Enhanced Wireless Sensing by Exploiting Opportunistic 5G-NR Signals

Rui Peng, Yafei Tian, and Shengqian Han
School of Electronics and Information Engineering, Beihang University
37 Xueyuan Road, Haidian District, Beijing 100191, P. R. China
E-mail: pengrui@buaa.edu.cn; ytian@buaa.edu.cn; sqhan@buaa.edu.cn

***Abstract*—Wireless sensing through opportunistic signals offers distinct advantages in diverse fields. Compared with 4G long term evolution (LTE), 5G new radio (NR) signal possesses larger bandwidth and more antenna ports, thus is a better candidate for wireless sensing. However, the commercial NR signals have not been widely exploited due to the absence of off-the-shelf modem for channel state information (CSI) extraction and intricate high-layer signaling interaction procedures to obtain the reference signal parameters. For this purpose, we present a channel feature based blind detection method that identifies complete CSI reference signal (CSI-RS) parameters solely from physical layer, which enables opportunistic exploitation of commercial NR signal and full-bandwidth multi-port CSI acquisition. The simulation results demonstrate the superiority of the proposed CSI-RS blind detection method in frequency-selective channel. Furthermore, a prototype system is built to showcase the enhanced sensing ability of commercial NR signal.**

***Index Terms*—Wireless sensing, 5G-NR signal, CSI-RS, blind detection, prototype.**

I. Introduction

Wireless sensing is a promising research area in recent years. As a complementary means to visual perception, wireless sensing offers distinct advantages in health monitoring, human-machine interaction, and obstacle penetrating imaging, etc [1]. Leveraging the opportunistic signal for sensing purposes will save the requests for infrastructure construction and spectrum authorization [2].

At present, the popular opportunistic signals are Wi-Fi and 4G long term evolution (LTE). Wi-Fi has ubiquitous indoor coverage and convenient off-the-shelf network interface cards to extract channel state information (CSI) [3]. This has sparked a large number of researches on Wi-Fi sensing [4], [5]. However, Wi-Fi is packet-based burst transmission, and works in unauthorized frequency bands, where co-channel interference may degrade the sensing performance [6].

As a kind of cellular signal, LTE has strict frame structure and spectrum authorization, as well as good coverage both indoors and outdoors. The cell-specific reference signal (CRS) of LTE is an always-on signal with transparent format for CSI acquisition [7], [8]. In addition, due to the overlapping coverage of multiple base stations, the robustness of sensing can be improved [9].

Compared to LTE, 5G new radio (NR) signal has broader spectrum occupation. The higher frequency band, including millimeter wave, is beneficial for recognizing more refined motions. NR also has significant improvements in bandwidth and antenna port number. Through CSI reference signal (CSI-RS), the channel can be measured in full signal bandwidth and multiple transmission ports. This will largely improve the multi-user sensing or interference suppression capability, as well as the positioning accuracy or imaging resolution.

Although many works consider using 5G-NR signals for wireless sensing [10], few studies have utilized commercial NR signals, because only the reference signal in the synchronization signal block (SSB) has transparent format, which can be directly used to estimate CSI [11], [12]. Unfortunately, SSB only occupies 20 resource blocks (RBs), corresponding to 3.6 MHz or 7.2 MHz bandwidth in typical sub-6 GHz settings, even narrower than LTE signal. In fact, acquiring CSI-RS configuration is a unique issue in NR, since the 5G base station (gNB) can flexibly configure the CSI-RS [13], and gNB notifies CSI-RS configuration to user equipment (UE) through the radio resource control (RRC) signaling. To complete the RRC interaction by a prototype receiver, an intact NR protocol stack in high-layer should be implemented. In addition, as gNB only assigns the bandwidth part (BWP) for a dedicated UE [14], even an authorized user may only acquire the configuration information in part of the bandwidth. Therefore, a question arises of whether it is possible to utilize the full bandwidth commercial NR as an opportunistic signal for wireless sensing?

In practical networks, it is costly to configure a separate set of CSI-RS for each UE. Typically, the gNB will transmit some sets of CSI-RS shared by all UEs. Each set usually occupies full bandwidth and transmits periodically with an invariant configuration, likes an always-on signal. That means, once we find the CSI-RS configuration, we can continually use it to acquire CSI, as using the CRS in LTE.

In this work, we present a blind detection method to identify the CSI-RS parameters in the downlink NR signal, which enables us to achieve wireless sensing through commercial NR signal. Leveraging the channel characteristic and NR specification constraints, we detect the complete CSI-RS parameters in a unified framework. Both simulation and practical prototype experiments are conducted to demonstrate the superiority of the proposed scheme, as well as the enhanced sensing capability provided by commercial NR signal.

The contributions of this work are summarized as follows:

1) We propose a CSI-RS blind detection approach capable of detecting all CSI-RS parameters without RRC signal-

ing. This scheme supports both single-port and multi-port CSI-RS configurations.

2) By introducing a channel continuity indicator, the proposed CSI-RS sequence search scheme exhibits robustness against frequency selectivity across the full bandwidth. Simulation results demonstrate that our blind detection approach performs well even in low signal-to-noise ratio (SNR) and severe frequency-selective fading channel.
3) We build a prototype system to receive 5G-NR signal from the commercial base stations. Through a wireless gesture recognition example, we demonstrate the enhanced discrimination and sensing ability of NR signal.

II. System Model

A. Channel Model

The time-variant channel response can be characterized as the summation of static channel, including the line of sight (LoS) path and reflections for stationary objects, along with dynamic paths generated by human movement. For angular frequency ω and time t, the CSI can be represented as

$$h(\omega,t) = e^{j\theta_{\mathrm{n}}(t)}\left[h_{\mathrm{s}}(\omega) + h_{\mathrm{d}}(\omega,t)\right] + n(\omega,t), \tag{1}$$

where $\theta_{\mathrm{n}}(t)$ denotes the phase noise, $h_{\mathrm{s}}(\omega)$ and $h_{\mathrm{d}}(\omega,t)$ correspond to the static and dynamic channels, respectively, $n(\omega,t)$ represents the white noise. In wireless sensing applications, by extracting $h_{\mathrm{d}}(\omega,t)$, we can further recognize the environmental variation and human activities.

B. NR Basis

An NR frame has a duration of 10 ms and consists of 10 subframes. The downlink signal utilizes the orthogonal frequency division multiplexing (OFDM) mechanism, where the resource element (RE) is the minimum resource unit. In the time domain, an RE occupies one OFDM symbol. In the frequency domain, it spans one subcarrier. The symbol number and subcarrier spacing (SCS) are flexible according to the numerology configuration μ, as listed in Table I [13]. In frequency range 1 (FR1, sub-6 GHz bands), numerology 0 to 2 are supported, resulting in a maximum bandwidth of 100 MHz [14]; in frequency range 2 (FR2, millimeter-wave bands), numerology 2 to 4 are supported, the maximum bandwidth can reach 400 MHz [15].

In addition, NR signal has wider occupation in the radio-frequency spectrum. As an example, Fig. 1 illustrates the in-operation commercial LTE and NR bands in a local area, where the labels "Bx" and "Nx" denote the band number of LTE and NR, respectively. It can be seen that all operating LTE bands are below 3 GHz, while NR is extensively deployed in 0-5 GHz. The millimeter wave band has not yet been commercialized locally, so that we do not show this range. The higher radio frequency introduces larger Doppler shift, which facilitates fine-grained human activity recognition. Furthermore, if we can splice the CSI measurements from multiple frequency bands, it is possible to derive extra-high resolution power delay profiles, so that the precision of localization, mapping, and imaging can be substantially enhanced [16].

TABLE I
FRAME PARAMETERS

Definition	Symbol	Value
numerology	μ	0,1,...,4
SCS	Δ_f	$15 \cdot 2^{\mu}$ kHz
slot number in a frame	$N_{\mathrm{slot}}^{\mathrm{frame},\mu}$	$10 \cdot 2^{\mu}$
symbol number in a slot	$N_{\mathrm{symb}}^{\mathrm{slot}}$	14
subcarrier number in an RB	$N_{\mathrm{sc}}^{\mathrm{RB}}$	12

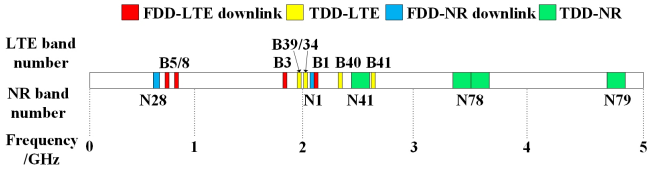

Fig. 1. The spectrum of commercial LTE and NR bands in a local area.

In NR, two types of reference signal are commonly employed, which are demodulation reference signal (DM-RS) and CSI-RS. The DM-RS is utilized for demodulation of the physical downlink control channel (PDCCH), physical downlink shared channel (PDSCH) and SSB [13]. It is transmitted alongside PDSCH/PDSCH/SSB. The DM-RSs in PDCCH and PDSCH are not suitable for wireless sensing since they only present when UEs request downlink data. The DM-RS inserted in SSB serves as an always-on signal, but its bandwidth is limited.

The CSI-RS is designed for time-frequency tracking, cell measurement and beam management, which supports full bandwidth and a maximum of 32 antenna ports. However, its format is not transparent to listeners. The related parameters are flexibly configured by the gNB, which determines the resource mapping and local sequence generation. Therefore, to estimate the CSI, the first priority is to obtain the CSI-RS configuration parameters.

III. CSI-RS Blind Detection

CSI-RS supports periodic, semi-persistent and aperiodic transmissions. In this work, our primary focus is on detecting the periodic CSI-RS, as it enables us to consistently acquire the CSI for sensing applications. CSI-RS configuration includes a series of parameters, as listed in Table II.

The challenge of CSI-RS blind detection lies in searching for local sequences, which are determined by the scrambling identification (ID), port number and multiplexing type. In the wideband scenario, the received CSI-RS not only depends on the local sequence, but also related to the frequency-selective channel. Before searching the local sequence, we can initially detect the time-frequency resource occupation of CSI-RS owing to its periodicity.

A. Resource Occupation Detection

We assume that the basic system information such as cell ID, numerology, common reference point (point A) and the number of RB N_{RB} is obtained through cell searching and the broadcast information. The master information block

TABLE II
CSI-RS PARAMETERS

Variable	Candidates	Explanation
X	1,2,4,6,8,12,16,24,32	antenna port number
n_{ID}	[0, 1023]	scrambling ID
T_{per}	4,5,8,10,16,20,32,40, 64,80,160,320,640 slots	period
T_{off}	$[0, T_{\text{per}}-1]$	slot offset
l_0	[0, 13]	starting symbol inside a slot
k_i	[0, 11]	starting subcarrier inside an RB for CDM group i
ρ	0.5,1,3	density, explained in Fig. 2
CDM type	*no-CDM,CDM4(FD2,TD2), FD-CDM2,CDM8(FD2,TD4)*	multiplexing type

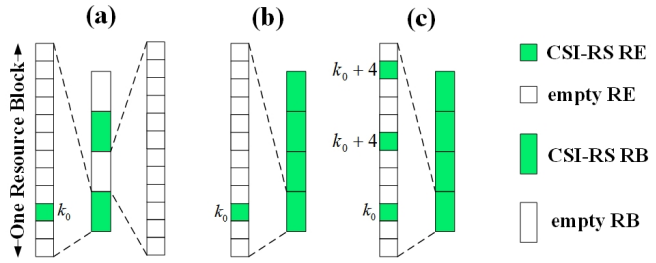

Fig. 2. Three examples of single-port CSI-RS transmission scheme. (a) $\rho = 0.5$. (b) $\rho = 1$. (c) $\rho = 3$.

(MIB) and system information block (SIB) are periodically transmitted and can be decoded by any listeners.

Then, we can try to find in which positions, i.e., symbols and subcarriers, the CSI-RS sequence are located. As shown in Table II and Fig. 2, CSI-RS may have different parameter setups for transmission period, density, slot offset, starting symbol and subcarrier. To detect these parameters, the periodicity in time domain is utilized, so that a correlation peak can be found by cross-correlation and accumulation.

Although the CSI-RS is periodically transmitted, the local sequence depends on the symbol index within a frame. Only when the time interval between two transmissions is an integer multiple of the frame length, their sequences are the same. Thus we utilize a long interval of $T_{\text{slot}}^{\max}$ slots, which is determined as the least common multiple of both CSI-RS period candidate and $N_{\text{slot}}^{\text{frame},\mu}$, to ensure that the CSI-RSs with interval of $T_{\text{slot}}^{\max}$ slots always share the same local sequence.

Denote the received signal in subcarrier k and symbol l as $y(k,l)$. Assume that we have received a period of data with $T_{\text{sym}}^{\max}$ symbols, where $T_{\text{sym}}^{\max} = T_{\text{slot}}^{\max} N_{\text{symb}}^{\text{slot}}$. The cross correlation is operated in an RE grid with the size of $N_{\text{RB}} N_{\text{sc}}^{\text{RB}} \times T_{\text{sym}}^{\max}$, which can be expressed as

$$r(\bar{k}, l, \bar{n}) = y(\bar{n} N_{\text{sc}}^{\text{RB}} + \bar{k}, l) \cdot y^*(\bar{n} N_{\text{sc}}^{\text{RB}} + \bar{k}, l + T_{\text{sym}}^{\max}), \quad (2)$$

where $\bar{k} \in [0, N_{\text{sc}}^{\text{RB}} - 1]$ is the subcarrier index within an RB, $l \in [0, T_{\text{sym}}^{\max} - 1]$ is the symbol index, $\bar{n} \in [0, N_{\text{RB}} - 1]$ is the RB index, and $(\cdot)^*$ represents conjugate operation. The correlation value in the even or odd RB is separately summed, as

$$r_{\text{x}}(\bar{k}, l) = \sum\nolimits_{\bar{n} \in \mathcal{I}_{\text{x}}} r(\bar{k}, l, \bar{n}), \quad (3)$$

where 'x' denotes either 'odd' or 'even', and $\mathcal{I}_{\text{x}}$ denotes the corresponding odd or even RB indices. As illustrated in Fig. 2(a), when CSI-RS density ρ is set as 0.5, the CSI-RS is only allocated in even or odd RBs, while when $\rho = 1$ or 3, there is CSI-RS in every RBs. By comparing $r_{\text{even}}(\bar{k}, l)$ with $r_{\text{odd}}(\bar{k}, l)$, and checking the peak number and positions in an RB, we can identify the density parameter ρ, as well as the starting subcarrier k_0 in single-port case. Then according to the peaks in time domain, we can extract the candidate set $\mathcal{L}_{\text{c}}$ that involves CSI-RS symbols.

B. Local Sequence Searching

After obtaining the candidate symbol set, the local sequence need to be solved, along with the number of ports, and multiplexing type in each symbol. Since the single-port and multi-port CSI-RSs have different resource mapping rules, we adopt different detection procedures for them. That is to say, we will first find all single-port CSIs in the candidate symbols, and then detect multi-port CSI-RSs in the remaining symbols. The complete procedure is summarized in Fig. 3.

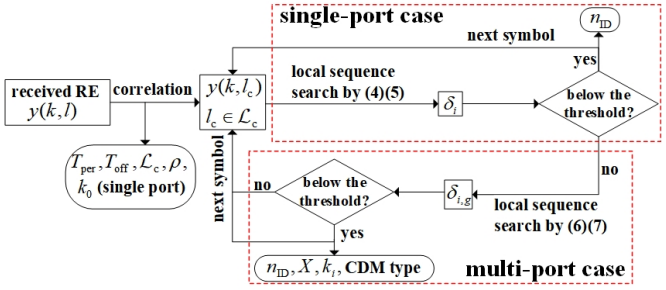

Fig. 3. The overall procedure of CSI-RS blind detection.

1) Single-port case: As illustrated in Fig. 2, the CSI-RS is mapped with a uniform interval of $N_{\text{sc}}^{\text{RB}}/\rho$, and occupies $N_{\text{RS}} = \lfloor \rho N_{\text{RB}} \rfloor$ REs in total. The CSI-RS employs a pseudo random sequence with a given generator polynomial [13], whose 31-bit initial state is generated as the binary value of

$$c_{\text{init}} = \left(2^{10}(N_{\text{symb}}^{\text{slot}} n_{\text{s,f}}^{\mu} + l_0 + 1)(2n_{\text{ID}} + 1) + n_{\text{ID}}\right) \mod 2^{31}.$$

For a certain candidate symbol $l_{\text{c}} \in \mathcal{L}_{\text{c}}$, $l_0 = l_{\text{c}} \mod N_{\text{symb}}^{\text{slot}}$ and $n_{\text{s,f}}^{\mu} = \lfloor l_{\text{c}}/N_{\text{symb}}^{\text{slot}} \rfloor \mod N_{\text{slot}}^{\text{frame},\mu}$, so the local sequence uniquely depends on the scrambling ID n_{ID}. A straightforward approach involves correlating the received CSI-RS with every possible local sequence and subsequently identifying the one that exhibits the highest correlation value. However, the frequency-selective channel may introduce amplitude attenuation and phase rotation in the received signal, thereby deteriorating the detection performance.

Therefore, the channel characteristic should be considered when searching for the local sequence. Given a scrambling ID $i \in [0, 1023]$, we can generate a local sequence of CSI-RS $x_i(n, l_{\text{c}})$, where $n \in [0, N_{\text{RS}} - 1]$ denotes the CSI-RS RE index. Let us first estimate the channel coefficients using this local sequence and the least square method, as

$$\hat{h}_i(n, l_{\text{c}}) = y(k(n), l_{\text{c}}) \cdot x_i^*(n, l_{\text{c}}), \quad (4)$$

where $k(n) = n N_{\text{sc}}^{\text{RB}}/\rho + k_0$ is the subcarrier index of the n-th CSI-RS RE. Although the channel is frequency-selective

across the full bandwidth, it is usually flat within a small bandwidth. The channel coefficients in adjacent REs should be very close. To examine whether the local sequence is correct, we can check the continuity of the coefficients. Thus we define a channel continuity indicator as

$$\delta_i = \sum_{n=0}^{N_{\text{RS}}-2} |\hat{h}_i(n+1, l_{\text{c}}) - \hat{h}_i(n, l_{\text{c}})|. \tag{5}$$

If the assumed scrambling ID is correct, δ_i will reach a minimum value. In addition, if the candidate symbol is a false alarm, there will be no distinct minimum among all 1024 calculated δ_i. A dynamic decision threshold δ_{th} is applied to assess the gap between the second and the first smallest value in δ_i. In this work, we adopt the triple standard deviation of δ_i as the threshold.

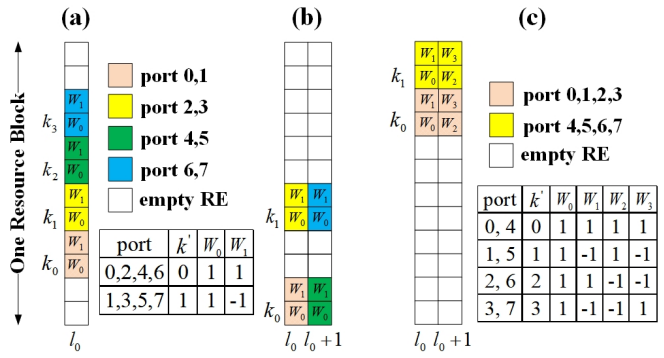

Fig. 4. Three types of 8-port CSI-RS transmission scheme. (a) 4 groups of FD-CDM2 in one symbol. (b) 4 groups of FD-CDM2 in two contiguous symbols. (c) Two groups of CDM4 (FD2,TD2) across two contiguous symbols.

2) Multi-port case: The multi-port case is more complicated, as the received CSI-RS comprises a superposition of signals transmitted via multiple ports, employing frequency division (FD), time division (TD) and code division multiplexing (CDM). These multiplexing mechanisms introduce additional parameters to be estimated, specifically the number of transmission ports and the multiplexing type. As an example, three multiplexing schemes for 8-port CSI-RS are illustrated in Fig. 4. Each scheme consists of either 4 or 2 CDM groups with each group including 2 or 4 ports. Summarizing the mapping rules of multi-port CSI-RS, there are some key requirements:

- A CDM group always occupies 2 contiguous subcarriers and starts from an even subcarrier, as shown in Fig. 4.
- For CDM4 or CDM8, there should be 2 or 4 contiguous symbols, as illustrated in Fig. 4(b) and 4(c).
- In each RB, all CDM groups use the same local sequence.

For the multi-port case, it is necessary to jointly estimate the port number, CDM type, occupied subcarriers and scrambling ID. According to the first rule, each RB contains 6 potential CDM groups. For the g-th group occupying subcarriers $[2g, 2g+1]$, we extract the corresponding REs from 1, 2 or 4 contiguous symbols to create a vector $\mathbf{y}_g(n, l_{\text{c}}) \in \mathbb{C}^{P\times 1}$ with the orthogonal code length $P \in \{2, 4, 8\}$, corresponding to CDM2, CDM4 and CDM8, respectively.

We enumerate the scrambling ID to generate the local sequence, then the channel coefficient of the n-th RB can be estimated through correlation with the local sequence as

$$\hat{h}_{i,g,p}(n, l_{\text{c}}) = \mathbf{x}_{i,p}^H(n, l_{\text{c}})\mathbf{y}_g(n, l_{\text{c}}), \tag{6}$$

where $\mathbf{x}_{i,p}(n, l_{\text{c}})$ represents the local sequence for orthogonal code index $p \in [0, P-1]$, $(\cdot)^H$ denotes the conjugate transpose of a vector. For each CDM group, we can obtain the channels of P ports. Thus, the channel continuity indicator in each CDM group is the summation of P ports as

$$\delta_{i,g} = \sum_{p=0}^{P-1} \sum_{n=0}^{N_{\text{RS}}-2} |\hat{h}_{i,g,p}(n+1, l_{\text{c}}) - \hat{h}_{i,g,p}(n, l_{\text{c}})|. \tag{7}$$

To determine whether a potential CDM group is a valid CSI-RS group, we employ the same threshold criteria as in the single-port case, verifying the minimum values in $\delta_{i,g}$.

C. Complexity Analysis

The computation complexity of CSI-RS blind detection can be analyzed in two stages. In the resource occupation detection stage, the computation mainly arises from the element-wise multiplication in the frequency-domain. For every $T_{\text{sym}}^{\max}$ symbols, we perform $T_{\text{sym}}^{\max} N_{\text{sc}}^{\text{RB}} N_{\text{RB}}$ multiplications.

In the local sequence searching stage, we need to consider 1024 possible scrambling IDs for each candidate CSI-RS symbol. Therefore, for single-port detection, we only perform $1024 N_{\text{RS}}$ multiplications. In multi-port cases, the channel estimation is carried out for P ports in all 6 potential frequency locations, resulting in a complexity of $6144 P N_{\text{RS}}$.

IV. Evaluations

We first verify the performance of CSI-RS blind detection by simulations. Then, we conduct the prototype experiments to demonstrate the potential of wireless sensing through commercial NR signals.

A. CSI-RS Detection Performance Simulations

In the simulation system, we assess the detection probability of CSI-RS blind detection with the influence of SNR and bandwidth. Each SNR-bandwidth configuration undergoes 10,000 tests. During each test, we generate the local sequence of CSI-RS according to the specification [13] with a random scrambling ID. The transmission signal is centered in 3.45 GHz, with a SCS of 30 kHz and a maximum bandwidth of 100 MHz. The received signal experiences an indoor non-line of sight (NLoS) channel and is superimposed with white Gaussian noise. We employ the clustered delay line (CDL) model [17] to approximate the real channel environment, where the delay spread DS, measured in seconds, follows a log-normal distribution, as $\lg(DS) \sim \mathcal{N}(-7.35, 0.014)$. The mean value of delay spread corresponds to a coherent bandwidth of 22.6 MHz, which is substantially narrower than the maximum system bandwidth, indicating that the channel exhibits frequency selectivity.

For comparison, we choose the correlation based blind detection [18] as the baseline. Notably, this baseline is limited to single-port cases. Therefore, we provide the comparison

specifically for single-port case. Additionally, we also present the error detection probabilities of the proposed method in multi-port cases.

In the single-port scenario, the CSI-RS transmission density ρ is set as 3. In real network, the gNB typically configures 4 sets of single-port CSI-RS across the consecutive slots, forming a group of tracking reference signal (TRS). We consider bandwidth configurations of 20 MHz, 50 MHz and 100 MHz, corresponding to 51, 133 and 273 RBs [14]. In each test, any mismatch between the detected and actual scrambling ID is considered a false detection. The resulting error detection probabilities are presented in Fig. 5.

As the SNR improves, the proposed method could eventually achieve an error detection probability of 0. In low SNR situation, a larger bandwidth exhibits better performance. Particularly, even at an SNR of -4 dB, a bandwidth of 100 MHz achieves 100% accuracy. However, the correlation based method converges to a non-zero error rate. In addition, when the bandwidth increases to 100 MHz, its accuracy degrades instead. This result demonstrates that the phase rotation in the frequency-selective channel may weaken the correlation peak, thereby deteriorating the performance of correlation detection.

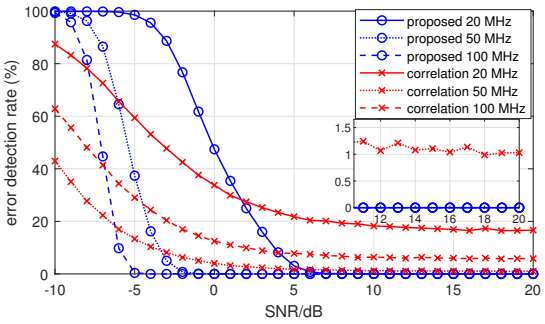

Fig. 5. Single-port CSI-RS error detection probabilities.

In the multi-port scenarios, both 2-port and 8-port CSI-RS configurations are considered, with a density of 1 and occupying one symbol in the time domain. Typically, the 2-port and 8-port are used in indoor and outdoor base stations, respectively. Any mismatch in either port number or scrambling ID is counted as a false detection. The error detection probabilities are presented in Fig. 6.

Regardless of the port number, the error rates converge to 0 in all bandwidth configurations. There is an SNR gap of $2 \sim 3$ dB between the 2-port and 8-port cases. With 100 MHz bandwidth, the proposed method could achieve 100% detection accuracy at -6 dB in 2-port case, and -4 dB in 8-port case.

B. CSI-RS Detection of Commercial NR Signals

In the prototype experiment, we receive the commercial NR signals in an apartment as shown in Fig. 7. The prototype receiver is built on a software defined radio platform YunSDR Y550s, which supports 4 Rx antennas with a sampling rate of 122.88 MHz. The baseband signal is processed on a host computer.

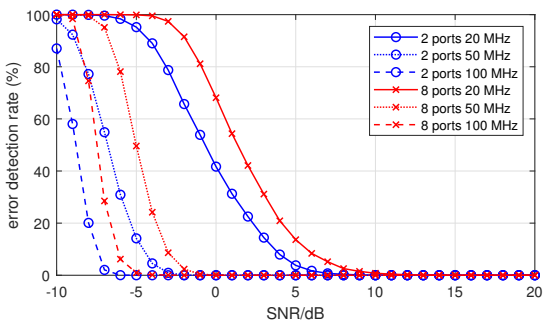

Fig. 6. Multi-port CSI-RS error detection probabilities of the proposed method.

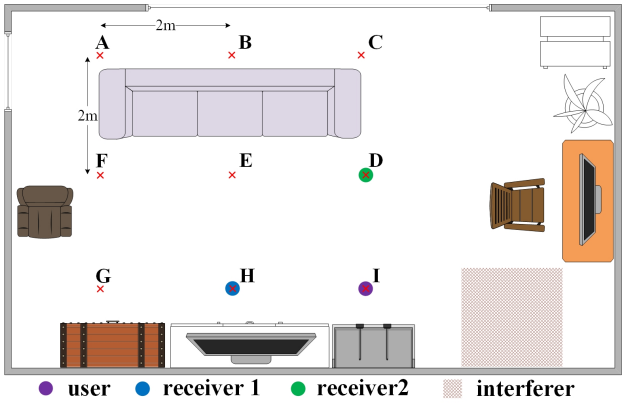

Fig. 7. The layout of the experiment environment.

We discover the commercial NR signals in 4 commonly used bands, N1, N28, N41 and N78. We set the correlation interval $T_{\text{slot}}^{\max}$ to 160 slots. The cell configuration and CSI-RS detection results in each band are presented in Table III.

Fig. 8 exhibits some intermediate results of CSI-RS detection in N78 band. In Fig. 8(a), cross-correlation results reveal several peaks. There are 4 sets of CSI-RS for single-port and another 4 sets for 8-port transmissions. Each single-port CSI-RS set exhibits 4 adjacent peaks with similar heights every 560 symbols, indicating a period of 40 slots. Whereas the 8-port CSI-RSs exhibit 4 peaks with different heights every 2240 symbols, corresponding to a period of 160 slots. The peak difference may attribute to the precoding matrices used for different set of CSI-RSs when the total antenna ports in gNB is much more than 8. In addition, there are some false alarms caused by the periodic SIBs. The scrambling ID searching results for the single-port case are shown in Fig. 8(b). We can observe that with the correct n_{ID}, the channel continuity indicator exhibits an evident small value. The same trend can be found in multi-port case as shown in Fig. 8(c), where the n_{ID} can be detected in 4 CDM groups, indicating an 8-port CSI-RS set. Using the CSI-RS parameters, we can acquire the CSI of each port in full bandwidth. A CSI waveform of the 100 MHz bandwidth is presented in Fig. 8(d), where the fluctuations around $t = 1$ s are caused by a hand waving disturbance.

TABLE III
CSI-RS DETECTION RESULTS

Band	N1	N28	N41					N78							
Operator*	CU, CT	CM, CBN	CM, CBN					CU, CT							
Center frequency	2.12 GHz	773 MHz	2.565 GHz					3.45 GHz							
Cell ID	19	236	65,241					222							
Bandwidth	20 MHz	30 MHz	100 MHz					100 MHz							
SCS	15 kHz	15 kHz	30 kHz					30 kHz							
X	4	4	1	8				1				8			
k_i	0,2	8,10	0	0,2,4,6				0				0,2,4,6			
ρ	1	1	3	1				3				1			
CDM type	CDM2	CDM2	noCDM	CDM2				noCDM				CDM2			
n_{ID}	19	236	65,241	101	102,278	103,279	104	222	222	222	222	222	222	222	222
$T_{\text{CSI-RS}}$	40	40	40	40	40	40	40	40	40	40	40	160	160	160	160
T_{offset}	1	3	1	0	10	20	30	5	5	6	6	0	10	20	30
l_0	13	13	13	13	13	13	13	4	8	4	8	13	13	13	13

*CU - China Unicom, CT - China Telecom, CM - China Mobile, CBN - China Broadcasting Network.

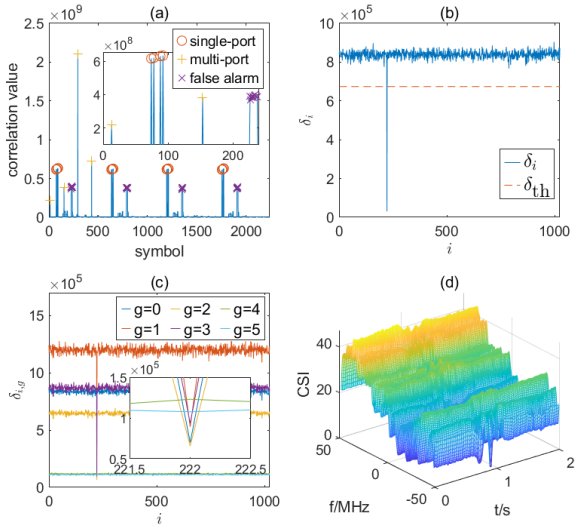

Fig. 8. An example of CSI-RS detection in N78 band. (a) Cross-correlation result. (b) Scrambling ID searching for single-port CSI-RS. (c) Scrambling ID searching for multi-port CSI-RS. (d) Full bandwidth CSI waveform.

C. Wireless Sensing Applications

Resorting to the large bandwidth and multi-port transmission, NR signal has great potential to inhibit interference or separate multiple users in spatial and delay domains. To evaluate the discrimination ability of NR signal, let us first conduct a correlation test among the CSIs captured from 9 different positions, as the points A∼I marked in Fig. 7.

In this test, we collect the 8-port CSI-RSs for a duration of 8 seconds at each position, and then extract their principal component in $8N_{\text{RS}}$ dimensions. The inner products are calculated and the correlation values among different positions are obtained. As a comparison, we also evaluated the channel correlations using only 2 ports and the central 20 MHz bandwidth, which is a common configuration in LTE signals. The results are presented in Fig. 9.

It can be seen that the distribution of channel correlations does not follow a regular pattern, due to the intricate indoor propagation. Nevertheless, with the increased number of Tx ports and bandwidth, the channel correlation noticeably diminishes. In the 8-Tx and 100 MHz configuration, some positions

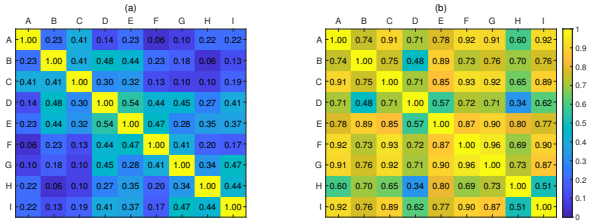

Fig. 9. A comparison of channel correlation in different bandwidth and antenna port. (a) 8-Tx, 100 MHz bandwidth. (b) 2-Tx, 20 MHz bandwidth.

exhibit nearly orthogonal channel responses, highlighting the strong discrimination capability of the NR signal. On the contrary, in the 2-Tx and 20 MHz configuration, the channel correlations are noticeably higher, even for distant points, such as A-I or C-G.

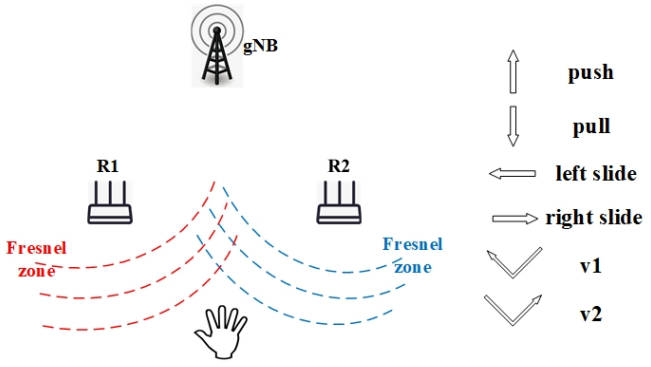

Fig. 10. Candidate gestures and user position.

We next demonstrate an example of wireless gesture recognition using commercial NR signal. As depicted in Fig. 7, we deploy two receivers to recognize 2-D gestures. Each receiver is equipped with 2 antennas for phase noise elimination. We design six gestures including push, pull, left slide, right slide, v1 (from right to left) and v2 (from left to right), as shown in Fig. 10. These gestures are performed 50 times each.

In addition to the regular interference-free scenario, we also test in a disturbed environment where an interferer shakes his body or walks in the marked area in Fig. 7. The human body, being a large moving object compared to a hand, introduces

significant interference to the dynamic channel response. We utilize the single-port CSI-RS in N78 band, since it has a period of 20 ms and can sense the Doppler shift from -25 Hz to 25 Hz. The interference mitigation capability relies on the resolution in delay domain. Using inverse fast Fourier transform (IFFT), we transform the frequency domain channel into the delay domain. According to the delay difference between the user and interferer, the reflection of them can be separated to various delay bins. We focus only on the bins where the hand reflection are concentrated on, excluding the interferer's reflections. In addition, the imperfection introduced by hardware should be considered. The CSI denoising and gesture identification procedures are detailed in [19].

In comparison, we also provide the result when acquiring CSI from the DM-RS in SSB [11], [12]. The SSB is centered in 3.40896 GHz, with a bandwidth of 7.68 MHz. Except for the CSI sources, the rest processings are the same for both schemes.

The recognition accuracies are presented in Fig. 11. Without interference, both schemes can achieve exceptionally high accuracies. The proposed CSI-RS based method has slightly better performance than that of SSB DM-RS based method. Even under the disturbed environment, the full bandwidth CSI provided by CSI-RS maintains good recognition performance, whereas a significant accuracy decline is observed in the SSB DM-RS based scheme, since the bandwidth of SSB is too narrow to provide enough delay resolution. The results highlight the importance to exploit CSI-RS, as well as the practicability of gesture recognition based on commercial NR signals.

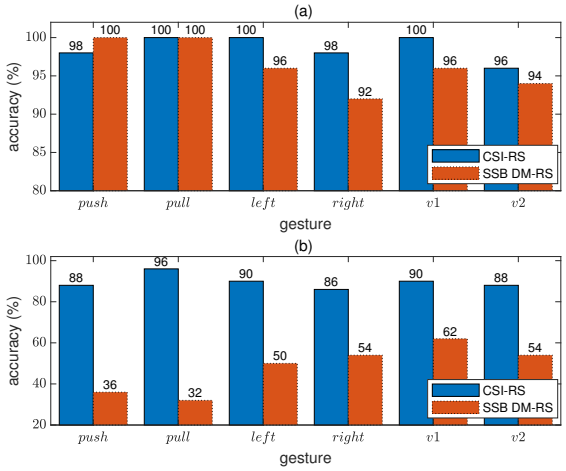

Fig. 11. Gesture recognition results. (a) Interference-free scenario, CSI-RS 98.7%, SSB DM-RS 96.3%. (b) Disturbed scenario, CSI-RS 89.7%, SSB DM-RS 48%.

V. Conclusion

In this study, we proposed the blind detection of CSI-RS and achieved wireless sensing through commercial NR signal. Leveraging the periodicity and specification constraints, we were able to detect complete CSI-RS parameters without RRC signaling. Specifically, by introducing the channel continuity indicator, the proposed blind detection method was robust to the frequency selectivity in wideband channels. The prototype experiments showcased the detection results in multiple commercial NR bands. With large bandwidth and multi-port transmission, we also demonstrated the strong discrimination ability of the NR signal. This work introduces a new tool for acquiring ubiquitous CSI, and will benefit various wireless sensing applications.

Acknowledgment

This work was supported by the National Natural Science Foundation of China under Grant 61971023.

References

[1] B. Wang, Q. Xu, C. Chen, F. Zhang, and K. R. Liu, "The promise of radio analytics: A future paradigm of wireless positioning, tracking, and sensing," *IEEE Signal Process. Mag.*, vol. 35, no. 3, pp. 59–80, May 2018.

[2] 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 J. Sel. Areas Commun.*, vol. 40, no. 6, pp. 1728–1767, Jun. 2022.

[3] F. Gringoli, M. Schulz, J. Link, and M. Hollick, "Free your CSI: A channel state information extraction platform for modern Wi-Fi chipsets," in *ACM WiNTECH*, 2019, pp. 21–28.

[4] S. Tan, Y. Ren, J. Yang, and Y. Chen, "Commodity WiFi sensing in ten years: Status, challenges, and opportunities," *IEEE Internet of Things J.*, vol. 9, no. 18, pp. 17 832–17 843, Sep. 2022.

[5] C. Chen, H. Song, Q. Li, F. Meneghello, F. Restuccia, and C. Cordeiro, "Wi-Fi sensing based on IEEE 802.11bf," *IEEE Commun. Mag.*, vol. 61, no. 1, pp. 121–127, Jan. 2023.

[6] J. Huang, B. Liu, C. Chen, H. Jin, Z. Liu, C. Zhang, and N. Yu, "Towards anti-interference human activity recognition based on WiFi subcarrier correlation selection," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6739–6754, Jun. 2020.

[7] S. Xu and Y. Tian, "Device-free motion detection via on-the-air LTE signals," *IEEE Commun. Lett.*, vol. 22, no. 9, pp. 1934–1937, Sep. 2018.

[8] W. Chen, K. Niu, D. Zhao, R. Zheng, D. Wu, W. Wang, L. Wang, and D. Zhang, "Robust dynamic hand gesture interaction using LTE terminals," in *ACM/IEEE IPSN*, 2020, pp. 109–120.

[9] Y. Feng, Y. Xie, D. Ganesan, and J. Xiong, "LTE-based pervasive sensing across indoor and outdoor," in *ACM SenSys*, 2021, pp. 138–151.

[10] Y. Chen, J. Zhang, W. Feng, and M.-S. Alouini, "Radio sensing using 5G signals: Concepts, state of the art, and challenges," *IEEE Internet of Things J.*, vol. 9, no. 2, pp. 1037–1052, Jan. 2022.

[11] Y. Ruan, L. Chen, X. Zhou, Z. Liu, X. Liu, G. Guo, and R. Chen, "iPos-5G: Indoor positioning via commercial 5G NR CSI," *IEEE Internet of Things J.*, vol. 10, no. 10, pp. 8718–8733, May 2023.

[12] L. Chen, X. Zhou, F. Chen, L.-L. Yang, and R. Chen, "Carrier phase ranging for indoor positioning with 5G NR signals," *IEEE Internet of Things J.*, vol. 9, no. 13, pp. 10 908–10 919, Jul. 2022.

[13] *Physical channels and modulation*, 3GPP TS 38.211 V15.2.0.

[14] *User Equipment (UE) radio transmission and reception; Part 1: Range 1 Standalone*, 3GPP TS 38.101 V15.2.0.

[15] *User Equipment (UE) radio transmission and reception; Part 2: Range 2 Standalone*, 3GPP TS 38.101 V15.2.0.

[16] Y. Xie, Z. Li, and M. Li, "Precise power delay profiling with commodity Wi-Fi," *IEEE Trans. Mob. Comput.*, vol. 18, no. 6, pp. 1342–1355, Jun. 2019.

[17] *Study on channel model for frequencies from 0.5 to 100 GHz*, 3GPP TR 38.901 V17.0.0.

[18] T. Wu, X. Yin, L. Zhang, and J. Ning, "Measurement-based channel characterization for 5G downlink based on passive sounding in sub-6 GHz 5G commercial networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 5, pp. 3225–3239, May 2021.

[19] R. Peng, Y. Tian, and S. Han, "ICI-free channel estimation and wireless gesture recognition based on cellular signals," *IEEE Wireless Commun. Lett.*, vol. 12, no. 12, pp. 2088–2092, Dec. 2023.