios, we collect CSI measurements for ten minutes. We randomly select two averaged CSIs from the trace with the same transmission pair to calculate the stability index, repeat this procedure for 1,000 times, and plot the CDFs in Figure 10(a). Moreover, we calculate the stability index values between different transmission pairs

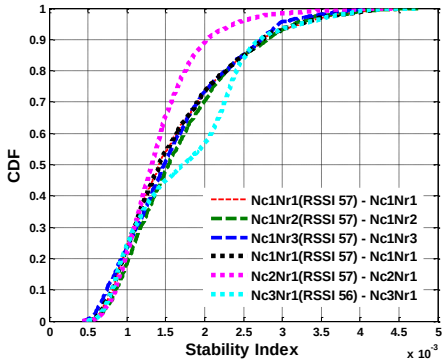

Fig. 10(a). CDF of stability index for the same transmission pair.

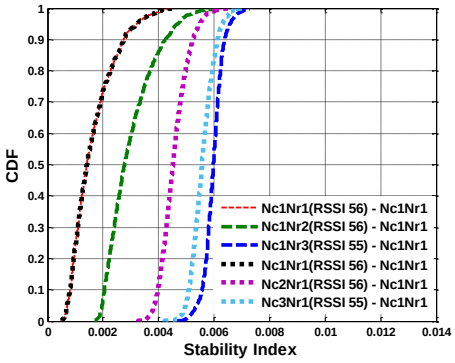

Fig. 10(b). CDF of stability index across different transmission pairs.

and plot the CDFs in Figure 10(b). It can be seen that the non-linear CSI phase errors are constant for the same transmission pair but very sensitive to different transmission pairs. Particularly, even when the same radio chain is used at the receiver side, different radio chains used at the transmitter side also lead to obvious distinction between non-linear phase errors.

IV. Discussion on Root Source

In this section, we discuss the possible root source of the identified non-linear CSI phase error. Recall that commodity WiFi 2.4GHz receivers normally adopt the direct down conversion architecture as shown in Figure 2. According to previous work [28, 29, 30, 31, 32, 33, 34], there is a universal performance-limiting issue, named *IQ imbalance*, in the design of direct down conversion receivers. A direct conversion receiver uses two quadrature sinusoidal signals to perform the so-called quadrature down conversion. This process requires shifting the local oscillator (LO) signal by 90 degrees to produce a quadrature sinusoidal component. When mismatches exist between the gain and phase of the two sinusoidal signals and/or along the two branches of down-conversion mixers, amplifiers, and low-pass filters, the quadrature baseband signals will be corrupted. Once I/Q imbalance exists, after sampling and FFT, the NIC would estimate and report an anamorphic CSI. We would verify the relationship between the IQ imbalance issue and the non-linear CSI phase error.

V. Related Work

A. CSI phase errors

Prior work also notice that the CSI traces reported by WiFi NICs contain phase errors introduced by hardware. Previous work [7, 16] explicitly point out the phase errors caused by SFO, and other studies such as [4, 8, 9, 13, 14, 15, 36] mention phase error cause by SFO. The phase errors caused by packet detection delay are studied by [7, 17, 18, 27], and are mentioned by [8, 9, 13, 14, 15]. The phase errors caused by center frequency offset are mentioned by [7, 8, 9, 14]. The phase error caused by PLL phase offset is point out and studied by [8] in recently. The phase error caused by phase ambiguity is observed and validated in [10] recently. However, all above phase errors are linear with subcarrier indexes. Of course, there is another phase error named measurement noise which follows additive Gauss distribution with mean of zero.

B. CSI phase calibration

As for CSI phase linear error, to the state of art, there are following strategies: [13, 14] recommend to perform a linear transform on the raw CSI phase. After transforming, the mean of a phase measures is forced to zero, and the phase slope between the first subcarrier and last subcarrier is forced to zero too. After the transformation, the CSI phase measure can be used as fingerprint for some applications. However, such a brute transform just adds or subtracts another linear error. [4, 15] search a linear fitting and subtract the fitting linear from the raw CSI phase. However, it's common to over subtraction. MegaMIMO aims to explicitly correct linear phase errors [36]. However, MegaMIMO requires both nanosecond-level synchronization and the access to the raw signal at PHY layer, which are not available on commodity NICs. [9] obtains CSIs from different frequency bands, averages raw CSI phase measures from the same individual frequency band to eliminate the rotation error due to the packet detection delay, and search a rotation to compensate the rotation error due to SFO. However, since it's hard to collect sufficient CSIs within the restriction of strict coherence time, the rotation error levels are without guarantee to be the same. In order to remove random initial phase offset, [8] proposes to collect and process CSIs both from transmitter and receiver for the same instant. However, even if CSIs can be collected at the instant, there is no guarantee for other phase offset errors to be the same. All strategies above are designed for kinds of linear error. They are all based on an assumption that all the notable phase errors except measurement noise are linear.

VI. Conclusion

In this paper, we conduct empirical studies on CSI measurements using two types of commodity WiFi NICs. We identify non-linear CSI phase errors and find such errors are prevalent among both WiFi NICs. In addition, such errors are stable along time and for different time-of-flight but sensitive to the received RSSI, channel frequency, and the specific radios between a transmission pair. We also point out that the IQ imbalance problem is the root source of the identified non-linear CSI phase errors.

REFERENCES

[1] F. Adib and D. Katabi, "See Through Walls with Wi-Fi!" in Proceedings of ACM SIGCOMM, 2013.

[2] L. Sun and S.Sen. WiDraw: Enabling Hands-free Drawing in the Air on Commodity WiFi Devices. In Proc. of ACM MobiCom Conference, 2015.

[3] Z. Zhou, Z. Yang, C. Wu, W. Sun and Y. Liu. LiFi: Line-Of-Sight Identification with WiFi. In Proc. of IEEE INFOCOM, 2014

[4] M. Kotaru, K. Joshi, D. Bharadia and S. Katti. SpotFi: Decimeter Level Localization Using WiFi. In Proc. of ACM SIGCOMM, 2015.

[5] S. Sen, B. Radunovic, R. Choudhury and T. Minka. Spot Localization using PHY Layer Information. In Proc. of ACM MobiSys, 2015.

[6] Z. Zhou, C. Wu, Z. Yang, and Y. Liu. Sensorless Sensing with WiFi. Tsinghua Science and Technology, vol. 20, no. 1, pp. 1–6, 2015

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

[8] D. Vasisht, S. Kumar and D. Katabi. Decimeter-Level Localization with a Single WiFi Access Point. In Proc. of NSDI, 2016

[9] Y. Xie, Z. Li and M. Li. Precise Power Delay Profiling with Commodity WiFi. In Proc. of ACM MobiCom, 2015.

[10] A. Tzur, O. Amrani and A. Wool. Direction Finding of rogue Wi-Fi access points using an off-the-shelf MIMO–OFDM receiver. http://www.sciencedirect.com/science/article/pii/S1874490715000452

[11] C. Han, K. Wu, Y. Wang, and L. Ni. WiFall: Device-free fall detection by wireless networks. InProc. of IEEE INFOCOM, 2014.

[12] Myscript. Myscript stylus app. http://myscript.com/.

[13] S. Sen, B. Radunovic, R. R. Choudhury, and T. Minka. You are Facing the Mona Lisa: Spot Localization using PHY Layer Information. in ACM MobiSys, 2012.

[14] C. Wu, Z. Y,Z. Zhou, K. Qian, Y. Liu and M. Liu. PhaseU: Real-time LOS Identification with WiFi. INFOCOM, 2015.

[15] 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. InProc. of ACM MobiCom, 2014.

[16] 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.

[17] J. Gjengset, G. McPhillips, and K. Jamieson. Arrayphaser:Enabling signal processing on WiFi access points. Proc. Of ACM MobiCom, 2014.

[18] L. He, L. Fu, L. Zheng, Y. Gu, P. Cheng, J. Chen, and J. Pan. Esync: An energy synchronized charging protocol for rechargeable wireless sensor networks. InProc. of ACM MobiHoc, 2014.

[19] G. Wang, Y. Zou, Z. Zhou and L. Ni. We can hear you with Wi-Fi! IEEE Transactions on Mobile Computing, 2016.

[20] D. Tse and P. Vishwanath.Fundamentals of Wireless Communications. Cambridge University Press, 2005.

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

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

[23] http://pdcc.ntu.edu.sg/wands/Atheros/

[24] http://dhalperi.github.io/linux-80211n-csitool/installation.html

[25] IEEE 802.11n-2009 Standard. 2009. http://standards.ieee.org/findstds/standard/802.11n-2009.html.

[26] IEEE 802.11n-2012 Standard. 2012. http://standards.ieee.org/findstds/standard/802.11n-2012.html.

[27] H. Rahul, H. Hassanieh, and D. Katabi. SourceSync: A Distributed Wireless Architecture for Exploiting Sender Diversity. In Proc. Of ACM SIGCOMM, 2010.

[28] K.-Y. Sung and C.-C. Chao. Estimation and compensation of I/Q imbalance in OFDM direct-conversion receivers. IEEE J. Sel. Topics Signal Process., vol. 3, no. 3, pp. 438–453, Jun. 2009.

[29] H. Lin and K. Yamashita. Time domain blind I/Q imbalance compensation based on real-valued filter. IEEE Trans. Wireless Commun., vol. 11, no. 12, pp. 4342–4350, Dec. 2012.

[30] W. Nam, H. Roh, J. Lee, and I. Kang. Blind adaptive I/Q imbalance compensation algorithms for direct-conversion receivers. IEEE Signal Process. Lett., vol. 19, no. 8, pp. 475–478, Aug. 2012.

[31] K. Sung, C. Chao. Estimation and Compensation of I/Q Imbalance in OFDM Direct-Conversion Receivers. IEEE Signal Process Lett., vol. 3, no. 3, June 2009.

[32] L. Anttila and M. Valkama, "Blind signal estimation in widely-linear signal models with fourth-order circularity: Algorithms and application to receiver I/Q calibration," *IEEE Signal Process. Lett.*, vol. 20, no. 3, pp. 221–224, Mar. 2013.

[33] M. Petit and A. Springer. Analysis of a Properness-Based Blind Adaptive IQ. IEEE Wireless Communications, vol. 15,no. 1,January 2016.

[34] https://en.wikipedia.org/wiki/IQ_imbalance

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

[36] H. Rahul, S. Kumar, and D. Katabi. MegaMIMO:Scaling Wireless Capacity with User Demands. InProc. of ACM SIGCOMM, 2012.

[37] J. Han, C. Qian, X. Wang, D. Ma, J. Zhao, P. Zhang, W. Xi,and Z. Jiang. Twins: Device-free object tracking using passive tags. InProc. of IEEE INFOCOM, 2014.

[38] 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.