Reshaping Wi-Fi ISAC with High-Coherence Hardware Capabilities

Rui Li, Yu Duan, Rui Du, Fangxin Xu, Hangbin Zhao, Yang Sun, Yiyan Zhang, Daiyang Zhang, Yiming Liu, Zhiping Jiang, and Tony Xiao Han

***Abstract*—Wi-Fi is promising for Integrated Sensing and Communication (ISAC), but its wider application is hampered by two pivotal challenges: the low-quality Channel State Information (CSI) and inadequate hardware capabilities.**

This paper introduces a paradigm shift with high-coherence hardware capabilities to fundamentally overcome these two challenges. Our approach is realized through four key breakthroughs. First, we uncover a novel category of CSI error sources, termed CODEs, which pose core challenges for Wi-Fi ISAC. The CODEs stem from the Wi-Fi hardware design, and addressing them requires hardware-level modifications. Then, we propose a list of high-coherence hardware capabilities aimed at eliminating these errors. Our analysis indicates that the majority of these capabilities can be implemented at the firmware level, with a minority requiring chip-level changes. Next, we introduce two robust and synergistic incentives to encourage vendors to integrate these capabilities into their hardware: the 802.11bf standard and its certification program, and the large-scale carrier-grade purchasing. Finally, we present two demonstrations: a sub-nanosecond level time-of-flight (ToF) estimation system, and a Wi-Fi based phased array. Both demonstrations show that remarkable sensing precision is achievable with the proposed high-coherence capabilities.

***Index Terms*—Wi-Fi ISAC, Wi-Fi Sensing, High-Coherence Hardware Capabilities, Hardware Modifications, Vendor Incentives.**

I. Introduction

Wi-Fi's ultra-dense deployment, coupled with its close proximity to a vast user base, position it as an ideal platform for large-scale ISAC applications [1]. Emerging representative research areas include breath detection [2], motion sensing [3], gesture recognition [4], fall detection [5], and life pattern recognition [6]. These areas reflect the versatility of Wi-Fi ISAC and also the field's potential for growth and innovation.

Unfortunately, the commercialization of Wi-Fi ISAC technologies has faced repeated failures, leaving the industry perplexed for a long time. Technical hurdles, including low spatio-temporal consistency, limited resolution, and high sensitivity to environmental variables and deployment contexts, have emerged as formidable barriers, consistently hindering the progress toward commercial viability [7].

To overcome these barriers, we have established a diverse task group—comprising academics, Wi-Fi standard experts, chip vendors, carrier operators, and regulatory bodies. Our expertise in Wi-Fi chip design and baseband signal processing has led us to a clear conclusion: *the multifaceted challenges of Wi-Fi ISAC fundamentally stem from low-quality CSI data and inadequate hardware capabilities*. In response, we call upon global Wi-Fi vendors to act decisively by supporting the ISAC-oriented IEEE 802.11az/bf/bk standards, providing high-quality CSI, granting access to low-level controls, and upgrading hardware for the demanded capabilities.

To transform what could be perceived as '*just another unrealistic academic daydream*' into tangible reality, we make four key breakthroughs: First, we unveil a new category of CSI errors, *communication-centric optimization-induced CSI errors* (CODEs). Contrary to common belief, it is these CODEs, rather than conventional transceiver errors, that present the greatest technical challenges in Wi-Fi ISAC. The complete elimination of CODEs and other errors requires fine-grained PHY-layer controls. Second, we identify a critical list of high-coherence hardware capabilities, which allows higher-level algorithms to correct errors and restore high-quality CSI, thus making the Wi-Fi hardware fully ISAC-ready. Third, we introduce two powerful incentives that, together, provide a strong motivation for vendors to integrate these capabilities into their hardware. Finally, we present two high-precision Wi-Fi ISAC demos: a sub-nanosecond level time-of-flight (ToF) estimation system, and a Wi-Fi based phased array. Both demos show that remarkable sensing precision is achievable with the proposed high-coherence capabilities.

This paper unfolds as follows: Section II compares Wi-Fi ISAC with radar to clarify the challenges of Wi-Fi ISAC. Section III attempts to define the "high-quality CSI" through five aspects of coherence. Section IV presents the CSI error model and highlights the CODEs. Section V introduces the proposed high-coherence hardware capabilities and vendor incentivization programs. Section VI shows the two demos. Section VII concludes the paper.

II. From Wi-Fi to Wi-Fi ISAC: The Challenges

The transition from conventional Wi-Fi to Wi-Fi ISAC is not as simple as adapting existing radar technologies to the Wi-Fi platform [8]. The challenge is much greater due to the fundamental differences between the systems. Unlike radar, purpose-built for sensing, Wi-Fi lacks both inherent design and hardware capabilities for RF sensing, thus giving rise to the following three main challenges:

Rui Li, Yu Duan, Daiyang Zhang, Yiming Liu and Zhiping Jiang are with the School of Computer Science and Technology, Xidian University, China.

Rui Du, Yiyan Zhang and Tony Xiao Han are with the Wireless Technology Laboratory, Huawei Technologies Co. Ltd., China.

Fangxin Xu is with the Shenzhen Longsailing Semiconductor Co. Ltd., China.

Hangbin Zhao is with the China Mobile (Hangzhou) Information Technology Co., Ltd., China.

Yang Sun is with the State Radio Spectrum Management Center, China.

Zhiping Jiang is the corresponding author.

- Low Sensing Resolution: Radars benefit from superior spatio-temporal resolution due to their large bandwidth and far-field sensing scenarios. In contrast, Wi-Fi typically operates with narrow bandwidth in short-range, rich-reflective environment. In this case, it is extremely difficult to differentiate the desired signals from the ambient reflections [9].
- Transmitter/Receiver (Tx/Rx) Asynchronization: Radars commonly operate in mono-static mode. In this mode, all transceivers are co-located and globally synchronized. Conversely, Wi-Fi involves multiple devices, somewhat similar to radar's bi/multi-static mode. However, Wi-Fi lacks the global synchronization system present in such radars. As a result, CSI suffers from frequency and timing errors such as carrier frequency offset (CFO), carrier phase offset (CPO), sampling frequency offset (SFO) and sampling time offset (STO).
- CODEs: Although both radar and Wi-Fi pursue high-quality channel, their approaches differ. Radars focus on minimizing errors for the *in-air channel* to support RF sensing; Wi-Fi seeks to improve the *full-baseband* channel quality for wideband communication purposes by deeply optimizing the entire transmission chain from Tx to Rx. However, these specific optimizations can lead to irrecoverable disturbances into CSI, *i.e.* CODEs. Section IV provides the first comprehensive analysis of the impact of CODEs on CSI.

Clearly, the combined impact of these three challenges greatly compromises the quality of CSI, posing huge barrier to the integration of radar technologies into Wi-Fi.

III. Defining High-Quality CSI

The definition of "High-Quality CSI" varies by application. Some require the CSI to capture environmental disturbances, while others demand predictable frequency and phase errors. Despite these diverse requirements, one expectation is universal: *"High-Quality CSI" should be coherent and predictable.*

However, an unexpected twist arises: *"High-Quality CSI" is not a synonym for minimal error; sometimes, it can be the opposite.* Efforts to reduce error can unintentionally disrupt the CSI, and that is where CODEs come into play. For example, the Automatic Gain Control (AGC) can improve Rx sensitivity and communication performance, however, it introduces randomness to the CSI amplitude, disrupting the amplitude consistency across frames.

Drawing on insights from radar and RF imaging [10], we define "High-Quality CSI" through five aspects of coherence:

- **T**iming: Differences between CSI should reflect time intervals between measurements.
- **A**mplitude: CSI should consistently reflect the channel changes due to environmental factors.
- **F**requency: Frequency errors should be predictable by algorithms.
- **P**hase: Phase errors should be predictable by algorithms.
- **S**patial: Spatial discrepancies, such as phase differences between antennas and errors in angle of arrival (AoA) estimation, should be predictable by algorithms.

This coherence-based framework is crucial for identifying the hardware capabilities required to restore the CSI coherence. We provide a comparative analysis of the non-coherent and coherent CSI in the *Supplementary File*.

IV. Paradox in CSI: Communication Hurts Sensing

How many kinds of errors are concealed in CSI? This question has puzzled researchers for long time. Leveraging our code-level access to the Wi-Fi chip design, we have identified a total of 14 distinct error sources in CSI, as shown in Fig. 1. These errors fall into two categories: the typical Wi-Fi transceiver errors, labeled (a) - (h), and CODEs, labled ① - ⑥. Given the extensive analysis in prior research [11], we skip the first category and mainly focus on CODEs. To the best of our knowledge, this is the first work that systematically explores the CODEs. The six types of CODEs are:

① Tx Bit Scrambler/Padding: The Tx bit scrambler is employed to address the issue of high peak-to-average power ratio (PAPR) by randomizing the input bits. This, however, introduces variability in the Tx power for identical frames. In Wi-Fi terminology: for identical MPDUs (MAC-layer frames), the scrambler generates distinct PSDUs (bit-level representation of a frame), and as a result, different PPDUs (signal-level representation of a frame), each with its own PAPR. To preserve the signal integrity of the transmitted signals, the Tx power control (TPC) must dynamically adjust the Tx power for each PPDU according to its PAPR, leading to inconsistent Tx power that disrupts the amplitude coherence.

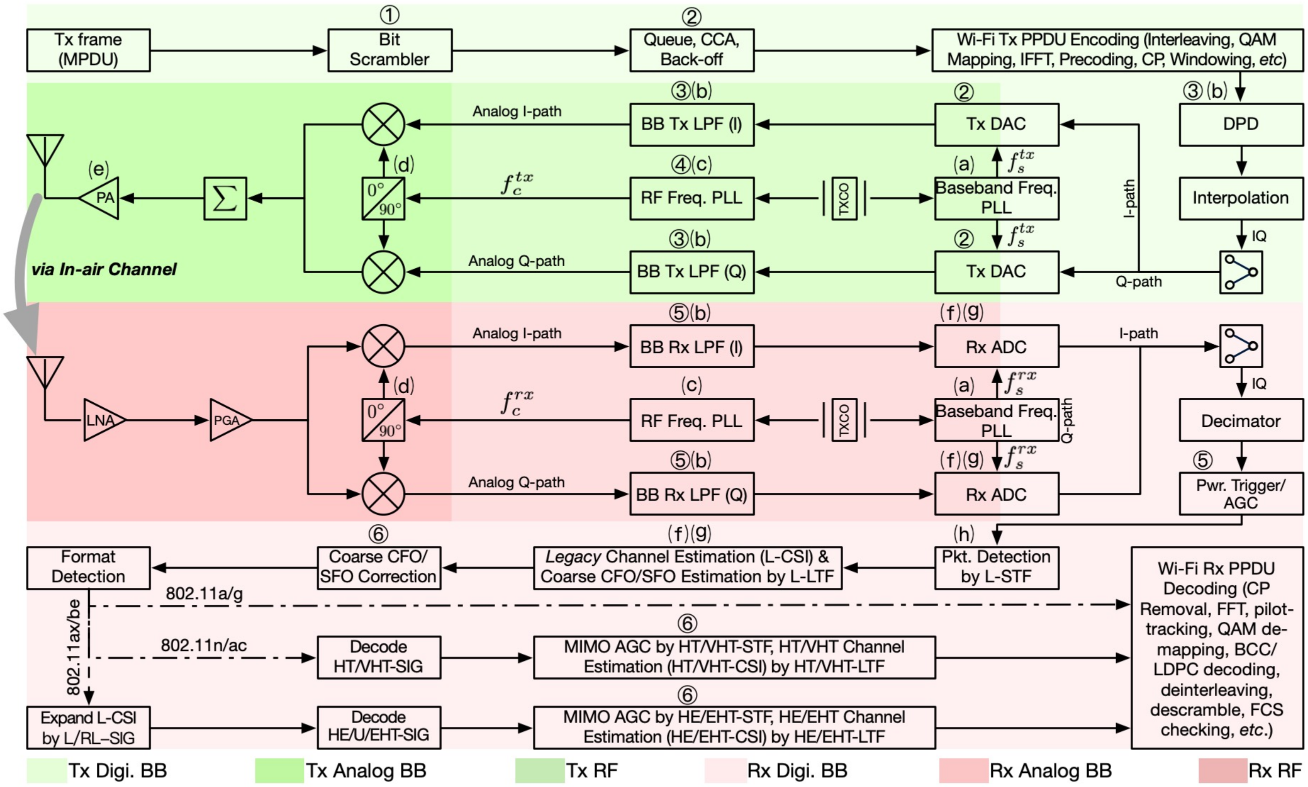
② Lack of Precise Timing: Precise timing is absent at both the Tx and Rx ends. At the Tx end, the timing imprecision stems from the clear channel assessment (CCA), ACK mechanism, Tx queuing, the multi-rate design between the digital baseband (DBB) and in-chip low-MAC (LMAC), *etc.* They together introduce random delays to the transmission intervals. At the Rx end, the multi-rate design degrades the Rx timing resolution, even worse, the μs-level timestamps are inadequate for CSI-based frequency and phase estimation. Combined, these timing issues impair the restoration of time and frequency coherence.

③ Modulation-Dependent Tx Filter Reconfiguration: To optimize the Tx signal's error vector magnitude (EVM) and spectrum flatness, Tx path filters, both digital and analog, are dynamically adjusted based on Tx parameters, such as channel frequency, bandwidth, Tx power, MCS (Modulation Coding Scheme), and beamforming. Such adjustments, even for identical PPDUs, introduce random CSI perturbations, undermining amplitude and phase coherence.

④ Tx LO Switching: To prevent power leakage from the Tx Local oscillator (LO) to the Rx, Wi-Fi chips adopt a LO switching mechanism, which deactivates the Tx LO during the Rx and then reactivates it for Tx. However, upon re-activation, the LO settles at a random initial phase and slightly different frequency, disrupting the frequency and phase coherence.

⑤ Rx AGC: AGC expands the Rx dynamic range by adaptively tuning the LNA, PGA, and related filters. Like the issue of Tx filter reconfiguration, AGC introduces random variations to CSI amplitude, disrupting the amplitude coherence.

⑥ Residual CFO and SFO: The Wi-Fi NIC-returned CSI is *not the original, pristine channel estimation*, but the third or fifth one, which is skewed by the residual CFO and SFO. To elaborate on this issue, we briefly revisit the Wi-Fi Rx decoding process. As shown in the lower part of Fig. 1, the decoder starts with the 'Power Trigger/AGC' and 'Packet De-



*** Typical Transceiver Errors**: (a) SFO, (b) Non-Linear Filter, (c) CFO, (d) I/Q Imbalance, (e) PA Nonlinearity, (f) STO, (g) CPO, (h) Packet Detection Offset (PDO);
*** CODEs**: ① Scrambler, ② Lack of Precise Tx/Rx Timing, ③ Dynamic Tx Filter, ④ Tx LO Switching, ⑤ Rx AGC, ⑥ Residual CFO/SFO

Fig. 1: Wi-Fi transceiver architecture and CSI error sources.

tection'. Subsequently, 'Legacy Channel Estimation' derives *the first two CSIs* using the L-LTF field. For 802.11ax/be-format frames, *two more CSIs* are derived using the L-SIG and its repetition (RL-SIG). These CSIs are then used to calculate coarse CFO and SFO estimations. Next, 'Coarse CFO/SFO Correction' applies phase and timing adjustments to the SIG field and all following symbols to rectify the estimated CFO and SFO. As a result, the CSI measured from HT/VHT/HE/EHT-LTF symbols-*the third or fifth CSI for the pre or post-11ax format*-contains the undesired correction, and is then returned by the NIC hardware. While this correction is critical for OFDM communication, it hurts sensing significantly. The crux of this issue is that: as the term 'coarse estimation' implies, the CFO and SFO estimations are not very accurate, leading to the CFO/SFO correction itself becoming an additional layer of uncertainty in phase and timing. This additional randomness fundamentally undermines the frequency and phase coherence.

V. Modifying Hardware and Incentivizing Vendors

Clearly, mitigating CODEs and other CSI errors requires hardware modifications. This section outlines the necessary modifications or hardware capabilities needed to achieve this goal, and also discusses the strategies to motivate vendors to implement these capabilities in their hardware.

A. High-Coherence Wi-Fi Hardware Capabilities

Aware of the substantial costs associated with the hardware modifications, we adhere to the principle of 'minimal modification, maximal utility, forward-looking, and interoperability', which *offers sufficient capabilities to help higher-level algorithms restore CSI coherence*. We identify 20 essential capabilities, as shown in Table I, and each assigned a unique code name for convenience. These capabilities are categorized across three levels: MPDU, DBB, and RF.

At the MPDU level, PIMO and CMM enable the hardware to inject Wi-Fi frames and measure CSI for frames sent by non-associated stations in monitor mode, respectively. This helps ISAC devices establish spatial awareness through association-free sensing. SEED improves amplitude coherence by controlling the scrambler and padding seeds.

We categorize the DBB capabilities into four sub-aspects:

DBB Sub-aspect I: *Tx-End Extra LTF Transmission (ELT)*. As discussed in Section IV ②, the random delays between transmissions undermine the CSI coherence across consecutive frames. ELT can address this issue by inserting extra LTF symbols within each frame, which allows the Rx end to obtain multiple rigorously spaced CSIs to restore CSI coherence by algorithms. ELT is implemented by DPLR and ESSL. DPLR utilizes the 802.11ax High-Doppler mode to insert additional HE-LTF symbols at predetermined intervals, allowing for up to 39 CSIs, each 136-μs spaced, within the longest PPDU of 5.484 *m*s. Likewise, ESSL, based on the Extra Sounding feature of the 802.11n/az/be/bf/bk standards, inserts extra HT/HE/EHT-LTF symbols to the preamble part to provide up to 8 CSIs spaced by 4 or 16-μs.

DBB sub-aspect II: *Rx-End High-Coherent CSI Measurement*. As explained in Section IV ⑥, CSI measured from

TABLE I: ISAC-Friendly Wi-Fi Hardware Modification List

Arch. Level	Code Name	Enhancement / Capability	Required Access	Affected Coherence	Path	Standardized	Modification Level	Difficulty
MPDU	PIMO	Packet injection in monitor mode	C	T, S	Tx		FW	★ • • • •
	CMM	Measure CSI for unassociated STAs in monitor mode	R	S	Rx	802.11az	FW	★★ • • •
	SEED	Initial seed for Scrambler and post-FEC padding	R+	A	Tx		FW	★★ • • •
DBB	DPLR	802.11ax High-Doppler mode	C	T	Tx	802.11ax		★ • • • •
	ESSL	802.11n/az/be/bf/bk Extra Sounding or LTF Repitition	C	T	Tx	802.11n+		★ • • • •
	CFOE	L-LTF based CFO and SFO estimation	R	F, P, T	Rx		FW	★ • • • •
	LCSI	Two Legacy CSIs by L-LTF	R	F, P, T	Rx		MEM	★★★★★
	MCSI	Multiple HT/VHT/HE/EHT-LTF based CSIs	R	F, P, T	Rx		MEM	★★★★★
	PILO	Values of pilot subcarriers per-OFDM symbol	R	F, P, T	Rx		MEM	★★★★★
	STMP	Frame's Tx/Rx timestamp with sample-level precision	R	F, P, T	Both	802.11mc+		★★★ • •
	TIME	Per-frame (or intra-batch) precise Tx timing	C	T	Tx	802.11ax+		★★★★ •
	RXOF	Rx OFDM demodulation offset	R+	T	Rx		FW	★ • • • •
	PCOD	Per-subcarrier/stream/antenna Tx precoding	C	A, P, S	Tx	802.11n+		★ • • • •
RF	NSLO	Unstopped Tx LO during Tx gaps	C	P, T	Tx		FW	★★ • • •
	TUNE	Manual fine-tuning for carrier/sampling frequency	C	F, P, T	Rx	802.11ax+		★ • • • •
	AGC	Manual gain control (include per-antenna gain)	C	A, S	Rx		FW	★★ • • •
	DPD	Digital pre-distortion and per-chain Tx/Rx filter	R+	A, P, S	Both		FW	★★★ • •
	DELY	Accurate per-chain frontend delay (in *ps*)	R	P, S	Both	802.11mc+		★ • • • •
	ANTD	Inter-antenna phase differences	C	S	Both		FW	★ • • • •
	SMLO	Same-band Multi-Link Operation	C	F,P,T	Both	802.11be		★★★★ •

* In 'Required Access' column, *R* for read, *C* for control, and *R+* for 'read or better control'; In 'Affected Coherence' column, A/T/F/P/S stands for amplitude, timing, frequency, phase, and spatial, which is detailed in Section III; In the 'Modification Level' Column, *FW* for firmware, MEM for in-chip memory, detailed on Section V (B).

HT/VHT/HE/EHT-LTFs are contaminated by the 'Coarse CFO/SFO Correction' operation. To remove these errors, we propose four capabilities for coherence restoration. LCSI requires the hardware to provide two CSIs measured from the L-LTF field, each spaced by 4-μs. CFOE returns the values of CFO/SFO coarse estimation. MCSI requires hardware to provide multiple CSIs for the frames containing extra LTF fields, *e.g.*, those frames augmented by DPLR or ESSL. Finally, PILO requires the pilot subcarriers of all OFDM symbols, which can be used to calculate the pilot subcarrier-based CSIs, enabling a more precise CSI coherence restoration.

DBB sub-aspect III: *Precise Timing*. Besides Tx-end ELT, another approach for restoring coherence involves Tx/Rx precise timing. We propose three capabilities, namely TIME, STMP and RXOF. TIME requires to transmit one PPDU at a given timestamp or transmit a batch of PPDUs with given inter-frame spacings (IFSs), both with sample-level precision. STMP requires accurate Tx and Rx timestamps. Last, RXOF requires to access the OFDM decoding offset.

DBB sub-aspect IV: *Tx-End Precoding*. The Tx signal precoding capability, PCOD, involves multiplying each OFDM symbol of a PPDU by a user-defined complex-valued steering matrix. This allows higher-level algorithms to proactively manipulate the steering, multipath delay and fading.

At the RF level, we propose seven capabilities. NSLO addresses the issue of random CPO and CFO between consecutive packets by temporarily disabling the Tx-end LO switching mechanism. TUNE requires to fine-tune the frequencies of the LO and the baseband ADC/DAC sampling rates. In terms of amplitude coherence, both AGC and DPD aim to provide fine-grained amplitude control. DELY and ANTD, targeting at the RF delay and its stability within the RF chain, contribute to establish spatial coherence. Finally, SMLO leverages the 802.11be Multi-Link Operation (MLO) feature to achieve synchronized multi-link sensing.

Due to the page limit, more explanations for some capabilities are detailed in the *Supplementary File*. We also acknowledge that as the initial exploration, this list is preliminary and may evolve as new insights emerge.

B. Implementing Capabilities? Half Done, Half Simplified!

There has been skepticism among researchers regarding whether NIC vendors would modify their hardware for ISAC. However, vendors are indeed working on these capabilities, albeit not for ISAC. This progress is driven by the latest Wi-Fi standards, which, in their advancement and complexity, mandate the development of various high-coherence technologies, which align with ISAC needs [12].

As shown in the 'Standardized' column of Table I, *half of the capabilities have been implemented by key technologies tied to specific standards*. For example, the 802.11mc standard demands a precision of 16-*ps* for the Tx/Rx timestamp, meeting the requirement of STMP. The 802.11n/ax/az/be/bf/bk standards [13], [14], featuring the Tx end ELT capabilities, require NIC to measure multiple rigorously spaced CSIs from one PPDU, which satisfies DPLR, ESSL and MCSI. The trigger-based up-link MU-MIMO (TB UL-MU-MIMO) mode, introduced by 802.11ax/be, demands precise Tx timing and requires client devices to maintain their CFO within a 350 Hz limit. This high accuracy requires accurate CFO estimation and LO adjustment, which matches TUNE and TIME.

For capabilities not tied to a specific Wi-Fi standard, we partner with experts from Huawei Technologies, Longsailing Semiconductor and China Mobile Communication Corporation (CMCC) to identify optimal solutions. For the sake of clarity, before exploring these solutions, let's briefly review modern Wi-Fi chip architecture. Modern Wi-Fi chips comprise three primary components: the RF front-end module (FEM), responsible for the analog-domain tasks such as filters and spectrum up/down conversions; Digital Baseband (DBB), realizing the high-speed baseband signal processing algorithm; and an on-chip CPU module, running the firmware code which manages the FEM, DBB and data transfer.

Bearing this architecture in mind, we identify two approaches to implement these capabilities. First, for '*settings or short result output*' capabilities, such as SEED, CFOE, and NSLO, firmware-level modifications are most appropriate since they are fundamentally firmware-based functionalities. Such modifications can be made without altering hardware or chips, thereby allowing vendors to implement them at minimal costs. We label these capabilities with FW in the 'Modification Level' column of Table I. Second, for '*high-speed or large-volume data transfer*' capabilities, such as LCSI, MCSI and PILO, chip-level changes are required. These capabilities, which involves moving large intermediate results out of the chip, necessitate an expansion of the chip's memory and I/O facilities. Fortunately, chip experts indicate that since the memory and I/O components are relatively peripheral within the chip's architecture, such modifications are easy and cost-effective. These are marked as MEM in Table I.

C. The Most Challenging Mission: Incentivize vendors!

How to encourage vendors to modify their hardware and open these capabilities to researchers? Undoubtedly, these two challenges, which go beyond the technical aspects, become the most formidable obstacles in realizing our goal. To overcome them, we rely on two synergistic and robust incentives: the 802.11bf standard along with its certification program, and mass purchasing by large Wi-Fi network provider.

The 802.11bf standard, referred to as Wi-Fi Sensing, is led by the standard experts from Huawei, Intel, and Qualcomm. It aims to bring interoperable Wi-Fi sensing capabilities into Wi-Fi ecosystem. As 802.11bf encapsulates the majority of the standardized capabilities in Table I, it aligns close with our goals. We expect that 802.11bf standard will encourage vendors to integrate these capabilities into their hardware.

Proponents of 802.11bf are actively leveraging their influence in both industry and academia to draw an increasing number of Wi-Fi vendors to the initiative. Discussion has been initiated with the Wi-Fi Alliance (WFA), the entity behind the 'Wi-Fi' brand and 'Wi-Fi Certified' trademarks, to establish a certification program focusing on 802.11bf, which is expected to be branded as 'Wi-Fi Sensing™'. The global reach of the WFA and its certificate program is projected to significantly motivate vendors to integrate these capabilities into their hardware and adhere to the standard.

It should be noted that the 802.11bf standard does not involve PHY-layer modifications. To address capabilities that fall outside the scope of 802.11bf, we are looking to the influence of major Wi-Fi network providers, such as CMCC.

CMCC, a leading 5G and ISP-backed Wi-Fi network provider in China, has developed a proprietary Wi-Fi sensing standard, which encompasses an extensive set of capabilities largely based on Table I. CMCC plans to use its colossal purchasing power to push this initiative. In the near future, only devices compliant with this standard will be considered for CMCC's purchasing. Apparently, CMCC's purchasing requirements will act as a powerful incentive, encouraging vendors to modify their hardware to meet CMCC's specifications.

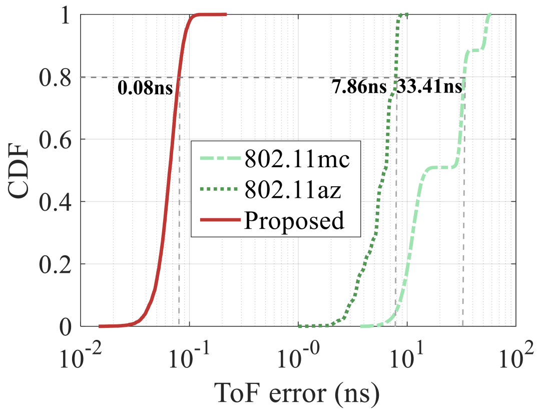


Fig. 2: MLOF-based accurate ToF estimation.

The influence of CMCC's initiative is expected to extend beyond China, potentially influencing the global Wi-Fi market. For vendors, adherence to CMCC's standards could be economically advantageous in the long term. This is largely because CMCC's standards covers a more comprehensive set of capabilities compared to the current standards, thereby reducing the frequency of chip redesigns.

VI. High-Coherence Capabilities in Action

In this section, we present two real-world demos that showcase the precise measurement capabilities enabled by the ISAC-friendly Wi-Fi hardware. Both demos are prototyped as plugins of the PicoScenes [15] Wi-Fi ISAC research platform, which leverages the NI USRP B210 devices as transceivers. PicoScenes enables transmitting and receiving 802.11a/g/n/ac/ax/be-format frames using SDR devices in real time, supporting up to 320 MHz bandwidth frames. Furthermore, PicoScenes supports most of the capabilities listed in Table I, thus enabling researchers to immediately implement and test cutting-edge Wi-Fi ISAC technologies without being constrained by the availability of commercial Wi-Fi hardware.

A. Sub-nanosecond Level ToF Measurement

The first demo showcases the capabilities of timing and frequency coherence. We develop a high-precision ToF estimation system employing the same Round-Trip Time (RTT) ranging protocol used by the 802.11mc/az standards, yet our system outperforms both standards by two orders of magnitude. Although 802.11az is the most accurate Wi-Fi ranging protocol, however, it still faces the STO accumulation error. Correcting this error requires accurate SFO estimation, which was unachievable due to inadequate measurement tools.

Leveraging the advanced capabilities in Table I, we achieve unprecedented precision in both SFO and ToF estimations. To evaluate its performance, we implement the 802.11mc and 802.11az standards for comparison. In order to shield against the multipath reflections, we conducted tests in an anechoic chamber, and the distance between Tx and Rx is 10 meters.

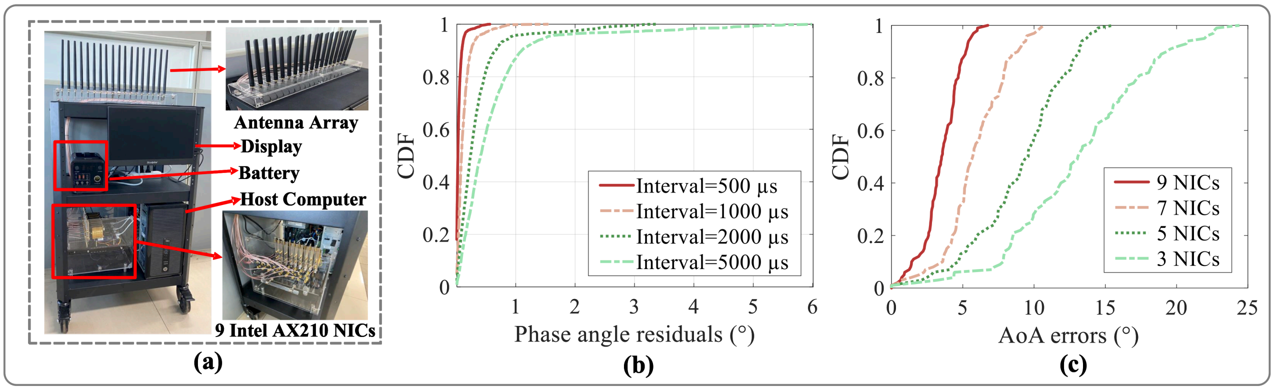


Fig. 3: Prototype of Wi-Fi based phased array, its phase tracking accuracy, and AoA estimation accuracy.

As shown in Fig. 2, our method achieves sub-nanosecond ToF accuracy using a 20 MHz channel. This level of precision highlights the significant enhancements enabled by the high-coherence capabilities.

We devise a technology called *ultra-long timing-coherence* (ULTC) to attain such exceptional precision. ULTC enhances the conventional RTT protocol, changing the '*non-coherent multi-initiation & multi-response*' approach to a '*rigorously-spaced multi-initiation & multi-response with ELT*' approach. This enhancement introduces two levels of timing coherence. At the intra-frame level, we harness the DPLR and MCSI capabilities to capture multiple CSI measurements per RTT measurement frame, each precisely spaced by 136-μs. At the inter-frame level, the TIME capability is utilized to specify the Inter-Frame Spacing (IFS) for the RTT measurement frames with sample-level accuracy, fostering consistent long-term timing coherence across frames. This dual-layer synchronization enables us to obtain a sequence of precisely timed CSI measurements across all RTT frames. By calculating the per-CSI STO using the pre-CSI phase slope, we achieve precise estimation for SFO, leading to high-precision ToF estimation.

B. COTS NIC-based Wi-Fi Phased Array

The second demo showcases the capabilities of phase and spatial coherence with a prototype Wi-Fi phased array system. As depicted in Fig. 3(a), this prototype synchronizes and calibrates nine unmodified Intel AX210 Wi-Fi NICs into an expandable phase-coherent uniform linear array (ULA). These NICs function collectively as a single 18-antenna phased array, pinpointing the AoA of incoming frames. Technically, this system consists of three stages: *multi-NIC carrier frequency synchronization*, and *in-site phase offset estimation and calibration*, and *AoA measurement*.

Stage 1: multi-NIC carrier frequency synchronization: There are two roles in this stage: the Sync Master, an SDR device, is placed nearby the array and broadcasts the Carrier Frequency Sync Frames (CFSFs); each NIC in the array operates as a Sync Client, receiving CFSFs, measuring their CSIs, performing CFO estimation & tracking, compensating for the CFO error, and ultimately achieving carrier frequency synchronization. The most challenging task in this process is CFO estimation & tracking, which was previously impossible due to the large phase error and phase 2π-wrapping.

We overcome this challenge with TIME capability. TIME enables direct observation of the linear relationship between IFS and the inter-frame CSI phase error (IFCPE), however, we cannot obtain correct CFO estimation due to the phase 2π-wrapping issue. Our trick is that the Sync Master transmits CFSFs not with a fixed IFS, but with *linearly growing IFSs*, *i.e.*, increasing the per-frame IFS by an incremental time $\Delta\tau_{ifs}$. And by choosing a small $\Delta\tau_{ifs}$, say, 100ns, the extra phase error in IFCPE, induced by $\Delta\tau_{ifs}$, will be small enough to avoid 2π-wrapping, leading to a unique and accurate CFO estimation. We then use a modified Kalman filter to track CFO and per-NIC phase error. During the tracking phase, Sync Master transmits CFSFs with a large and fixed-value IFS to reduce system's duty cycle. As shown in Fig. 3(b), even with an IFS up to 5000 μs, the tracked phase error remains $< 1°$ in most of time. Last, for each NIC, we compensate the CFO for all received frames, at this end, the NIC array is frequency synchronized and behaves as if they shared the same LO.

Stage 2: In-situ phase offset estimation and calibration: We leverage the straight-line geometry of ULA to perform in-situ self-calibration. Let's assume the $2N$ antennas ares linearly placed like $[A_1^l, A_1^r, A_2^l, \ldots, A_N^r]$ each separated by $d = 3$cm. Here A_i^l and A_i^r represent the left and right antennas of the i-th NIC, respectively. To calibrate the *intra-NIC phase offset* of NIC i, Phase Offset Measurement (POM) frames are transmitted from the adjacent antennas A_{i-1}^r and A_{i+1}^l. Then, NIC i receives the frames and computes the phase difference between its two antennas, denoted by $\Delta\Theta_i$. To achieve calibration, we adjust for any discrepancies between $\Delta\Theta_i$ and the ideal offset $\pm 2\pi\lambda/d$. This method is also applied to *Inter-NIC phase offset*. To calibrate the phase offset between NIC i and $i+1$, POMs are sent from A_{i-1}^r and A_{i+2}^l, and the phase offset between A_i^l and A_{i+1}^l is compensated to $\pm 4\pi\lambda/d$.

Readers might wonder about the possibility for multipath interference. Intriguingly, extensive evaluations have led to a somewhat counterintuitive but defensible conclusion: while our calibration scheme could theoretically be affected by multipath interference, in reality, the impact is negligible. This resilience stems from two factors, the compact layout of the antenna array and Rx AGC. First, With each antenna separated by roughly $\lambda/2$, signal transmission between adjacent antennas is predominantly governed by the near-field inductive coupling mechanism. As a result, the signal's line-of-sight (LoS) path is significantly stronger—by tens of dB—than any reflective paths from the far-field. Second, the Rx AGC further amplifies this disparity. To prevent potential saturation of Rx ADC in facing the strong LoS path, Rx AGC is adjusted to such a low level that insufficient quantization levels is left for the much weaker reflected signals. This insufficiency causes the multipath signals to be deeply submerged in quantization noise, severely degrading their quality. With these two elements combined, our calibration approach is endowed with a robust immunity to the multipath interference.

Stage 3: AoA Estimation: After the above two steps, this stage is straightforward. For all frames received by each NIC, we compensate for phase errors due to both intra/inter-NIC phase offsets, essentially restoring the phase and spatial coherence of the antenna array. MUSIC algorithm is then used to perform AoA estimation. We test the AoA performance in an anechoic chamber. The array is placed on a rotation platform to simulate Tx directions and is 10 meters distant from the Tx. As shown in Fig. 3(c), when all nine NICs are operational, the phased array attains an angular resolution of 5°.

VII. Conclusions & Future Work

This paper proposes a paradigm shift of Wi-Fi ISAC research through the Wi-Fi high-coherence hardware capabilities. With these capabilities, CODEs and other CSI errors can be completely removed, which are exemplified through two beyond the state-of-the-art demos. Key technologies in both demos will be open-sourced in near future to help researchers to build more advanced researcher. We will also promote these capabilities through extensive industry collaborations and update the list according to new hardware features.

References

[1] Z. Wei, H. Qu, Y. Wang, X. Yuan, H. Wu, Y. Du, K. Han, N. Zhang, and Z. Feng, "Integrated Sensing and Communication Signals Toward 5G-A and 6G: A Survey," *IEEE Internet of Things Journal*, vol. 10, no. 13, pp. 11 068–11 092, 2023.

[2] B. Yu, Y. Wang, K. Niu, Y. Zeng, T. Gu, L. Wang, C. Guan, and D. Zhang, "WiFi-Sleep: Sleep Stage Monitoring Using Commodity Wi-Fi Devices," *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 13 900–13 913, 2021.

[3] Z. Chen, T. Zheng, C. Cai, and J. Luo, "MoVi-Fi: Motion-Robust Vital Signs Waveform Recovery via Deep Interpreted RF Sensing," in *Proc. of the 27th ACM MobiCom*, 2021, pp. 392–405.

[4] Y. Zheng, Y. Zhang, K. Qian, G. Zhang, Y. Liu, C. Wu, and Z. Yang, "Zero-Effort Cross-Domain Gesture Recognition with Wi-Fi," in *Proc. of the 17th ACM MobiSys*, 2019, p. 313–325.

[5] Y. Hu, F. Zhang, C. Wu, B. Wang, and K. J. R. Liu, "DeFall: Environment-Independent Passive Fall Detection Using WiFi," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8515–8530, 2022.

[6] C. Wu, B. Wang, O. C. Au, and K. R. Liu, "Wi-Fi Can Do More: Toward Ubiquitous Wireless Sensing," *IEEE Communications Standards Magazine*, vol. 6, no. 2, pp. 42–49, 2022.

[7] F. Gringoli, M. Schulz, J. Link, and M. Hollick, "Free your csi: A channel state information extraction platform for modern wi-fi chipsets," in *Proc. of the 13th ACM WiNTECH*, 2019, p. 21–28.

[8] Z. Wang, K. Han, X. Shen, W. Yuan, and F. Liu, "Achieving the Performance Bounds for Sensing and Communications in Perceptive Networks: Optimal Bandwidth Allocation," *IEEE Wireless Communications Letters*, vol. 11, no. 9, pp. 1835–1839, 2022.

[9] S. Tan, Y. Ren, J. Yang, and Y. Chen, "Commodity WiFi Sensing in Ten Years: Status, Challenges, and Opportunities," *IEEE Internet of Things Journal*, vol. 9, no. 18, pp. 17 832–17 843, 2022.

[10] Z. Chen, T. Zheng, and J. Luo, "Octopus: A Practical and Versatile Wideband MIMO Sensing Platform," in *Proc. of the 27th ACM MobiCom*, 2021, pp. 601–614.

[11] Y. Ma, G. Zhou, and S. Wang, "WiFi Sensing with Channel State Information: A Survey," *ACM Computer Survey*, vol. 52, no. 3, pp. 1–36, jun 2019.

[12] F. Liu, Y. Cui, C. Masouros, J. Xu, T. X. Han, Y. C. Eldar, and S. Buzzi, "Integrated Sensing and Communications: Toward Dual-Functional Wireless Networks for 6G and Beyond," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 6, pp. 1728–1767, 2022.

[13] IEEE 802.11 WG, "Amendment 2: Enhancements for Wireless LAN Sensing," *IEEE P802.11bf D0.1*, 2022.

[14] C. Chen, H. Song, Q. Li, F. Meneghello, F. Restuccia, and C. Cordeiro, "Wi-Fi Sensing Based on IEEE 802.11bf," *IEEE Communications Magazine*, vol. 61, no. 1, pp. 121–127, 2023.

[15] Z. Jiang, T. H. Luan, X. Ren, D. Lv, H. Hao, J. Wang, K. Zhao, W. Xi, Y. Xu, and R. Li, "Eliminating the Barriers: Demystifying Wi-Fi Baseband Design and Introducing the PicoScenes Wi-Fi Sensing Platform," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4476 – 4496, 2022.

Biography

Rui Li is a Professor and the Vice Dean of the School of Computer Science and Technology, Xidian University. His research interests include Wi-Fi ISAC and signal processing.

Yu Duan and **Daiyang Zhang** are PhD students with the School of Computer Science and Technology, Xidian University. Their research interests include Wi-Fi ISAC, ultra-wideband sensing.

Rui Du and **Yiyan Zhang** are Senior Research Engineers with the Wireless Technology Laboratory, Huawei Technologies Co., Ltd. Their current research interests include wireless communication, ISAC, and standardization of wireless communication.

Fangxin Xu is a Senior Manager with the Department of Technical Planning, Shenzhen Longsailing Semiconductor Co. Ltd. He is a Voting Member of the IEEE 802.11 Working Group. His research interests include next-gen wireless LAN, and full-duplex technology.

Hangbin Zhao is a Senior System Architect with the Department of Home and Short-Range Communication Connectivity Technology, China Mobile Information Technology Co., Ltd. He is an enterprise standard setter for CMCC, and a Voting Member of the IEEE 802.11 Working Group.

Yang Sun is a Senior Member with the International Accreditation Team, State Radio Spectrum Management Center, China. He has over a decade of testing experience in wireless communication technology, primarily focusing on WFA certification and interoperability testing.

Yiming Liu is a Graduate students with the School of Computer Science and Technology, Xidian University. Her research interests include Wi-Fi sensing and radar imaging.

Zhiping Jiang is an Associate Professor with the School of Computer Science and Technology, Xidian University, and is the founder of PicoScenes Wi-Fi ISAC research platform. His research interests include Wi-Fi ISAC and signal processing.

Tony Xiao Han is a Research Expert and Project Manager with the Wireless Technology Laboratory, Huawei Technologies Co. Ltd. He chairs the IEEE 802.11bf WLAN Sensing Task Group, and serves as the Founding Industry Chair of IEEE ComSoc ISAC ETI and the Vice Chair of IEEE WTC SIG on ISAC.