System Error Calibration in Large Datasets of Wireless Channel Sounding for Industrial Applications

Qi Wang, Richard Candell, *Senior Member, IEEE,* Wei Liang, *Senior Member, IEEE,* Zhibo Pang, *Senior Member, IEEE*

***Abstract*—Channel impulse response (CIR) datasets, which represent the characteristics of wireless channels, play a vital role in industrial applications. Unfortunately, systematic errors have been discovered within CIR datasets. These errors have undesirable effects in wireless localization, physical layer security, and related applications. In addition, existing CIR calibration methods do not consider applicability to industrial scenarios. To address this concern, two channel sounder error calibration (CSEC) methods are proposed. The first CSEC method based on phase compensation (CSEC-Phase) extracts the direct path signal to estimate errors to avoid interference from rich multipath signals for stationary measurements in complex industrial environments. Moreover, to solve the problem of the inability to estimate the CIR error in mobile measurements due to the rapid dynamic change of the channel, a second CSEC method based on carrier frequency recovery (CSEC-Frequency) is proposed that extracts the frequency offset of the system clock to compensate for systematic error utilizing the stability of clock drift. Furthermore, the L1-norm distance metric is employed to measure the differences between CIRs and evaluate the calibration performance. Our results reveal that the proposed CSEC methods are effective on diverse CIR datasets measured by different equipment in different scenarios.**

***Index Terms*—wireless channel sounding, channel impulse response calibration, synchronization, NIST dataset, physical layer authentication.**

I. Introduction

WIRELESS communication is a critical technology for industrial cyber-physical systems due to its low cost, ease of scaling, and flexibility arising from the lack of need for cables [1]. However, industrial wireless communication faces various challenges, including requirements of low latency, high reliability, and high security. In typical industrial environments, which contain many metal objects, large machinery, and rotating parts, a channel experiences fast temporal fading due to the rich multipaths [2], [3]. Moreover, mobile equipment, a killer application in industrial scenarios, induces rapid spatial variations in the channel [4]. Therefore, wireless communication systems designed for general office and home scenarios may not be applicable in industrial scenarios. The design of industrial wireless communication systems requires a precise understanding of the nature of industrial wireless channels.

The channel impulse response (CIR) represents the change in a transmitted signal after it traverses a channel. The CIR can be employed as channel state information (CSI) to address a large number of issues relevant to industrial applications, such as wireless localization and physical layer security [5]–[10]. Research on these industrial applications can be facilitated by high-accuracy CIR data.

To meet the needs of CIR measurements, channel sounder systems have been developed, and several CIR datasets measured by different researchers are currently available [11], [12]. Despite the use of high-precision equipment and careful synchronization of the transmitter and receiver, carrier frequency offset and record clock glitch, which are two types of systematic error, are found in CIR datasets, such as the National Institute of Standards and Technology (NIST) CIR reference dataset [11] and a CIR dataset measured by the University of Utah [12]. These two types of error are naturally introduced due to clock drift and cart vibration [11], as even high-performance channel sounder systems may not be completely free of errors.

For traditional wireless digital receiver systems, many synchronization algorithms have been proposed to eliminate the time and frequency offsets introduced by receiver systems and wireless channels [13]–[17]. However, the influence of a wireless channel on signal propagation is meaningful information for corresponding CIR measurements. Therefore, we need to retain channel information while eliminating only the errors introduced by a measurement system. Channel sounder systematic error calibration is needed to improve the accuracy of CIR data and the fidelity of subsequent analyses using CIR datasets.

A few methods have been proposed for calibrating channel sounder systematic errors in CIR data. One method relies

Qi Wang is with the State Key Laboratory of Robotics and Key Laboratory of Networked Control Systems, Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang 110016, China, and with Institutes for Robotics and Intelligent Manufacturing, Chinese Academy of Sciences, Shenyang 110169, China, and also with the University of Chinese Academy of Sciences, Beijing 100049, China (e-mail: wangqi@sia.cn).

Richard Candell is with the Intelligent Systems Division, National Institute of Standards and Technology, Gaithersburg, MD, 20899 USA (e-mail: richard.candell@nist.gov).

Wei Liang is with the State Key Laboratory of Robotics and Key Laboratory of Networked Control Systems, Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang 110016, China, and with Institutes for Robotics and Intelligent Manufacturing, Chinese Academy of Sciences, Shenyang 110169, China (e-mail: weiliang@sia.cn).

Zhibo Pang is with the ABB AB, Corporate Research, Forskargränd 7, 72178, Västerås, Västmanland Sweden (e-mail: zhibo@kth.se).

Corresponding author: Wei Liang

The MATLAB code of the CSEC methods has been shared on GitHub: https://github.com/QiWang-GH/Industrial-Wireless-Channel-Sounding-Error-Calibration-IW-CSEC.

on the conjugate multiplication of the CIRs of a pair of antennas, as all antennas on the same receiver have the same system effects [18], [19]. However, this method requires no less than two antennas. A linear transformation can be utilized in a single-antenna receiver system [20], [21]. However, these methods do not consider the complex and dynamic environments in industrial scenarios. To achieve the applicability of a calibration method to industrial scenarios, the following challenges need to be addressed: (1) How can stable CIR errors be extracted under disturbances caused by rich multipath signals in complex industrial environments? (2) How can CIR calibration be achieved for fast-changing dynamic channels in a mobile equipment application scenario? (3) How can the high time delay requirements in industrial applications be met?

In this paper, we focus on channel sounder error calibration of the CIR for industrial scenarios. The main contributions are as follows:

- We propose a channel sounder error calibration method based on phase compensation (CSEC-Phase) for stationary CIR measurements. This proposed method extracts CIR errors from the direct path due to its relative stability in dynamic channels and employs the L1-norm distance as a metric to measure the differences in CIRs since this metric can highlight strong multipath signal features. This proposed method achieves better performance than the linear transformation in complex industrial wireless environments. This proposed method can be solved by one-dimensional searches and therefore does not increase the complexity compared with existing methods, which confirms that it is applicable in practical systems as a runtime operation.
- We propose a channel sounder error calibration method based on frequency recovery (CSEC-Frequency) for mobile CIR measurements. This proposed method is validated on mobile measurements by compensating for the fixed carrier frequency offset of the channel sounder system based on the pattern of clock drift. Without increasing the algorithm complexity, this proposed method extends the CIR error calibration from stationary to mobile measurements, which avoids the interference caused by the fast-changing dynamic channels.

It is valuable to mention that the proposed methods are validated using diverse CIR datasets measured by different equipment in different scenarios. Moreover, a case study of physical layer authentication confirms the positive impact of the CSEC method in a real-world application scenario.

The remainder of this paper is organized as follows: Section II summarizes related works. Section III briefly introduces the NIST reference dataset. Section IV analyzes the two types of systematic errors in detail. Section V models the systematic errors. Section VI describes the CSEC scheme. Section VII presents the simulation results and introduces an application case of CSEC. The paper is concluded in Section VIII.

II. Related works

In this section, we briefly review the most relevant works on two categories of synchronization algorithms: synchronization for demodulation of received signals and calibration for acquisition of CIRs.

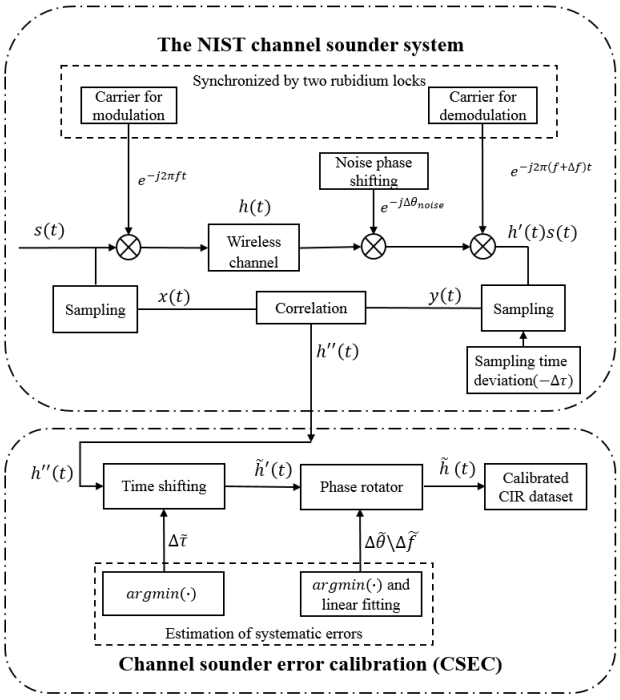


Fig. 1. System overview.

Synchronization for demodulation of received signals. Timing and frequency synchronization methods for demodulation of received signals in traditional wireless communication systems have long been established. In orthogonal frequency division multiplexing (OFDM) systems, Schmidl and Cox's method uses two consecutive differentially encoded training sequences at the beginning of a radio frame to estimate the frequency offset [13]. For satellite systems, there is an algorithm that utilizes the symmetric properties of Zadoff-Chu sequences to eliminate the frequency offset and determine the transmission delay [14]. To reduce the need for training sequences, a joint maximum likelihood (ML) time and frequency offset estimator has been proposed for OFDM systems [15]. This joint ML estimator involves a high-complexity bidimensional grid search, which is replaced with a simpler mono-dimensional search suitable for practical implementation [16]. However, time and frequency recovery is performed to demodulate the received signal from interference caused by time delays and phase shifts. The synchronizer cannot distinguish between phase shifts introduced by channel effects and those introduced by carrier frequency offsets [17], although the former is meaningful information for the CIR.

Calibration for acquisition of CIRs. CIR-based applications have attracted increasing attention in recent years since CIR data can represent fine-grained channel sounding features. Similar to their influence on synchronization for demodulation of received signals, phase shifts will reduce the performance in wireless localization, physical layer security, and other related applications. However, the purpose of calibration methods proposed for CIR data is to acquire information that can

describe channel states while eliminating systematic errors introduced due to clock drift. A few methods have been proposed for calibrating systematic errors in CIR data. A calibration method has been proposed for wireless localization based on the averaging of continuous CIRs, which is a simple method of extracting channel features that cannot eliminate systematic errors [6]. Meaningful CIR phase information can be preliminarily derived by employing a linear transformation [20], [21]. The linear transformation method can yield a usable estimation of the true phase; however, the extracted phase features are coarse, and this method is not suitable for industrial applications. For a multiple-antenna system, the conjugate multiplication of the CIRs of a pair of antennas can be used to eliminate the phase offset, since all antennas on the same receiver experience the same phase offset introduced by the channel sounder system [18], [19]. These methods do not consider the complex conditions in industrial environments.

III. Channel Sounding Dataset Measured by NIST

To clearly illustrate the phenomenon of channel sounder systematic errors, the NIST CIR reference dataset is taken as an example in this paper. The NIST channel sounding measurements have been processed and improved to acquire CIR data for multiple real industrial scenarios [11], yielding a CIR reference dataset. One of thses industrial scenarios, a steam plant, is shown in Fig. 2. In this section, this dataset is briefly introduced to support the motivations for the methods proposed in this paper.

Fig. 2. Example of an industrial scenario: a steam plant [11].

Channel Sounder System. The channel sounder system used in the NIST measurements was based on pseudo noise (PN) sequence correlation. The channel sounder system included a signal transmitter (Tx), a signal receiver (Rx), and a controller. The Rx and Tx were not connected by cables for synchronization, meaning that the Rx could be freely moved during the measurement process.

Measured Data. The channel sounder collected complex characteristics of the CIR in the time domain, retaining not only the time domain characteristics but also the amplitude and phase characteristics of the channel. The channel sounder controller performed correlation processing to obtain a CIR after Rx and Tx signal sampling [11], as shown in Fig. 1. $h(t)$ is the real CIR of the channel at time t, i.e., the real CSI. After demodulation, let $h^{'}(t)$ denote the CIR with carrier frequency offset. $h^{''}(t)$ denotes the CIR measured by the channel sounder, i.e., the measured CSI, which carries carrier frequency offset and record clock glitch. $h^{''}(t)$ is calculated by the correlation processing formula $h^{''}(t) = x(t)^{-1}y(t)$, where $x(t)$ denotes the samples of the PN sequence $s(t)$ transmitted by Tx and $y(t)$ denotes the samples of the distorted signal received by Rx. The CIR can be used to characterize the multipath fading of a channel in terms of the amplitude and phase:

$$h(t,\tau) = \sum_{i=1}^{p(t)} |c_i(t)|e^{-j\theta_i(t)}\delta(\tau - \tau_i(t)), \tag{1}$$

where $c_i(t)$, $\theta_i(t)$, and $\tau_i(t)$ denote the amplitude, phase, and delay, respectively, of the $i-th$ multipath component. Here, $i = 1, 2, ..., p(t)$, where $p(t)$ is the total number of multipath components. τ denotes the delay, and δ is the Dirac function. The specific parameters of the NIST measurements are listed in Table I.

TABLE I
Specific parameters of the NIST measurements [11]

Parameter	Value
Carrier frequency (f)	2.245 GHz
Sampling frequency (f_s)	200 MHz
CIR Sampling Interval (T_s)	5 ns
Capture time of a CIR ($T_{capture}$)	40.94 μs
Interval time between CIRs ($T_{interval}$)	20.47 ms
Acquisition time of a channel ($T_{acquire}$)	0.8188 s
Allan variance of a rubidium clock	2×10^{-11} at one second
20 year stability of a rubidium clock	less than 0.005 ppm

Synchronization. The Rx and Tx of the channel sounder system achieved clock synchronization by means of two rubidium clocks, which were synchronized for 72 hours before measurement. The specific synchronization method is described in [11]. To avoid additional synchronization algorithms removing the channel effects, Rx performs no channel correction, and only synchronization hardware using rubidium clocks is involved.

Postprocessing. Following data acquisition by the channel sounder system, postprocessing was conducted to reject CIR data with excessive drift. During the measurement process, power delay profile (PDP) images of the CIRs were displayed on the desktop terminal of Tx. The PDP calculation formula is given as follows:

$$PDP(\tau) = |h(\tau)|^2. \tag{2}$$

The sampling time of the PDP peaks of the CIRs should be kept within an error of one CIR Sampling Interval. Any greater drift indicates poor synchronization between two rubidium clocks or excessive timing drift in the timing distribution circuits.

IV. Causes and Consequences of Systematic Errors

In the NIST dataset, two types of systematic error phenomena exist: 1) carrier frequency offset and 2) record clock glitch. The causes and consequences of these systematic errors are introduced in this section.

A. Introduction of the CIRs in a measurement

In this paper, a channel is a wireless signal propagation environment, which will change if the location of TX or RX changes. The interval between successive measurements (20.47 ms) is short enough to be consistent with the channel coherence time. The direct path signal is the signal component traversing the straight line between Tx and Rx, which corresponds to the earliest rise component of the PDP. This signal always exists and is more stable than the signals along other reflected paths [26], as shown in Fig. 3. Hence, in theory, two measurements for spatially coincident channels should produce CIRs with minor random differences in the direct path signal as long as there is no the movement of humans or objects appearing at the straight line location of Rx and Tx during the measurements.

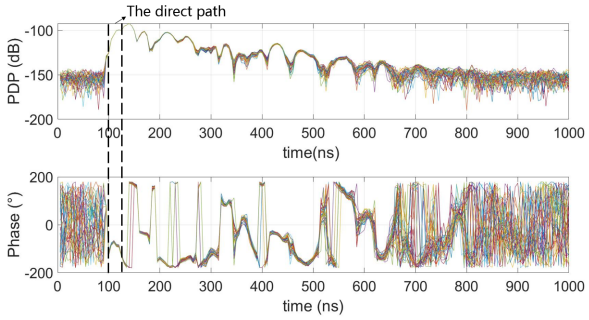


Fig. 3. PDP and phase characteristics of CIRs over time. Forty CIRs are represented.

B. Phenomenon of Carrier Frequency Offset

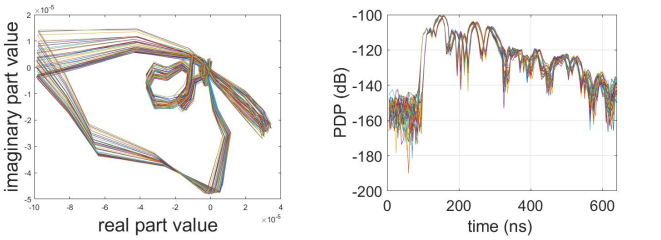
As previously explained, multiple measurements of the same channel should yield similar CIRs or the CIRs having similar direct path signals. Unfortunately, in reality, although the measured CIR characteristics are similar, a small rotation effect is observed among different CIR measurements on the same channel, as shown in Fig. 4(a). This rotation effect can be understood as a phase shift among different CIR measurements.

As shown in Fig. 5, for the sample that corresponds to the direct path of CIR data, the phase shift (°) between each measured CIR and the first CIR of the channel linearly increases with time. We can infer that this phase shift phenomenon is caused mainly by carrier frequency offset $\triangle f$ in the channel sounder hardware between Tx and Rx, as shown in Fig. 1.

C. Phenomenon of Record Clock Glitch

The PDPs of the CIR direct path signals of the same channel should be at least similar, but there are some varying lags between the sample PDPs, as shown in Fig. 4(b). Moreover, the possible values of this lag are different for each measurement. This lag phenomenon is referred to as record clock glitch in this paper.

As described in Section III, CIR data with an error of more than one CIR Sampling Interval may be excessive timing drift, i.e., sampling time deviation $\triangle \tau$, as shown in Fig. 1.



(a) Phase shift phenomenon. (b) Record clock glitch phenomenon.

Fig. 4. Channel sounder systematic error phenomena among CIRs from multiple measurements on the same channel. Forty CIR measurements are represented.

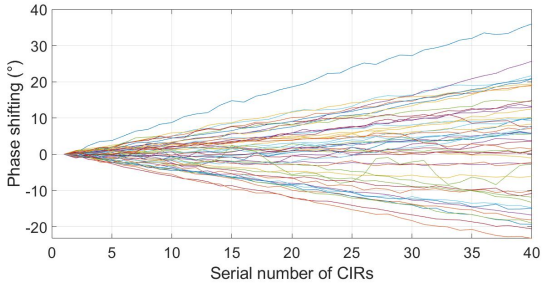


Fig. 5. Carrier frequency offset phenomenon. Each line represents a channel. Forty-nine channels are represented

D. Examples of Consequences

A critical application of the CIR is to research issues associated with the CSI in industrial applications, which include wireless localization, physical layer security, and performance simulation and deep optimization. In this subsection, we illustrate some of the consequences of systematic errors in the CIR for these typical CSI-based applications.

1) Wireless Localization: In [23], a new indoor position localization system (IPLS) method based on information fusion, "Fuse LOC", was proposed. By extracting the amplitude and phase information from the CSI, Fuse LOC can predict the position of an unknown object by comparing the CSI of known and unknown objects. Moreover, an IPLS algorithm was proposed to obtain stable CSI features through noise and interference elimination. The IPLS performs position matching by comparing the differences between CIRs corresponding to different positions [6]. The accuracy of the IPLS may be affected if there are systematic errors in the CSI.

2) Physical Layer Security: Channel security and reliability are reduced in the case of incomplete CSI data affected by channel estimation error [7]. A threshold-based physical layer authentication method using the CSI differences between two locations was proposed in [8]. The accuracy of the CSI affects the calculation of these CSI differences. A machine learning method was proposed in [9], in which CSI models were trained to ascertain the authenticity of user access in different locations. In this approach, the accuracy of the CSI affects the accuracy of the CSI-based authentication model. The authors of [25] combined the threshold method with machine learning to authenticate the identities of users seeking access. In this

method, the authentication accuracy is also reduced due to incomplete CSI data.

3) Performance Simulation and Deep Optimization: The results of channel sounding are often employed in simulations to assess the performance of a physical layer design. Deep optimization has been investigated for adaptation to stringent industrial requirements. One example of this optimization is the delay optimization method based on the channel characterization (CCDO) proposed in [10]. The CCDO method was proposed to minimize the packet transmission time under reliability constraints. For small latencies on the order of microseconds, small characteristic errors may affect the performance of such an optimization method; hence, accurate sounding measurements are required.

V. Error Modeling and Constraints

In this section, we model the two systematic errors introduced in Section IV and investigate the relevant constraints. The capture time for one CIR measurement is 40.94 μs, which is substantially smaller than the time interval between CIR records (20.47 ms). We therefore assume that the effect of the carrier frequency offset during a single CIR measurement is negligible. Hence, we consider only systematic errors between CIRs.

A. Error Modeling

The L1-norm distance metric is employed to measure the differences between CIRs in this paper, as this metric can highlight the strong multipath signal features of a CIR [27], [28]. In an industrial environment, strong multipath signals are the most important and stable components affecting a CIR. The difference between two CIRs measured on the same channel can be assessed in terms of the L1-norm distance D as follows:

$$D(t) = \|h(t) - h(t_0)\|_1, \tag{3}$$

where $\|\cdot\|_1$ denotes the L1-norm and t_0 is the start time of a CIR measurement. In this paper, the first CIR $h(t_0)$ for a channel is treated as the reference CIR to obtain highly consistent CIR data on the same channel. When two CIRs belong to the same channel, $D(t)$ should ideally be near 0.

1) Carrier Frequency Offset: During the measurement process, a carrier frequency offset is first introduced by demodulation, as shown in Fig. 1. We analyze the carrier frequency offset based on the phase shift. The relationship between the frequency offset and the phase shift is expressed as follows:

$$\triangle\theta(t) = 2\pi\triangle f(t - t_0) + \triangle\theta_{noise}, \tag{4}$$

where $\triangle\theta(t)$ is the phase shift, $\triangle f$ is the carrier frequency offset, and $\triangle\theta_{noise}$ is the phase shift caused by noise in the equipment and environment. $\triangle\theta(t)$ will accumulate over time.

From (1), we can deduce the expression for the CIR with carrier frequency offset $h^{'}(t,\tau)$ as follows:

$$h^{'}(t,\tau) = \sum_{i=1}^{p(t)} |c_i(t)| e^{-j(\theta_i(t)+\triangle\theta(t))}\delta(\tau - \tau_i(t)). \tag{5}$$

2) Record Clock Glitch: Following the processing illustrated in Fig. 1, the record clock glitch phenomenon occurs during sampling after demodulation. The expression for the measured CIR $h^{''}(t,\tau)$ with the carrier frequency offset and the record clock glitch is given as follows:

$$h^{''}(t,\tau) = \sum_{i=1}^{p(t)} |c_i(t)| e^{-j(\theta_i(t)+\triangle\theta(t))}\delta(\tau - \tau_i - \triangle\tau(t)), \tag{6}$$

where $\triangle\tau(t)$ is the record clock glitch time.

B. Constraints on the Carrier Frequency Offset

Three constraints on the carrier frequency offset are calculated based on the channel sounder system performance as follows.

1) Upper Bound: During measurement, the received signal is sampled by an analog-to-digital converter (ADC), as shown in Fig. 1. The CIR Sampling Interval T_s determined by the ADC is the maximum error time for the carrier frequency offset, as described in Section II. Thus, the upper bound on the carrier frequency offset $\triangle f_{upper}$ introduced by the ADC can be calculated as follows:

$$\triangle f_{upper} = \pm f \frac{T_s}{T_{acquire}}. \tag{7}$$

where f is the carrier frequency and $T_{acquire}$ is the acquisition time of a channel, as listed in Table I.

2) Long-term Stability Bound: The long-term stability of a rubidium clock is 0.005 parts per million (ppm) over 20 years, as shown in Table I. Accordingly, we can obtain the long-term stability bound $\triangle f_{long}$ on the carrier frequency offset as follows:

$$\triangle f_{long} = \pm f \times 0.005 \times 10^{-6}. \tag{8}$$

3) Allan Variance: The Allan variance of a rubidium clock is 2×10^{-11} at one second in the channel sounder. Based on the Allan variance, we can compute the variance of the carrier frequency offset $\triangle f^2_{Allan}$ as follows:

$$\triangle f^2_{Allan} = f \times 2 \times 10^{-11}. \tag{9}$$

The values of the constraints on the carrier frequency offset in the NIST reference dataset are shown in Table II.

TABLE II
Constraints on the Carrier Frequency Offset

Constraint	Value
Upper bound ($\triangle f_{upper}$)	$\pm$13.709 Hz
Long-term stability bound ($\triangle f_{upper}$)	$\pm$11.225 Hz
Allan variance ($\triangle f^2_{Allan}$)	0.045 Hz

Our goal is to estimate the values of $\triangle\tau$ and $\triangle\theta$ under the relevant constraints and then compensate for the errors in the CIRs.

VI. Methods of System Error Calibration

To estimate and remove systematic errors from CIR data, i.e., calibrate CIR measurements, a CSEC approach is proposed. We assume that the direct path could be characterized and with no moving obstacles. Under this condition,

interference from multipath reflections or relative changes in the environment can be avoided even in an industrial environment. First, the direct path of the CIR is extracted to estimate the systematic errors. Second, the record clock glitch is estimated and compensated. Last, the carrier frequency offset is estimated and compensated. The CSEC process is shown in Fig. 1.

A. Estimation of Record Clock Glitch

In accordance with the principle that the error introduced latest should be eliminated first, we should eliminate the record clock glitch first, as shown in Fig. 1. Considering the influence of random noise, $D(t)$ cannot be 0 in practice; instead, we estimate the record clock glitch using the optimization algorithm. The record clock glitch satisfies the following formula, deduced from (5) and (6):

$$\min_{\triangle\tau(t)} \quad \|h^{''}(t,\tau+\triangle\tau(t))-h^{'}(t_0,\tau)\|_1. \tag{10}$$

During the error estimation process, the CIR difference caused by the carrier frequency offset is the distance between the direct path before and after the phase shift. The CIR difference caused by the record clock glitch introduces the distance of the direct path and the next reflection path. Hence, the CIR difference caused by the record clock glitch is substantially greater than that caused by the carrier frequency offset, and the existence of a carrier frequency offset will not affect the estimation of the record clock glitch. Therefore, $h^{'}(t_0,\tau)$ can be approximately replaced by $h(t_0,\tau)$ in (10). Then, the optimization estimation formula for the record clock glitch is:

$$\min_{\triangle\tau(t)} \quad \|h^{''}(t,\tau+\triangle\tau(t))-h(t_0,\tau)\|_1. \tag{11}$$

Let $\triangle\tilde{\tau}(t)$ denote the estimated record clock glitch, which is calculated via a monodimensional search, as expressed in (11). Once the step size of $\triangle\tau(t)$ is determined, the number of search steps is equal to the range of $\triangle\tau(t)$ divided by the step size. Hence, the time complexity of the optimization estimation of $\triangle\tau(t)$ is $O(1)$. When the size of the CIR dataset is N, the time complexity of calibrating the record clock glitch of the dataset is $O(N)$.

B. Compensation of Record Clock Glitch

The record clock glitch phenomenon corresponds to a translation in time between two CIRs; thus, the record clock glitch can be compensated through reverse shifting of the sampling time. This time shift is performed as follows:

$$\tilde{h}^{'}(t,\tau)=h^{''}(t,\tau+\triangle\tilde{\tau}(t)). \tag{12}$$

We introduce $\triangle\tilde{\tau(t)}$ to the time shift to obtain the calibrated $h^{'}(t,\tau)$, i.e., $\tilde{h}^{'}(t,\tau)$.

C. Estimation of Carrier Frequency Offset

After compensating for the record clock glitch, we need to remove the carrier frequency offset, as shown in Fig. 1. We can estimate the phase shift by analyzing the CIRs, and then, the carrier frequency offset can be extracted by fitting the phase shift of CIRs on the same channel.

1) Phase Shift: Inspired by the data preprocessing for localization presented in paper [24], the optimization formula for the phase shift can be deduced from (1) and (5) as follows:

$$\min_{\triangle\theta(t)} \quad \|\tilde{h}^{'}(t,\tau)e^{j\triangle\theta(t)}-h(t_0,\tau)\|_1 \tag{13}$$

$$\text{s.t.} \quad \triangle\theta(t)\le 2\pi\triangle f_{long}(t-t_0), \tag{14}$$

$$\triangle\theta(t)\le 2\pi\triangle f_{upper}(t-t_0), \tag{15}$$

$$\sigma^2(\triangle\theta(t))\le\triangle f_{Allan}^2, \tag{16}$$

where we assume that noise is small enough to be negligible, and constraints (14), (15), and (16) are obtained from Section V-B. $\sigma^2(\triangle\theta(t))$ denotes the variance in $\triangle\theta(t)$. Let $\triangle\tilde{\theta}(t)$ denote the estimated phase shift including the phase caused by the carrier frequency offset $\triangle f$ as follows:

$$\triangle\tilde{\theta}(t)=2\pi\triangle f(t-t_0). \tag{17}$$

Similar to the time complexity of the estimation of the record clock glitch, the time complexity of the optimization estimation of $\triangle\theta(t)$ is also $O(1)$ for a CIR and $O(N)$ when the size of the CIR dataset is N.

2) Carrier Frequency Offset: The relationship between the carrier frequency offset and the phase shift is assumed to be linear, as shown in Fig. 5. Therefore, linear fitting is chosen to extract the carrier frequency offset as follows:

$$\triangle\tilde{f}=\frac{\triangle\tilde{\theta}(t_e)-\triangle\tilde{\theta}(t_0)}{2\pi(t_e-t_0)}, \tag{18}$$

where t_e is the end time of a channel measurement. $\triangle\tilde{f}$ is the slope of the linear fit, and its physical meaning is the estimated carrier frequency offset. $\triangle\tilde{\theta}_0$ is the intercept of the linear fit, and its physical meaning is the estimated initial phase shift of the channel sounder system.

D. Compensation for Carrier Frequency Offset

Two types of methods for carrier frequency recovery are proposed in this paper. One method is CSEC based on the phase shift (CSEC-Phase), and the other method is CSEC based on the carrier frequency offset (CSEC-Frequency).

1) CSEC-Phase: The CSEC-Phase method compensates for the carrier frequency offset by phase rotation for all kinds of phase shifts caused by the carrier frequency offset and phase instability in the CIR at time t. The phase rotator expression for CSEC-Phase is as follows:

$$\tilde{h}(t,\tau)=\tilde{h}^{'}(t,\tau)e^{j\triangle\tilde{\theta}(t)}. \tag{19}$$

2) CSEC-Frequency: The CSEC-Frequency method performs phase rotation only for the phase shift caused by the carrier frequency offset estimated by the start and end CIR of a channel measurement. The phase rotator expression for CSEC-Frequency is as follows:

$$\tilde{h}(t,\tau)=\tilde{h}^{'}(t,\tau)e^{j2\pi\triangle\tilde{f}(t-t_0)}. \tag{20}$$

The carrier frequency offset of the channel sounder is stable over a period of time that is substantially longer than the duration of a CIR measurement. As long as we estimate the carrier frequency offset before moving, CSEC-Frequency can be applied in mobile scenarios.

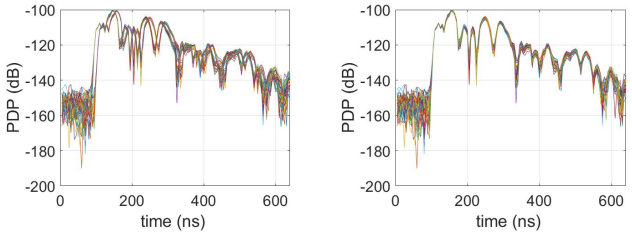
Finally, we obtain the calibrated CIR, i.e., $\tilde{h}(t,\tau)$, through the phase rotator.

VII. Results

In this section, we evaluate the proposed CSEC methods by comparison with the linear transformation method [20] in stationary and mobile industrial scenarios. The CSEC calibration results of the Utah CIR dataset and a CIR dataset measured using our experimental platform are also shown. Finally, a case of applying CSEC-Phase for physical layer authentication is presented.

A. Record Clock Glitch Compensation via CSEC for the NIST CIR Dataset

We can see that the record clock glitch phenomenon is present in the original CIRs, as shown in Fig. 6(a). The PDP of the CIRs after calibration is shown in Fig. 6(b). There is higher consistency among the CIRs after compensation.



(a) PDP of the original CIRs. (b) PDP after CSEC

Fig. 6. Record clock glitch calibration effect on the NIST CIR dataset.

B. Carrier Frequency Offset Compensation via CSEC for the NIST CIR Dataset

After compensation for the record clock glitch phenomenon, estimation of and compensation for carrier frequency offset are carried out. The carrier frequency offsets in the original CIRs are shown in Fig. 8(a). The rotation effect is decreased by the linear transformation method, as shown in Fig. 8(b). After CSEC methods, an obvious rotation effect among the CIRs does not exist, as shown in Fig. 8(c) and Fig. 8(d). Both CSEC methods show better performance than the linear transformation method. Moreover, the effect of the CSEC-Phase is better than that of CSEC-Frequency compensating only for the phase shift caused by the carrier frequency offset, whereas CSEC-Phase compensates for all kinds of phase shifts.

We estimate the carrier frequency offsets of 49 channels, as shown in Fig. 7. The estimated carrier frequency offsets do not exceed the upper bound (13.7 Hz) or the long-term stability bound (11.2 Hz). Moreover, the values are similar to the variance of the carrier frequency offset (0.045 Hz). The values of the constraints are shown in Table II.

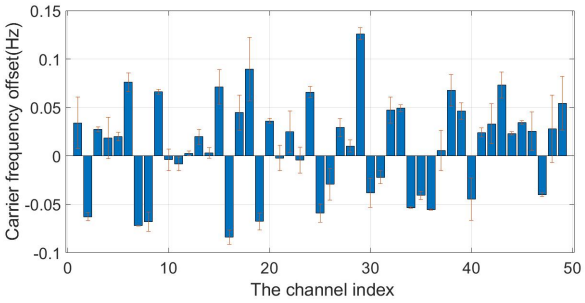


Fig. 7. Carrier frequency offsets of 49 channels. The standard deviations of the carrier frequency offsets are marked in the form of error bars.

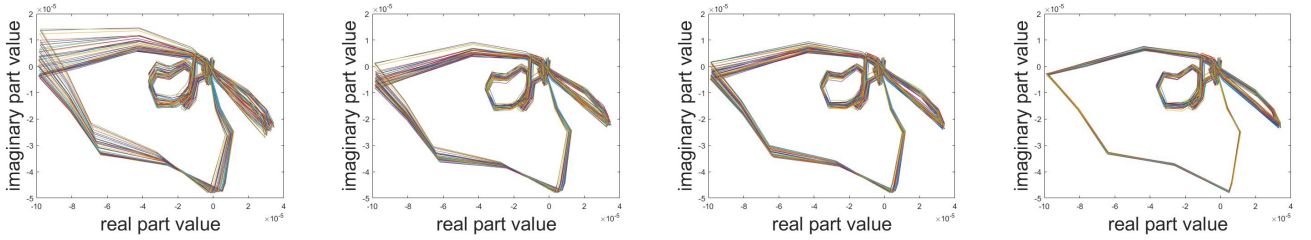
C. Assessment of CSEC on Industrial CIR Datasets

To assess the effect of the CSEC methods, we choose the NIST CIR dataset, which was measured in an industrial environment at fixed locations. To simultaneously compare the performance of different methods, the L1-norm distance is normalized to evaluate the effectiveness of calibration. The linear transformation method [20], CSEC-Frequency, and CSEC-Phase are compared in the evaluation. The effects of the three methods are shown in Fig. 9. The normalized L1-norm distance of the original CIRs accumulates over time, as shown in Fig. 9(a), because the phase shift accumulates over time due to the carrier frequency offset. With CSEC-Frequency and CSEC-Phase methods, the normalized L1-norm distance does not increase over time, although there are random fluctuations within a certain range close to 0. Both of the proposed CSEC methods have better calibration effects than the linear transformation method, as shown in Fig. 9(a), because the phase compensation of the linear transformation method is simply an end-to-end transformation, as shown in Fig. 9(b). By contrast, CSEC-Phase compensates for all kinds of phase shifts, while CSEC-Frequency compensates for the phase shift due to the carrier frequency offset through linear fitting, as shown in Fig. 9(b).

We also verify the calibration effect of the CSEC methods on two CIR datasets from different industrial environments. The first CIR dataset was measured in the Automotive Assembly Plant (AAP), which is an automotive assembly factory. This factory contains many metal and mobile devices, which provide a rich multipath dynamic industrial environment. The second CIR dataset was measured in an industrial steam generation plant containing large machinery, such as boilers, which provides a rich multipath industrial environment. As shown in Fig. 10, CSEC-Phase is suitable for both industrial environments.

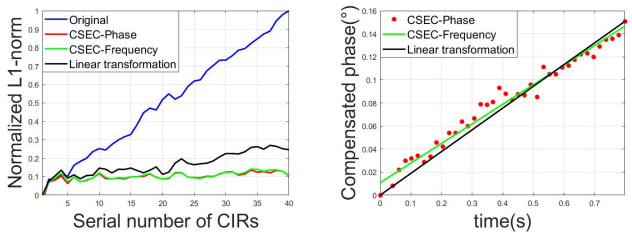
D. Applicability of CSEC-Frequency to Mobile Measurements

NIST conducted stationary and mobile measurements in the AAP. Before a mobile measurement is performed, the channel sounder acquires the CIRs for a while at an initial fixed location. As described in the CSEC-Frequency method, these initial CIRs are used to estimate the frequency offset of clocks, and then, the estimated frequency offset is used to calibrate CIRs from mobile measurements.



(a) Original CIRs. (b) CIRs after linear transformation (c) CIRs after CSEC-Phase (d) CIRs after CSEC-Frequency

Fig. 8. Carrier frequency offset calibration effect on the NIST CIR dataset.



(a) Calibration effect. (b) Phase compensation.

Fig. 9. Assessment of the three calibration methods.

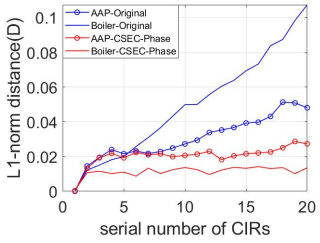
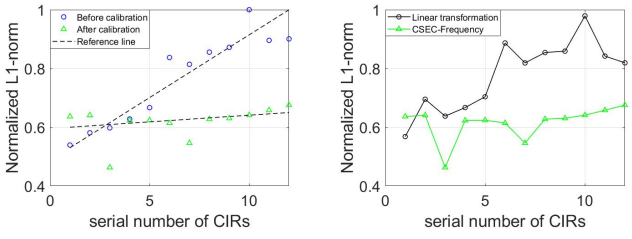


Fig. 10. Calibration effect in different industrial scenarios.

As shown in Fig.11(a), the normalized L1-norm distance between the reference CIR and the CIRs before calibration accumulates with measurements because the error of a CIR accumulates over time. However, the error accumulate tendency disappears after calibration by CSEC-Frequency. We can also see that the distance between the reference CIR and the CIRs from mobile measurements fluctuates around the reference line because the channel is dynamic during mobile measurements. Moreover, we can see from Fig.11(b) that the calibration effect of CSEC-Frequency is better than that of linear transformation, which is not considered suitable for the mobile scenario.

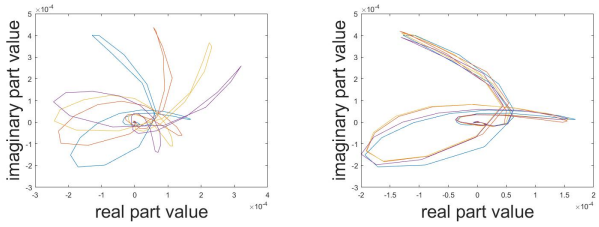


(a) calibrated effect. (b) method comparison.

Fig. 11. Applicability of CSEC-Frequency to a mobile scenario.

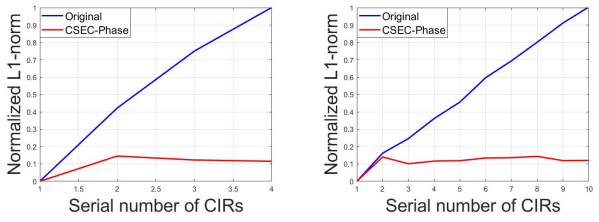
E. Performance of CSEC on other CIR Datasets

To verify the performance of the proposed CSEC method on another CIR dataset, we select a CIR dataset measured by the University of Utah. The Utah CIR dataset is publicly available from the Community Resource for Archiving Wireless Data at the Dartmouth (CRAWDAD) measurement repository [12]. The data acquisition system was similar to the NIST channel sounder system shown in Fig. 1. Four CIRs were acquired on each of 1892 channels with a 120 MHz sampling frequency and a 2443 MHz carrier frequency. For each channel measurement, the carrier frequency offset was found, as shown in Fig. 12(a). The CIRs calibrated with CSEC-Phase have high consistency for the same channel, as shown in Fig. 12(b). After CSEC processing, the CIR distances of the same channel are reduced compared with those of the original CIRs, as shown in Fig. 13(a).



(a) Original CIRs. (b) CIRs after CSEC-Phase.

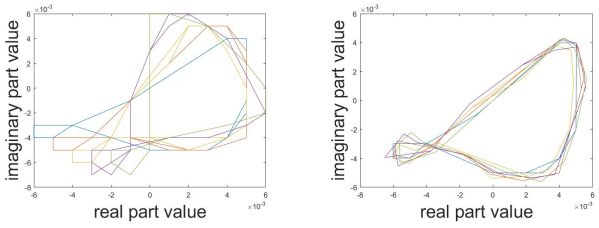
Fig. 12. Calibration effect on the Utah CIR dataset.



(a) Utah CIR dataset. (b) Our CIR dataset.

Fig. 13. Normalized L1-norm distance.

Moreover, we collected a CIR dataset using our experimental platform, which has a system architecture similar to that of the NIST channel sounder system shown in Fig. 1. Two Universal Software-defined Radio Platforms (NI USRP-2954R) were employed as Tx and Rx. Ten CIRs were acquired on each of 36 channels with a 4 MHz sampling frequency and



(a) Original CIRs. (b) CIRs after CSEC-Phase.

Fig. 14. Calibration effect on our CIR dataset.

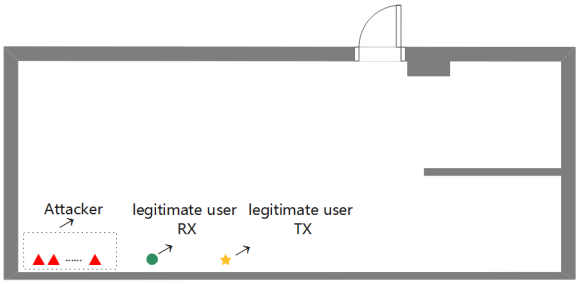
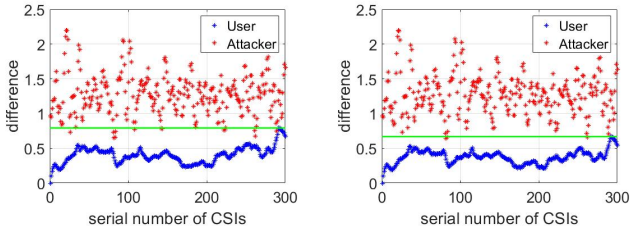


Fig. 15. Position of legitimate users and attackers in the AAP factory.



(a) Before calibration (b) After calibration

Fig. 16. Authentication performances before and after calibration. The threshold is represented by a green line. The accuracy of authentication is 94.67% before calibration and 99.3% after calibration.

a 2387 MHz carrier frequency. The carrier frequency offset phenomenon is observed for each channel, as shown in Fig. 14(a). We applied CSEC-Phase to calibrate the systematic errors in our CIR dataset, resulting in relatively better performance in terms of consistency and CIR distance, as shown in Fig. 14(b) and Fig. 13(b).

F. Case Study

As mentioned in Section IV, a threshold-based physical layer authentication method was proposed in [8] based on the NIST reference dataset. The difference between the CIR of a node requesting access to the network and the reference CIR is utilized to determine the identity of this node. If the difference is less than the threshold, this node is treated as a legitimate user and allowed to access the network; otherwise, the node is considered an attacker. To ensure that legitimate users can access the network normally, the threshold is set to the maximum difference between the CIRs of legitimate users. The difference is defined as [8]:

$$h_{difference} = \frac{\|h(t) - h(t_0)\|_2}{\|h(t_0)\|_2}. \tag{21}$$

In this case, we assume that a legitimate user requests access to the network 300 times at the same normal working position. When the legitimate user do not request access, 300 attackers attempt to penetrate the network at distances of 6-12 m from the legitimate user. The CIRs of legitimate user and attackers are all measured by the channel sounder at their respective stationary positions in the AAP factory, which are shown in Fig. 15. Moreover, there is no moving human or object on the direct path between Tx and Rx. With CSEC-Phase, the differences in the CIRs of the legitimate user are smaller after calibration, as shown in Fig. 16. The accuracy of authentication is 94.67% before CIR calibration and 99.3% after CIR calibration.

VIII. Conclusion

In this paper, we have presented two CSEC methods to improve the accuracy of CIR measurements in an industrial environment with a single-antenna receiver system. Under two conditions of negligible noise and no moving obstacles in the direct path, the proposed CSEC methods can compensate for record clock glitch and carrier frequency offset within CIR datasets. The carrier frequency offsets estimated via the CSEC methods remain within the upper and long-term stability bounds, and the deviation in the estimated carrier frequency offsets is consistent with the Allan variance. CSEC-Frequency method compensates only for the phase shift caused by the carrier frequency offset, whereas CSEC-Phase method compensates for all kinds of phase shifts caused by the carrier frequency offset and phase instability. Although CSEC-Phase method shows better performance than the linear transformation method and CSEC-Frequency method in stationary measurements, CSEC-Frequency method can be applied to stationary and mobile measurements. We have validated the CSEC methods in different industrial environments. Moreover, the results prove that the CSEC methods are also effective for another public CIR dataset and for a CIR dataset measured with our experimental platform. In addition, a case study of physical layer authentication confirms the positive impact of the CSEC method on the application of CIR data in a real-world scenario, in which CIR accuracy is important.

The proposed CSEC methods are applicable to most wireless channel sounding measurements with similar systematic errors. However, the efficiency of these methods in a runtime scenario needs to be investigated in the future. Moreover, we will study how to improve the authentication accuracy through algorithm design for the case of physical layer authentication. More effort is needed to meet the challenge of extending the case study to a generic target industrial environment where, e.g., no prior CIR data are available.

Disclaimer

Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply

that the materials or equipment identified are necessarily the best available for the purpose.

ACKNOWLEDGMENTS

This work was partially supported by the Special Fund for Strategic Pilot Technology of the Chinese Academy of Sciences (XDC02020600), the Liaoning Provincial Natural Science Foundation of China (2020JH2/10500002) and the LiaoNing Revitalization Talents Program (XLYC1902110).

REFERENCES

[1] C. Lu et al., "Real-Time Wireless Sensor-Actuator Networks for Industrial Cyber-Physical Systems," in *Proc. IEEE*, vol. 104, no. 5, pp. 1013-1024, May 2016.

[2] F. Pan et al., "Physical layer security to enhance the security in critical industrial wireless control: Basics and future directions," in *IEEE Ind. Electron. Mag.*, vol. 12, no. 4, pp. 18–27, 2018.

[3] A. M. Sayeed and B. Aazhang, "Joint multipath-Doppler diversity in mobile wireless communications," in *IEEE Trans. Commun.*, vol. 47, no. 1, pp. 123-132, Jan. 1999, doi: 10.1109/26.747819.

[4] Z. Y. Wu et al., "Channel Characterization and Realization of Mobile Optical Wireless Communications," in *IEEE Trans. Commun.*, vol. 68, no. 10, pp. 6426-6439, Oct. 2020, doi: 10.1109/TCOMM.2020.3009256.

[5] Yang, Zheng, Z. Zhou, and Y. Liu. "From RSSI to CSI : Indoor Localization via Channel Response." in *Acm Computing Surveys* 46.2(2013):1-32.

[6] H. Yu, et al., "Indoor passive localisation based on reliable CSI extraction," in *IET Communications*, vol. 13, no. 11, pp. 1633-1642, 16 7 2019.

[7] J. You, et al., "Security and Reliability Performance Analysis for Cloud Radio Access Networks With Channel Estimation Errors," in *IEEE Access*, vol. 2, pp. 1348-1358, 2014.

[8] X. Jiang, et al., "Using a Large Data Set to Improve Industrial Wireless Communications: Latency, Reliability, and Security," in *IEEE Ind. Electron. Mag.*, vol. 13, no. 1, pp. 6-12, March 2019.

[9] F. Pan et al., "Threshold-Free Physical Layer Authentication Based on Machine Learning for Industrial Wireless CPS," in *IEEE Trans. Ind. Inform.*, vol. 15, no. 12, pp. 6481-6491, Dec. 2019.

[10] X. Jiang, et al., "Delay Optimization for Industrial Wireless Control Systems based on Channel Characterization," in *IEEE Trans. Ind. Inform.*, in press, doi: 10.1109/TII.2019.2958708.

[11] Quimby, Jeanne T., et al. "NIST Channel Sounder Overview and Channel Measurements in Manufacturing Facilities". NIST TN 1979, National Institute of Standards and Technology, 8 Nov. 2017, p. NIST TN 1979. DOI.org (Crossref), doi:10.6028/NIST.TN.1979.

[12] Neal Patwari, CRAWDAD dataset utah/CIR (v. 2007 09 10), downloaded from https://crawdad.org/utah/CIR/20070910, https://doi.org/10.15783/C7630J, Sep 2007.

[13] T. M. Schmidl and D. C. Cox, "Robust frequency and timing synchronization for OFDM," *IEEE Trans. Commun.*, vol. 45, no. 12, pp. 1613–1621, Dec. 1997, doi: 10.1109/26.650240.

[14] P. Li, et al., "A novel timing advanced estimation algorithm for eliminating frequency offset in satellite system," in *2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Aug. 2015, pp. 1792–1796, doi: 10.1109/PIMRC.2015.7343589.

[15] J. J. van de Beek, M. Sandell, and P. O. Borjesson, "ML estimation of time and frequency offset in OFDM systems," *IEEE Trans. Signal Process.*, vol. 45, no. 7, pp. 1800–1805, Jul. 1997, doi: 10.1109/78.599949.

[16] M. Morelli and M. Moretti, "Fine carrier and sampling frequency synchronization in OFDM systems," *IEEE Trans. Wirel. Commun.*, vol. 9, no. 4, pp. 1514–1524, Apr. 2010, doi: 10.1109/TWC.2010.04.091058.

[17] M. Morelli, C. J. Kuo, and M. Pun, "Synchronization Techniques for Orthogonal Frequency Division Multiple Access (OFDMA): A Tutorial Review," *Proc. IEEE*, vol. 95, no. 7, pp. 1394–1427, Jul. 2007, doi: 10.1109/JPROC.2007.897979.

[18] K. Qian, et al., "Inferring Motion Direction using Commodity Wi-Fi for Interactive Exergames," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, May 2017, pp. 1961–1972, doi: 10.1145/3025453.3025678.

[19] Y. Zheng et al., "Zero-Effort Cross-Domain Gesture Recognition with Wi-Fi," in *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services*, New York, NY, USA, Jun. 2019, pp. 313–325, doi: 10.1145/3307334.3326081.

[20] K. Qian, et al., "PADS: Passive detection of moving targets with dynamic speed using PHY layer information," in *2014 20th IEEE International Conference on Parallel and Distributed Systems (ICPADS)*, Dec. 2014, pp. 1–8, doi: 10.1109/PADSW.2014.7097784.

[21] Y. Zheng, et al., "Detecting radio frequency interference for CSI measurements on COTS WiFi devices," *2017 IEEE International Conference on Communications (ICC)*, Paris, 2017, pp. 1-6, doi: 10.1109/ICC.2017.7997069.

[22] M. Kashef, R. Candell and Y. Liu, "Clustering and Representation of Time-Varying Industrial Wireless Channel Measurements," *IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society*, Lisbon, Portugal, 2019, pp. 2823-2829.

[23] T. F. Sanam and H. Godrich, "FuseLoc: A CCA Based Information Fusion for Indoor Localization Using CSI Phase and Amplitude of Wifi Signals," *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Brighton, United Kingdom, 2019, pp. 7565-7569.

[24] Zhang, Junxing, et al. "Advancing wireless link signatures for location distinction." *Proceedings of the 14th Annual International Conference on Mobile Computing and Networking, MOBICOM 2008*, San Francisco, California, USA, September 14-19, 2008 ACM, 2008.

[25] S. Chen, et al., "Automated Labeling and Learning for Physical Layer Authentication against Clone Node and Sybil Attacks in Industrial Wireless Edge Networks," in *IEEE Trans. Ind. Inform.*, in press, doi: 10.1109/TII.2020.2963962.

[26] S. Sen, et al., "Avoiding multipath to revive inbuilding WiFi localization," in *11th Annual International Conference on Mobile Systems, Applications, and Services, MobiSys 2013*, Taipei, Taiwan, 2013, pp. 249–262, doi: 10.1145/2462456.2464463.

[27] O. Taheri and S. A. Vorobyov, "Reweighted l1-norm penalized LMS for sparse channel estimation and its analysis," in *Signal Process.*, vol. 104, pp. 70–79, Nov. 2014

[28] Vargas, H, Ramirez, J, and Arguello, H, "ADMM-based l(1) - l(1) optimization algorithm for robust sparse channel estimation in OFDM systems," in *Signal Process.*, vol. 167, Nov. 2020. dio: 10.1016/j.sigpro.2019.107296