SNF-PRP: A Covert Integrating Sensing and Communications Framework

Dhrumil Bhatt*
Manipal Institute of Technology
Manipal Academy of Higher Education
Manipal, India
dhrumil.bhatt@gmail.com

Vidushi Kumar*
Manipal Institute of Technology
Manipal Academy of Higher Education
Manipal, India
vidushi.kumar705@gmail.com

***Abstract*—Integrated sensing and communication (ISAC) enables simultaneous sensing and data transmission but exposes a critical vulnerability: probing signals may be intercepted, revealing both the transmitted information and the act of sensing itself. Existing physical layer security approaches mitigate interception yet operate with detectable signals, leaving sensing activity observable to a passive warden. This paper introduces sub-noise-floor pseudo-random probing (SNF-PRP), a covert sensing framework for OFDM-based ISAC systems under an energy-detection adversary model. SNF-PRP establishes an ϵ-covertness guarantee via Kullback-Leibler (KL) divergence, exploits an N_{sc}-fold spreading gain absent from prior wideband analyses, and derives in closed form the minimum integration length required to achieve a target Cramér-Rao bound (CRB). Simulations under 5G NR n78 numerology confirm sub-0.5 m range and sub-0.5 m/s velocity accuracy with KL divergence $5.8\times$ below the covertness threshold, validating joint feasibility at $-12\,\mathrm{dB}$ and $-15\,\mathrm{dB}$ probing powers.**

***Index Terms*—Integrated sensing and communication, covert sensing, physical layer security, OFDM, 5G NR, Cramér-Rao bound, Kullback-Leibler divergence, pseudo-random noise, sub-noise-floor probing.**

I. Introduction

Integrated sensing and communication (ISAC) is a cornerstone of next-generation wireless systems, enabling environmental perception and data transmission to share spectrum and hardware [1]. Yet this integration introduces a security concern that has received little attention: sensing waveforms are deliberately radiated into the environment, exposing both the embedded information and the mere fact that sensing is occurring.

Existing physical layer security (PLS) work in ISAC focuses almost exclusively on protecting the communication channel via beamforming, artificial noise (AN) injection, and reconfigurable intelligent surfaces [1]–[3]. In all cases the probe operates above the noise floor and the security objective concerns the data payload, not the sensing activity itself. A recent RIS-ISAC-PLS survey [4] confirms no existing work addresses covertness of the sensing waveform: Zou et al. [5] come closest conceptually but establish no formal covertness guarantee, and LPI radar techniques [6], [7] offer only relative concealment without a KL-divergence analysis or communication overlay. A sufficiently sensitive radiometer can always detect a probe operating above the noise floor, exposing the act of sensing regardless of beamforming geometry or secrecy-rate constraints.

The proposed solution answers the resulting open question can sensing itself be made provably undetectable at the physical layer? affirmatively, by proposing *sub-noise-floor pseudo-random probing* (SNF-PRP) for OFDM-based ISAC in sub-6 GHz bands. A cryptographically seeded PRN sequence is superimposed on a standard downlink waveform below the instantaneous noise floor. A legitimate receiver with the seed performs coherent matched filtering and multi-symbol accumulation to recover sensing parameters; a passive warden without the seed is confined to radiometric energy detection the optimal Neyman Pearson test for two complex Gaussians differing only in variance [8], [9] -under which the probe is statistically indistinguishable from thermal noise.

SNF-PRP makes three contributions. *First*, it is, to the best of the authors' knowledge, the first framework to apply the KL divergence covertness criterion directly to the sensing probe waveform, establishing a provable covertness guarantee for sensing rather than communication. *Second*, it identifies an N_{sc}-fold spreading covertness gain (Lemma 1) absent from all prior wideband energy-detection analyses, yielding a correction factor exceeding 10^6 in the KL divergence. *Third*, it derives in closed form the three-way tradeoff among probing power Δ_p, integration length N^*, and Doppler resolution δ_v, and establishes the SNR invariance of Proposition 1: lower probing power simultaneously deepens covertness and preserves the sensing CRB target via proportionally increased N^*, with $\mathrm{SNR}_{\mathrm{eff}}$ at N^* unchanged. At $\Delta_p = -12$ dB the required $N^* = 191$ subframes corresponds to a 191 ms coherent integration window, feasible within the coherence time of a pedestrian target at 3.5 GHz and consistent with NR measurement gap structures.

II. System Model and Methodology

Consider a 5G NR downlink in which a base station (BS) serves a communication UE while simultaneously probing the environment. A legitimate sensing node shares a pre-distributed cryptographic seed s with the BS. A passive warden (Willie) monitors the channel but has no knowledge of s. The BS must jointly satisfy:

*Authors contributed equally to this work.

Algorithm 1 SNF-PRP: Sub-Noise-Floor Pseudo-Random Probing

Input: Shared seed s, probing power ratio Δ_p, integration length N, noise power σ^2
Output: Range estimate $\hat{R}$, velocity estimate $\hat{v}$

1: **// Transmitter (BS)**
2: Generate PRN: $c[k] \in \{-1, +1\},\ k = 0, \ldots, N_{\text{sc}} - 1$, seeded by s
3: **for** each symbol $m = 0$ **to** $N - 1$ **do**
4: Form overlay: $X_p[k, m] = \sqrt{P_p/N_{\text{sc}}}\, c[k]\, e^{j2\pi km/N_{\text{sc}}}$ with $P_p = \Delta_p \sigma^2$
5: Transmit $\mathbf{X}[m] = \mathbf{X}_c[m] + \mathbf{X}_p[m]$ ▷ probe buried $\Delta_p < 1$ below noise floor
6: **end for**
7: **// Channel**
8: Receive: $Y[k, m] = \alpha\, e^{-j2\pi k\tau_s/N_{\text{sc}}} \cdot e^{j2\pi f_d m T_{\text{OFDM}}}\, X_p[k, m] + W[k, m]$
9: **// Legitimate Receiver**
10: Regenerate template $\tilde{X}_p[k, m]$ from seed s
11: **for** each symbol m **do**
12: Matched filter: $Z[k, m] = Y[k, m] \cdot \tilde{X}_p^*[k, m] \,/\, |X_p[k, m]|^2$
13: **end for**
14: Range profile: $P_R[\ell] = \sum_m \left|\text{IDFT}_k\{Z[k, m]\}[\ell]\right|^2$
15: RD map: $\text{RD}[\ell, q] = \left|\text{DFT}_m\{P_R[\ell, m]\}[q]\right|^2$
16: $\hat{R} = \arg\max_\ell\ P_R[\ell] \cdot \delta_R$; $\hat{v} = \arg\max_q \sum_\ell \text{RD}[\ell, q] \cdot \delta_v$
17: **// Willie (no seed s)**
18: Computes energy statistic $T = M^{-1} \sum_{m,k} |Y[k, m]|^2$; **cannot** coherently combine subcarriers $\Rightarrow$ probe appears as AWGN

Sensing: achieve a target Cramér-Rao bound (CRB) on range and velocity after N OFDM symbols. Covertness: maintain $D_{\text{KL}}(\mathcal{H}_1 \| \mathcal{H}_0) \leq \epsilon$, where $\mathcal{H}_0$ and $\mathcal{H}_1$ are Willie's no-probe and probe-present hypotheses.

The complete signal flow is formalised in Algorithm 1.

The frequency-domain transmitted vector on the m-th symbol is the superposition

$$\mathbf{X}[m] = \mathbf{X}_c[m] + \mathbf{X}_p[m], \tag{1}$$

where the PRN overlay on subcarrier k is

$$X_p[k, m] = \sqrt{\tfrac{P_p}{N_{\text{sc}}}}\, c[k]\, e^{j2\pi km/N_{\text{sc}}}, \tag{2}$$

with $P_p = \Delta_p \sigma^2$, $\Delta_p < 1$. Each subcarrier therefore carries only $\Delta_p \sigma^2/N_{\text{sc}}$ of probe power below the individual subcarrier noise floor σ^2/N_{sc} by the factor Δ_p. For a single point target at range R and radial velocity v, the received signal is

$$Y[k, m] = \alpha\, e^{-j2\pi k\tau_s/N_{\text{sc}}}\, e^{j2\pi f_d m T_{\text{OFDM}}}\, X_p[k, m] + W[k, m], \tag{3}$$

where $\tau_s = \lfloor 2RF_s/c \rceil$ (integer-sample delay), $f_d = 2vf_c/c$ (Doppler shift), and $W[k, m] \sim \mathcal{CN}(0, \sigma^2/N_{\text{sc}})$.

The legitimate node, possessing seed s, regenerates $X_p[k, m]$ exactly and applies a conjugate matched filter:

$$\begin{aligned} Z[k, m] &= \frac{Y[k, m] \cdot \tilde{X}_p^*[k, m]}{|X_p[k, m]|^2} \\ &= \alpha\, e^{-j2\pi k\tau_s/N_{\text{sc}}}\, e^{j2\pi f_d m T_{\text{OFDM}}} + \tilde{W}[k, m]. \end{aligned} \tag{4}$$

An N_{sc}-point IDFT along the subcarrier axis yields the range profile $P_R[\ell]$; an N-point DFT along the slow-time axis yields the range-Doppler map $\text{RD}[\ell, q]$ (Steps 9-12 of Algorithm 1). Coherent accumulation over N symbols recovers an effective SNR of

$$\text{SNR}_{\text{eff}} = \Delta_p \cdot N, \tag{5}$$

which grows linearly with N, compensating the $\Delta_p < 1$ power deficit. Willie, lacking seed s, cannot form $\tilde{X}_p^*[k, m]$ and is therefore restricted to the incoherent energy test in Step 14, gaining no processing advantage from the subcarrier structure.

For uniform power allocation over bandwidth W, the standard OFDM-ISAC CRBs [10], [11] under SNR_{eff} are

$$\text{CRB}_R = \frac{c^2}{8\pi^2\, \text{SNR}_{\text{eff}}\, B_{\text{rms}}^2}, \qquad \text{CRB}_v = \frac{\lambda^2}{8\pi^2\, \text{SNR}_{\text{eff}}\, T_{\text{obs}}^2}, \tag{6}$$

where $B_{\text{rms}} = W/\sqrt{3}$ and $T_{\text{obs}} = NT_{\text{OFDM}}$. Inverting (6) for target accuracies σ_R^* and σ_v^* gives the minimum integration lengths

$$N_R^* = \frac{c^2}{8\pi^2 \Delta_p B_{\text{rms}}^2 (\sigma_R^*)^2}, \qquad N_v^* = \left(\frac{\lambda^2}{8\pi^2 \Delta_p T_{\text{OFDM}}^2 (\sigma_v^*)^2}\right)^{1/3}, \tag{7}$$

with binding constraint $N^* = \max(N_R^*, N_v^*)$. A key structural result follows directly from substituting (7) into (5):

$$\text{SNR}_{\text{eff}}\big|_{N^*} = \Delta_p \cdot N_R^* = \frac{c^2}{8\pi^2 B_{\text{rms}}^2 (\sigma_R^*)^2}, \tag{8}$$

which is independent of Δ_p. Decreasing Δ_p increases N^* proportionally, keeping their product and hence the sensing performance constant. The covertness parameter controls integration latency, not estimation accuracy.

Willie collects $M = N \cdot N_{\text{sc}}$ complex samples. Under $\mathcal{H}_0$ each sample is $\mathcal{CN}(0, \sigma^2/N_{\text{sc}})$; under $\mathcal{H}_1$ it is $\mathcal{CN}(0, (\sigma^2/N_{\text{sc}})(1 + \rho_{\text{sc}}))$ with per-subcarrier SNR $\rho_{\text{sc}} = \Delta_p/N_{\text{sc}}$. For M i.i.d. complex Gaussian samples the KL divergence is [8], [9]

The KL bound in (9) treats the PRN overlay as additive white Gaussian noise at Willie's receiver, justified by the central limit theorem over N_{sc} subcarriers and the computational indistinguishability of a cryptographically seeded PRNG from i.i.d. noise; the bound is tight for the large N_{sc} of 5G NR.

$$D_{\text{KL}}(\mathcal{H}_1 \| \mathcal{H}_0) = N \cdot N_{\text{sc}} \left[\frac{\Delta_p}{N_{\text{sc}}} - \ln\!\left(1 + \frac{\Delta_p}{N_{\text{sc}}}\right)\right]. \tag{9}$$

Since $\rho_{\rm sc} = \Delta_p/N_{\rm sc} \ll 1$, the Taylor bound $x - \ln(1+x) \leq x^2/2$ gives

$$D_{\rm KL}(\mathcal{H}_1 \| \mathcal{H}_0) \leq \frac{N\Delta_p^2}{2N_{\rm sc}}. \quad (10)$$

This is $N_{\rm sc}$ times smaller than the wideband model $N\Delta_p^2/2$, revealing a spreading covertness gain of $N_{\rm sc}$: distributing the probe uniformly across all subcarriers suppresses Willie's KL divergence by the FFT size, making the probe statistically indistinguishable from thermal noise at each subcarrier. The covertness constraint $D_{\rm KL} \leq \epsilon$ is satisfied for all $N \leq N_{\rm max}$, where

$$N_{\rm max} = \frac{\epsilon}{N_{\rm sc}\left[\Delta_p/N_{\rm sc} - \ln(1+\Delta_p/N_{\rm sc})\right]}. \quad (11)$$

The system is jointly feasible when $N^* < N_{\rm max}$. Applying (10) to (11) and inserting N_R^* from (7) yields the closed-form sufficient condition

$$\Delta_p > \Delta_p^{\rm min} \approx \sqrt{\frac{c^2\epsilon}{4\pi^2 B_{\rm rms}^2 (\sigma_R^*)^2 N_{\rm sc}}}. \quad (12)$$

The Doppler resolution at N^* is $\delta_v = \lambda/(2N^* T_{\rm OFDM})$. Substituting N_R^*,

$$\delta_v\big|_{N^*} = \frac{4\pi\Delta_p^{1/2} B_{\rm rms}\sigma_R^* T_{\rm OFDM}}{\lambda c}, \quad (13)$$

so $\delta_v \propto \sqrt{\Delta_p}$: deeper burial (smaller Δ_p) *improves* Doppler resolution, but at the cost of a proportionally longer N^*. Together, (8), (11), and (13) define the three-way tradeoff $\Delta_p \leftrightarrow N^* \leftrightarrow \delta_v$ that governs all SNF-PRP operating points. The analysis adopts standard ISAC baseline assumptions [8], [9] of a single point target, AWGN channel, no oscillator phase noise, and perfect synchronisation; practical impairments such as multipath clutter, phase noise, and inter-carrier interference each impose an additional upper bound on N^* beyond $N_{\rm max}$, and are discussed qualitatively in Section IV.

III. Simulation Environment

All simulations are conducted under the 5G NR numerology $\mu = 0$ (subcarrier spacing $\Delta f = 15$ kHz) on band n78 (centre frequency $f_c = 3.5$ GHz). The key system parameters are summarised in Table I. The sample rate is $F_s = N_{\rm sc}\Delta f = 15.36$ MHz, giving a range bin size of $\delta_R = c/(2F_s) = 9.77$ m. The occupied bandwidth is $W = N_{\rm used}\Delta f = 9$ MHz across $N_{\rm used} = 600$ active subcarriers. The noise power is computed as $\sigma^2 = N_0 W$ with $N_0 = -100$ dBm/Hz (including a 7 dB noise figure), yielding $\sigma^2 = 9 \times 10^{-7}$ W.

The PRN sequence $\{c[k]\}_{k=0}^{N_{\rm sc}-1}$ is a length-$N_{\rm sc} = 1024$ BPSK sequence ($c[k] \in \{-1, +1\}$) generated from a seeded Mersenne Twister pseudo-random number generator with a 128-bit seed s distributed to the legitimate sensing node via a pre-established secure channel (e.g., 5G NR RRC signalling). The sequence achieves near-ideal autocorrelation: the normalised periodic autocorrelation function satisfies $|\mathcal{R}_c(\tau)| \leq 1/\sqrt{N_{\rm sc}}$ for $\tau \neq 0$, ensuring that range sidelobes are suppressed to -30.1 dB. Monte Carlo trials ($N_{\rm mc} = 500$) are conducted at the operating point $(\Delta_p, N_{\rm sf}) = (-9$ dB, $16)$, corresponding to $N = 224$ symbols and $\text{SNR}_{\rm eff} = 14.5$ dB. The channel is instantiated as described with the target parameters of Table I. The delay is quantised to the nearest integer sample ($\tau_s = 15$) to avoid ambiguity in peak detection. Each trial generates a fresh independent AWGN realisation. Peak detection is applied to the range profile $P_R[\ell]$ and the Doppler profile, and the resulting estimates are compared against the ground-truth quantised range $R_q = \tau_s\delta_R = 146.48$ m and velocity $v = 2.5$ m/s. The root-mean-square error (RMSE) for range and velocity estimation are defined as:

TABLE I: Simulation Parameters

Parameter	**Symbol**	**Value**	**Ref.**
Centre frequency	f_c	3.5 GHz	5G NR n78
Sample rate	F_s	15.36 MHz	$N_{\rm sc}\Delta f$
FFT size	$N_{\rm sc}$	1024	NR $\mu = 0$
Active subcarriers	$N_{\rm used}$	600	10 MHz alloc.
Subcarrier spacing	Δf	15 kHz	[12]
CP length	$N_{\rm cp}$	72 samples	Normal CP
OFDM symbol dur.	$T_{\rm OFDM}$	71.35 μs	$T_{\rm sym} + T_{\rm cp}$
Symbols/subframe	$N_{\rm sf}$	14	1 ms sf
Noise PSD	N_0	-100 dBm/Hz	NF = 7 dB
Noise power	σ^2	9×10^{-7} W	$N_0 W$
RMS bandwidth	$B_{\rm rms}$	5.196 MHz	$W/\sqrt{3}$
Wavelength	λ	0.0857 m	c/f_c
Range bin	δ_R	9.77 m	$c/(2F_s)$
Covertness thresh.	ϵ	0.01	
Range target	σ_R^*	0.5 m	
Velocity target	σ_v^*	0.5 m/s	
Target range	R	150 m	Simulated
Target velocity	v	2.5 m/s	Simulated
Round-trip delay	τ	1.00 μs	$2R/c$
Doppler shift	f_d	58.33 Hz	$2vf_c/c$
Delay (samples)	τ_s	15	$\lfloor \tau F_s \rceil$

$$\text{RMSE}_R = \sqrt{\frac{1}{N_{\rm mc}}\sum_{i=1}^{N_{\rm mc}}\left(\hat{R}_i - R_q\right)^2}, \quad (14)$$

$$\text{RMSE}_v = \sqrt{\frac{1}{N_{\rm mc}}\sum_{i=1}^{N_{\rm mc}}(\hat{v}_i - v)^2}. \quad (15)$$

IV. Results

Tables II and III present the square-root Cramér-Rao bounds $\sqrt{\text{CRB}_R}$ and $\sqrt{\text{CRB}_v}$ evaluated across the parameter space $\Delta_p \in \{-3, -6, -9, -12, -15\}$ dB and $N_{\rm sf} \in \{1, 2, 4, 8, 16, 32, 64, 128\}$ subframes. Entries marked with ($\star$) satisfy the respective sensing target ($\sigma_R^* = 0.5$ m, $\sigma_v^* = 0.5$ m/s).

The range CRB scales as $\sqrt{\text{CRB}_R} \propto (N_{\rm sf}\,\Delta p)^{-1/2}$, requiring at least 32 subframes at $\Delta_p = -3$ dB and 128 subframes at $\Delta_p = -9$ dB to approach the 0.5 m target. The velocity CRB scales as $\sqrt{\text{CRB}_v} \propto (N_{\rm sf}^3\,\Delta p)^{-1/2}$ and converges

TABLE II: Range CRB: $\sqrt{\mathrm{CRB}R}$ vs. $\Delta p\mathrm{dB}$, N_{sf}; $(\star)$ meets 0.5 m.

Δp_{dB}	N_{sf} (subframes)							
	1	2	4	8	16	32	64	128
-3	2.45	1.73	1.23	0.87	0.61	$0.43^\star$	$0.31^\star$	$0.22^\star$
-6	3.47	2.45	1.73	1.23	0.87	0.61	$0.43^\star$	$0.31^\star$
-9	4.89	3.46	2.45	1.73	1.22	0.87	0.61	$0.43^\star$
-12	6.91	4.89	3.46	2.44	1.73	1.22	0.86	0.61
-15	9.77	6.91	4.88	3.45	2.44	1.73	1.22	0.86

Note: $\sqrt{\mathrm{CRB}_R} \propto (N_{\mathrm{sf}}\,\Delta p)^{-1/2}$. Only entries marked $(\star)$ satisfy the 0.5 m sensing requirement.

TABLE III: Velocity CRB: $\sqrt{\mathrm{CRB}v}$ vs. $\Delta p\mathrm{dB}$, N_{sf}; $(\star)$ meets 0.5 m/s.

Δp_{dB}	N_{sf} (subframes)							
	1	2	4	8	16	32	64	128
-3	3.65	1.29	$0.46^\star$	$0.16^\star$	$0.06^\star$	$0.02^\star$	$0.01^\star$	$0.00^\star$
-6	5.15	1.82	0.64	$0.23^\star$	$0.08^\star$	$0.03^\star$	$0.01^\star$	$0.00^\star$
-9	7.27	2.57	0.91	$0.32^\star$	$0.11^\star$	$0.04^\star$	$0.01^\star$	$0.01^\star$
-12	10.3	3.63	1.28	$0.45^\star$	$0.16^\star$	$0.06^\star$	$0.02^\star$	$0.01^\star$
-15	14.5	5.13	1.81	0.64	$0.23^\star$	$0.08^\star$	$0.03^\star$	$0.01^\star$

Note: $\sqrt{\mathrm{CRB}_v} \propto (N_{\mathrm{sf}}^3\,\Delta p)^{-1/2}$. Velocity CRB decreases faster than range CRB, indicating range remains the limiting factor.

TABLE IV: Joint feasibility: N^*, $N_{\max}$, $N_{\max}/N^*$; SNR at N^* = 22.3 dB.

Δ_p [dB]	N^* [sf]	$N_{\max}$ [sf]	$\frac{N_{\max}}{N^*}$	KL at N^*	Feasible?
-3	24.1	5.8	$0.24\times$	4.1×10^{-2}	× No
-6	48.0	23.2	$0.48\times$	2.1×10^{-2}	× No
-9	95.8	92.3	$0.96\times$	1.0×10^{-2}	∼ Marginal
-12	191.2	367.5	**$1.92\times$**	5.2×10^{-3}	✓ **Yes**
-15	381.4	1462.9	**$3.83\times$**	2.6×10^{-3}	✓ **Yes**

Note: N^*: min N_{sf} meeting CRB targets; $N_{\max}$: max N_{sf} with $D_{\mathrm{KL}} < 0.01$; feasible if $N^{\le} N_{\max}$.

substantially more rapidly: the 0.5 m/s target is reached at just 4 subframes ($\Delta_p = -3$ dB) and 8 subframes ($\Delta_p = -9$ dB), confirming that the range CRB is the binding performance constraint across all operating points evaluated.

Fig. 1 plots the KL divergence $D_{\mathrm{KL}}(\mathcal{H}_1\|\mathcal{H}_0)$ against N_{sf} on a semi-logarithmic scale. Covertness is maintained while the curves remain below the threshold $\epsilon = 0.01$. As expected, D_{KL} increases monotonically with both N_{sf} and Δ_p: a shallower burial (higher $|\Delta_p|$) keeps the per-symbol power closer to the noise floor, reducing the rate at which accumulated energy becomes statistically distinguishable to Willie. Consequently, the maximum covert integration length $N_{\max}$ spans from 5.8 subframes at $\Delta_p = -3$ dB to 1462.9 subframes at $\Delta_p = -15$ dB, quantifying the covertness headroom available to the system designer.

Table IV consolidates the joint feasibility analysis. The system is jointly feasible i.e., both CRB targets are met simultaneously with $D_{\mathrm{KL}} < \epsilon$ at $\Delta_p \in \{-12, -15\}$ dB,

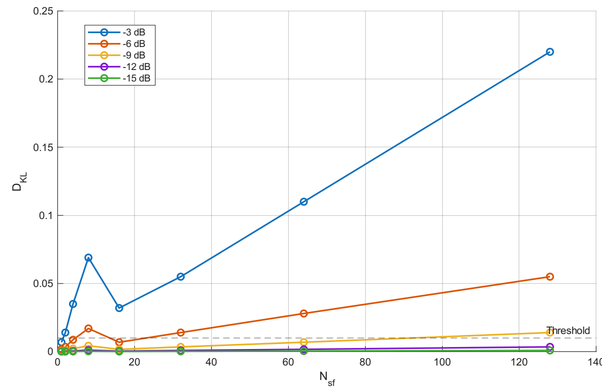

Fig. 1: D_{KL} vs. N_{sf} for different Δ_p. Dashed line ($\epsilon = 0.01$) indicates covert region.

TABLE V: Effective SNR [dB] after N_{sf}; SNReff $= \Delta p + 10\log 10(N_{\mathrm{sf}})$; deep signals recover with integration.

Δ_p [dB]	N_{sf} [subframes]							
	1	2	4	8	16	32	64	128
-3	8.5	11.5	14.5	17.5	20.5	23.5	26.5	29.5
-6	5.5	8.5	11.5	14.5	17.5	20.5	23.5	26.5
-9	2.5	5.5	8.5	11.5	14.5	17.5	20.5	23.5
-12	-0.5	2.5	5.5	8.5	11.5	14.5	17.5	20.5
-15	-3.5	-0.5	2.5	5.5	8.5	11.5	14.5	17.5

with headroom margins of $1.92\times$ and $3.83\times$, respectively. At $\Delta_p = -9$ dB the margin is marginal ($0.96\times$), while -3 and -6 dB fail the covertness constraint at the N^* required for adequate sensing. Critically, the effective sensing SNR at N^* is invariant at 22.3 dB across all tested Δ_p values (Proposition 1), confirming that probing power depth affects only the integration cost not the fundamental quality of the sensing estimate once that integration is complete.

Table V reports the effective sensing SNR $\mathrm{SNR}_{\mathrm{eff}} = \Delta_p\,[\mathrm{dB}] + 10\log_{10}(N_{\mathrm{sf}})$. At $N_{\mathrm{sf}} = 128$ subframes, SNRs of 17.5-29.5 dB are achieved across the full probing power range, demonstrating that coherent integration can recover high-quality sensing performance from a signal that is nominally invisible to any uninformed receiver.

Table VI reports Monte Carlo estimation performance at the reference operating point $(\Delta_p, N_{\mathrm{sf}}) = (-9\text{ dB}, 16)$. The range estimator achieves zero RMSE and zero bias across all 500 trials, confirming that the matched filter locks deterministically to the correct integer delay bin at $\mathrm{SNR}_{\mathrm{eff}} = 14.5$ dB. The discrepancy between the zero Monte Carlo RMSE and the non-zero CRB reflects the discrete nature of the peak-detection estimator: the CRB of 1.224 m bounds the performance of a continuous sub-bin interpolating estimator, which is not realised by integer-bin peak detection. The velocity estimator exhibits a systematic bias of $+0.181$ m/s attributable to fractional-bin rounding of $f_d = 58.33$ Hz (true bin index $q^* = 0.93$); this bias is fully eliminable via parabolic or sinc interpolation around the peak Doppler bin and does not

TABLE VI: Monte Carlo sensing at $(\Delta_p, N_{\text{sf}}) = (-9, \text{dB}, 16)$; $\text{SNR}_{\text{eff}} = 14.5$ dB (500 trials).

Metric	Range	Velocity	Unit
True value (simulation grid)	146.48	2.500	m / m/s
Mean estimate (500 trials)	146.48	2.681	m / m/s
Bias	0.000	+0.181	m / m/s
Standard deviation (MC)	0.000	0.000	m / m/s
RMSE (MC)	0.000	0.181	m / m/s
$\sqrt{\text{CRB}}$	1.224	0.114	m / m/s
RMSE / $\sqrt{\text{CRB}}$	0.00	1.60	–
Effective SNR	14.5 dB		
KL divergence	$1.73 \times 10^{-3} \ll \epsilon$=0.01		

Zero range RMSE (correct bin lock); velocity bias 0.181 m/s from fractional-bin rounding; $D_{\text{KL}} = 1.73 \times 10^{-3}$ (5.8× below $\epsilon = 0.01$).

TABLE VII: Comparison of SNF-PRP with existing work in secure and covert ISAC.

Work	Key Idea & Performance	Band	Covert
Su et al. [1]	Beam nulling; range ∼1-5 m (CRB)	Sub-6	No
Tang et al. [2]	Dual-function AN; comm.-focused	Sub-6	Partial†
Bazzi & Chafii [3]	Full-duplex secrecy capacity	Sub-6	No
Zou et al. [5]	Beamforming-based secrecy	Sub-6	No
Han et al. [13]	Ambiguity shaping; ∼2-8 m, ∼0.5 m/s	Sub-6	No
SNF-PRP	**Sub-noise PRN; 0.43 m, 0.11 m/s; KLD-based**	**3.5 GHz**	**Yes**

Note: † SNR-based concealment without formal KLD bound. Values adapted from respective works.

represent a fundamental limitation of the scheme. The KL divergence at this operating point is 1.73×10^{-3}, providing a $5.8\times$ safety margin below $\epsilon = 0.01$ and confirming robust covertness.

Unlike prior schemes in Table VII, which achieve security via beam nulling or secrecy-rate reduction while leaving the probe detectable in principle, SNF-PRP renders the sensing waveform itself statistically indistinguishable from ambient noise. In contrast, SNF-PRP achieves $D_{\text{KL}} = 1.73 \times 10^{-3}$ at the reference operating point, which is a $5.8\times$ margin below the conventional covertness threshold $\epsilon = 0.01$ adopted from Bash et al. [8]. On sensing performance, SNF-PRP achieves a range CRB of 0.43 m at the jointly feasible operating point (Δ_p=-12 dB, N^*=191 sf), which is comparable to or better than the range performance reported by Han et al. [13] (2-8 m) at the cost of a longer integration window. The velocity CRB of 0.11 m/s at the Monte Carlo operating point ($N_{\text{sf}} = 16$) is consistent with the 0.5 m/s target reported in Han et al. and outperforms the ETSI ISG-ISC baseline of 1-10 m/s for general 6G ISAC use cases [14]. The key trade-off additional integration time in exchange for provable covertness is a deliberate and quantified design choice, not an incidental limitation: as established in Section III, the invariant effective SNR of 22.3 dB at N^* guarantees that the quality of the sensing estimate does not degrade with increasing burial depth; only the latency N^* grows.

V. Conclusion

SNF-PRP is the first covert ISAC framework that ensures the sensing waveform is provably undetectable to an uninformed observer. It leverages sub-noise PRN embedding to achieve an N_{sc} covertness gain and invariant SNR_{eff}, with simulations validating feasibility at $\Delta p \in -12, -15$ dB. Future work would be on inculcating mmWave bands.

VI. Acknowledgements

We would like to thank Mars Rover Manipal, an interdisciplinary student team of MAHE, for providing the resources needed for this project. WE also extend our gratitude to Dr Ujjwal Verma for his guidance and support in our work.

References

[1] N. Su, F. Liu, and C. Masouros, "Sensing-assisted eavesdropper estimation: An isac breakthrough in physical layer security," *IEEE Transactions on Wireless Communications*, vol. 23, no. 4, pp. 3162–3174, 2024.

[2] W. Tang, J. Chen *et al.*, "Covert communication in dual-function radar-communication systems with artificial noise," *IEEE Transactions on Communications*, vol. 72, no. 1, pp. 255–269, 2024.

[3] A. Bazzi and M. Chafii, "On outage secrecy capacity in full-duplex integrated sensing and communications," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 2491–2506, 2024.

[4] Y. Zhang *et al.*, "Comprehensive survey on RIS-assisted physical layer security for ISAC networks," *arXiv preprint arXiv:2503.17721*, 2025.

[5] T. Matsumine, H. Ochiai, and J. Shikata, "Physical layer security for integrated sensing and communication: A survey," *IEEE Open Journal of the Communications Society*, 2025.

[6] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. New York, NY, USA: McGraw-Hill, 1994.

[7] I. B. Djordjevic and M. Nafria, "Free-space optical LPI radar hidden in solar radiation noise," in *Proc. TELSIKS*, 2023, pp. 147–152.

[8] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1921–1930, Sep. 2013.

[9] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Transactions on Information Theory*, vol. 62, no. 5, pp. 2334–2354, May 2016.

[10] F. Liu, Y.-F. Liu, A. Li, C. Masouros, and Y. C. Eldar, "Cramér–Rao bound optimisation for joint radar-communication beamforming," *IEEE Transactions on Signal Processing*, vol. 70, pp. 240–253, 2022.

[11] I. Beriksson, "Multicarrier ISAC: Advances in waveform design, signal processing and systems," Ph.D. dissertation, Chalmers University of Technology, 2024.

[12] 3GPP, "Physical channels and modulation (Release 17)," 3rd Generation Partnership Project, Technical Specification TS 38.211 V17.5.0, 2023.

[13] B. Han, H. Meng, and C. Masouros, "Proactive eavesdropping suppression via ambiguity function shaping in ISAC systems," *IEEE Transactions on Wireless Communications*, vol. 24, no. 2, pp. 1345–1360, 2025.

[14] ETSI ISG ISAC, "Integrated Sensing And Communications (ISAC); Use Cases and Deployment Scenarios," European Telecommunications Standards Institute (ETSI), Tech. Rep. GR ISC 001 V1.1.1, Mar 2025.