
gr-ntnisac: An Open GNU Radio Testbed for NTN-ISAC

Soham Dhiren Desai

Skylo Technologies, California, USA

SOHAM.D.DESAI@GMAIL.COM

Abstract

A passive receiver can sense nearby objects from the echoes of a 5G downlink. When the transmitter is a low-Earth-orbit (LEO) satellite, one transmitter covers a wide area, but the receiver must handle tens of kHz of Doppler and a direct-path delay that changes within every observation interval. Such a receiver should be tested where the correct answer is known before it is tried on a satellite. This paper presents *gr-ntnisac*, an open GNU Radio testbed that applies an emulated LEO channel to a standard 5G New Radio downlink, sends it through two cabled USRPs, and scores the receiver against the delay and Doppler commanded for every path. The same receiver code runs in simulation, on recorded captures, and on hardware. As a first use, we measure cancellation of the direct path, the strong satellite signal that masks weak echoes. Depth is 34.8 dB on hardware and 37.6 dB in a matched simulation without radios, so the radios are not the main limit. Controlled simulation shows that the emulator's 8-tap fractional-delay filter and a simulated rotating blade at almost the direct path's delay each limit depth to about 40 dB; without either, depth reaches 71.0 dB. A diagnostic canceller that also removes the per-subcarrier response and per-symbol phase reaches 72.7 dB on the same captures. On a conducted capture, a payload-aided receiver detects a -25 dB moving path in 76.9% of dwells.

1. Introduction

A 5G base station transmits a wideband downlink of known reference signals and payload data. Objects near a receiver reflect part of it, so a receiver that detects the echoes can sense its surroundings without any change to the transmitter: a form of integrated sensing and communications (ISAC) [1]. 3GPP has written service requirements for 5G

sensing [2], and the Next G Alliance treats ISAC as a foundational capability of 6G [3].

In a non-terrestrial network (NTN), the transmitter is on a LEO satellite that illuminates a very large area [4, 5]. The receiver must handle tens of kHz of Doppler, hundreds of Hz/s of Doppler rate, and a direct-path delay that changes within every observation interval [5]. Simulation tests the algorithms but omits converter filters, oscillator phase noise, and clock offsets. A satellite trial includes them, but gives no repeatable path-level truth and no matched target-absent control. Between the two, a lab setup is needed that runs the receiver on real radios while the delay and Doppler of every path are known.

Terrestrial 5G passive radar has been demonstrated with the synchronization signal block (SSB) alone [6], with the full downlink [7], and on deployed networks [8], and an open real-time OFDM-ISAC platform exists for terrestrial links [9]. For LEO illuminators, the published work known to us is analytical or simulated; we are not aware of an open hardware-in-the-loop testbed.

gr-ntnisac provides one. It applies the LEO channel to a standard 5G New Radio (NR) downlink in software, trans-

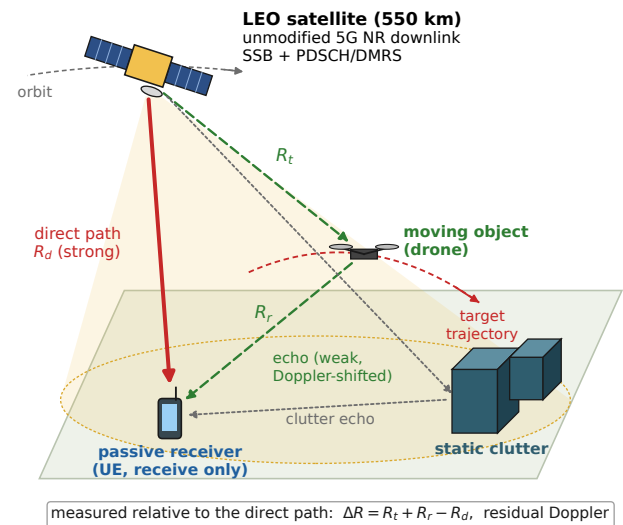


Figure 1. NTN-ISAC scenario emulated by *gr-ntnisac*.

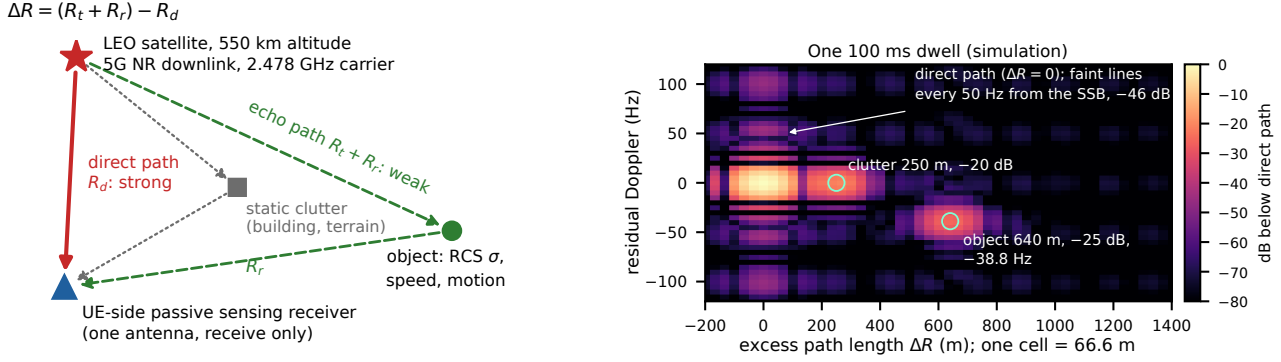


Figure 2. Bistatic geometry (left) and the delay–Doppler map of one simulated dwell (right).

mits the result through real radios, and compares the receiver’s output with the path trajectories written in a scene file. Real converters, oscillators, and host streaming are in the loop, and every path’s commanded delay and Doppler remain known on the sample clock. The same receiver code runs in simulation, on recorded captures, and on hardware, so a result that changes between steps points to the effect that step adds. GNU Radio suits this because stream processing, message passing, hardware access, and replay share one flowgraph [10].

Figure 1 shows the scenario. The receiver gets a strong *direct path* and much weaker *echoes* from moving objects and static clutter. It measures each echo relative to the direct path: its *excess path length* $\Delta R = (R_t + R_r) - R_d$ from the extra delay, and its *residual Doppler* from the rate at which ΔR changes. Each delay–Doppler map is computed from one observation interval, a *dwell*, here 100 ms. Figure 2 shows a bench simulation with a static scatterer at 250 m and a -25 dB drone whose excess path grows at 4.7 m/s; both appear where commanded, the drone at 640 m and -38.8 Hz.

The contributions are:

- *LEO channel*: a real-time C++ channel in which range is the only kinematic input, so Doppler, Doppler rate, and delay walk stay consistent; a truth block on the sample clock; and per-symbol retiming that removes the direct path’s delay walk (§3.1, §4.2).
- *Sensing scenes*: 3GPP models terrestrial sensing channels (TR 38.901, Clause 7.9) and NTN propagation (TR 38.811) separately [11, 12]; a scene file places sensing objects and 3GPP multipath under an analytic or SGP4 orbit with commanded truth (§3.3).
- *Payload-aided references*: known references are a small part of the downlink [7, 13]; the receiver com-

pares reference-only, payload-aided, and genie references on the same dwell (§4.3, §6.2).

- *Hardware in the loop*: two radios add frequency, timing, and sample-clock offsets [9]; every capture is recorded for replay and compared with matched and controlled simulations (§5, §6).

The channel and objects are emulated and the radios are cabled, so the testbed does not test real satellite reception or distant targets; it tests the receiver on real hardware against known truth. Installation and operating instructions are provided with the public code [14].

2. Architecture

Figure 3 shows the system. Three design decisions shape it.

The waveform is generated offline. The released waveform is one 20 ms NR frame (20 slots, 153,600 samples) written with the MATLAB 5G Toolbox [15] following TS 38.211 [16], with the reference values and occupancy masks the receiver needs. The transmitter repeats this frame. Slot 0 carries the SSB and no data; slots 1–19 carry QPSK data on all 25 resource blocks. Because the occupancy changes once per frame, every strong path has weak Doppler side-lobes at multiples of 50 Hz (about 46 dB below the direct path in Figure 2). A live downlink with a 20 ms SSB period has the same frame-rate structure. The repeated payload is a simplification that the payload-aided receiver does not exploit: it re-creates the data in every dwell from its own decisions. The receiver contains no NR sequence generation, so another standards-compliant source or recorded IQ can replace the generator.

The satellite channel is applied digitally on the transmit side, before the digital-to-analog converter (DAC). The radios then add their converters, filters, and clocks without

Table 1. Blocks of gr-ntnisac

Block	Function
leo_channel (C++)	Applies each path’s range history and gain
leo_truth	Each scored path’s commanded excess range and Doppler, time-stamped on the sample clock
esn0_noise	Noise referenced to energy per occupied RE
ssb_coarse	Stage 1: SSB matched filter, delay gate, Kalman track
grid_sense	Stage 2: full-grid delay–Doppler map, CLEAN, CFAR, clustering
ota_sense	Acquisition, clock tracking, direct-path CLEAN, micro-Doppler
link_budget	Echo-to-direct ratio for a cross section and range
msg_print	Text sink for any message port

changing the commanded trajectories used for scoring.

Displays are separate processes. Detections and truth leave the flowgraph over ZeroMQ, so a dashboard failure cannot stop a capture.

Table 1 lists the blocks. Every Python block is a thin wrapper around the `py/ntn_isac` library, which the offline tests call directly, so tests and flowgraphs use the same receiver functions. The `ota` prefix is historical: those blocks were first written for two free-running radios.

3. Channel and Scenes

3.1. Range Is the Only Input

Each path p is described only by its range $R_p(t)$ and gain over time, read from a trajectory table. The channel computes

$$y(t) = \sum_p a_p(t) x(t - \tau_p(t)) e^{-j2\pi f_c \tau_p(t)}, \quad (1)$$

where x is the baseband waveform, y the output sent to the DAC, a_p the path amplitude, $\tau_p = R_p/c$ its delay, and f_c the carrier. As the range changes, the carrier phase rotates, which is the Doppler shift; Doppler is not a parameter anywhere in the code. A channel with separate delay and Doppler inputs could describe an object whose range and Doppler disagree, and a frequency-shift-only model omits the *delay walk*, the change of delay during a dwell. For the pass in Table 2, the direct path’s delay changes by up to $2.2 \mu\text{s}$ (17 samples at 7.68 MS/s) within one 100 ms dwell. One delay bin of the 5 MHz waveform (4.5 MHz occupied) is 222 ns, or 66.6 m of path, so the direct path migrates across about 10 bins per dwell.

The direct path comes from an analytic circular orbit in Python or from MATLAB SGP4 propagation of a two-line

Table 2. Sample SGP4 Pass

Quantity	Value
Orbit / pass	550 km circular, 600 s, 67.5° peak elevation
Slant range	594 to 2170 km
Range rate / Doppler	$\pm 6.636 \text{ km/s}$ / $\pm 54.9 \text{ kHz}$
Doppler rate	up to 678 Hz/s
Delay walk, 7.68 MS/s	170 samples/s

element set (TLE); both write the same trajectory format. Table 2 is an SGP4 pass of a synthetic 550 km TLE over Mountain View, California.

3.2. Implementation

The C++ block evaluates Equation (1) for every sample, with the delay from a cubic spline through the trajectory and the carrier phase reduced modulo one cycle in double precision. An interpolation filter supplies each fractional-sample delay. Its frequency response is not flat and varies with fractional delay, which puts sidebands on the direct path; longer filters reduce them at a cost in throughput. The 5 MHz waveform is sampled at 7.68 MS/s (512-point FFT, 15 kHz subcarrier spacing). With the 8-tap windowed-sinc filter used on hardware, the block measured 20.4 MS/s on three paths, 2.66 times real time. This filter’s response reappears in the hardware results.

3.3. Scenes

A scene is a YAML file listing the orbit and every path (Figure 4); `tools/build_scene.py` compiles it into a trajectory. Path types are `direct`, `static`, `linear`, `rotating` (a point on a blade, for micro-Doppler), `pendulum`, `custom` (an expression in t), and `ntn_tdl`. Any path can be limited to a visibility window, giving target-absent epochs inside one capture, and any field can be overridden on the command line, so a sweep is a shell loop.

Object size. An echo’s gain is its power relative to the direct path. For a distant transmitter it is approximately $\sigma/(4\pi R_r^2)$ for radar cross section σ at distance R_r from the receiver, which `link_budget` computes. For example, -25 dB is 400 m^2 at 100 m, and -40 dB is 12.6 m^2 at 100 m or $1,260 \text{ m}^2$ at 1 km. Cross sections can come from electromagnetic simulation tools.

Geometry. Objects near the line of sight have little excess path: one meter off the middle of a five-meter baseline gives 0.39 m, under 1% of a delay bin. Such objects are separated by Doppler, which is why the bench scenes include a rotating target.

3GPP multipath. The scene imports the TR 38.811 tapped-

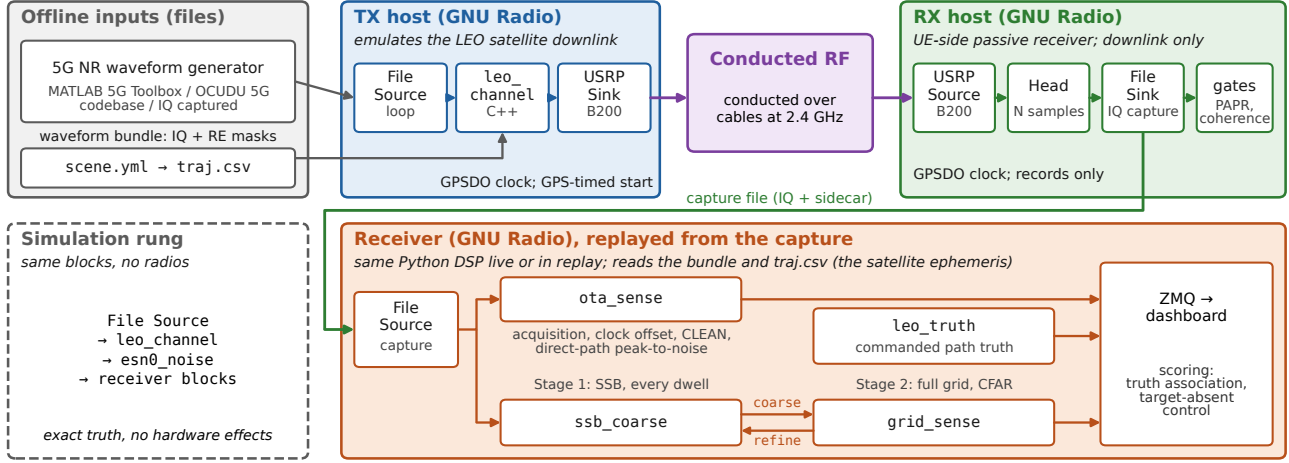


Figure 3. End-to-end testbed: emulated LEO channel, two cabled USRPs, and a replay receiver.

```

name: bench_both
carrier_hz: 2.478e9
orbit: {source: circular, alt_km: 550,
        max_elev_deg: 67.5} # or SGP4
paths:
- {type: direct}
- {type: static, excess_m: 250,
  gain_db: -20}
- {type: linear, excess_m: 640,
  excess_rate_mps: 4.7, t_ref_s: 500,
  gain_db: -25}
- {type: rotating, excess_m: 0.4,
  radius_m: 0.25, rot_hz: 7,
  gain_db: -30}
noise: {esn0_db: 45}

```

Figure 4. Scene file scenes/bench_both.yml, condensed.

delay-line profiles [11]. A tap with a time-varying complex gain would reintroduce a Doppler not constrained by range, so each cluster is built from sub-rays whose range ramps at the rate that gives their Doppler. With several sub-rays spread in angle, as in Jakes' model [17], the cluster fades by interference, with no new channel code. These clusters carry no truth and are switched off when sensing is scored.

4. Receiver

4.1. OFDM Sensing

Each OFDM symbol carries one complex value on each of 300 subcarriers spaced 15 kHz apart; one subcarrier in one symbol is a *resource element* (RE). Each symbol is preceded by a *cyclic prefix* (CP), a copy of its last portion. At 15 kHz with normal CP and 7.68 MS/s, most symbols have a 36-sample (4.69 μ s) CP, while symbols 0 and 7 of

each 14-symbol slot have 40 samples [16, Sec. 5.3.1]. An echo arriving within the CP after the direct path is a circularly shifted copy of the symbol, so after the FFT its delay is a linear phase across subcarriers and its Doppler a linear phase across symbols. Once the transmitted values are divided out, two FFTs give the delay-Doppler map [18]. Bins are 66.6 m by 10 Hz for a 100 ms dwell, the shortest CP bounds the excess path at 1405 m, and coherent use of all 374,650 occupied REs gives 55.7 dB of integration gain.

4.2. Retiming and De-Walk

The goal is to hold the direct path at zero delay and Doppler in every symbol. Its Doppler reaches ± 55 kHz, almost four subcarrier spacings, and its delay walks up to 17 samples (10 bins) per dwell; a window placed once per dwell would smear every path across those bins and use up half the CP. An NTN user equipment pre-compensates from the broadcast ephemeris [19, 20], and radar calls this range migration [21]. Here the trajectory file is the ephemeris. The receiver removes the direct path's carrier phase, which takes out its Doppler and Doppler rate; places each symbol's FFT window at that symbol's arrival sample, found by two fixed-point iterations because delay must be evaluated at arrival time; and removes the remaining fractional sample as a phase ramp after the FFT. Echoes walk only 0.5 m per dwell relative to the direct path at 5 m/s, so they need no further correction.

4.3. Sensing References

The receiver must know the transmitted values to divide them out [18, 22]. *Reference-only* uses the known reference signals, 8.1% of the occupied REs. *Payload-aided* also re-creates the data REs from its own channel estimate,

equalizer, and hard decisions. *Genie* uses the transmitted grid; it exists only in emulation and bounds the payload-aided result. All three share one code path, with untrusted REs masked and the map normalized by the number of REs used. Payload reconstruction is established in passive radar [23, 24] and is not claimed as new.

4.4. Cancellation and Detection

The direct path is at least 20 dB stronger than every modeled echo, so it is removed first. From the reference grid and occupancy mask, the receiver builds the ideal point-spread function of a hypothesized path, finds and refines the direct-path peak, fits its amplitude by least squares, and subtracts it: Högbom’s CLEAN [25, 26], using the actual NR symbol times and a bounded search so that a side-band or target is not removed first. Detection then applies an ephemeris-derived clutter mask, cell-averaging CFAR, density clustering [27], and rejection of the 50 Hz frame-rate sidelobes. The CFAR is set for about one noise-only candidate per dwell [28]; deterministic residue can violate this. The LEO-specific parts are per-symbol retiming with fractional de-walk, a CLEAN built from the exact occupancy and symbol times, and one trajectory file serving as both ephemeris and truth.

4.5. Two-Stage Processing

Following Khawaja et al. [29], a low-cost stage runs on every dwell and a full stage on demand. `ssb_coarse` matched-filters each SSB and publishes a delay gate; `grid_sense` runs the full-grid chain inside it. Messages carry sample-clock time stamps, so a late result is applied to the right dwell. GNU Radio runs each block in its own thread; in Python, Stage 1 takes 82 ms per 100 ms dwell and keeps pace, while Stage 2 takes about 480 ms and live runs at most once every five dwells. All results here are from replay, where Stage 2 runs on every dwell.

5. Method

Experiments climb three rungs with the waveform, scene, and receiver held fixed, so each step isolates the effects it adds. The *bench* rung runs the whole chain on one host. *Loopback* connects one radio’s ports through at least 40 dB of attenuation, checks sustained streaming, and measures the fixed hardware delay. The *conducted* rung uses two hosts, two USRP B200s, a splitter, and fixed attenuation (Figure 5); each radio has its own GPS-disciplined oscillator and the capture starts on a common GPS epoch. Gain keeps the direct path 15–20 dB below full scale. The carrier is 2.478 GHz, not an NTN allocation, and every hardware run is conducted over cable.

Capture, then replay. The Python sensing chain can run

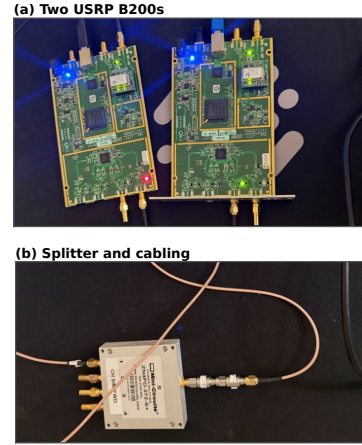


Figure 5. Conducted hardware setup.

slower than real time and back-pressure the USRP source, and dropped samples can corrupt delay and Doppler while level and spectrum look normal. The receive host therefore records with a minimal flowgraph and sensing runs on replay. Receive gain is fixed. Each capture must pass a peak-to-average gate, within 1.5 dB of the waveform’s own value, which catches a starved transmitter (ratio rises) or clipping (ratio falls), and a frame-to-frame coherence gate that detects a sample splice.

6. Hardware Results

6.1. Direct-Path Cancellation

The conducted captures used the full-allocation 5 MHz waveform. The direct-path peak-to-noise ratio was 82.49 ± 0.70 dB over 28 dwells ($\pm$ is one standard deviation), about 33 dB of E_s/N_0 per occupied RE after the 55.7 dB integration gain and 6.0 dB window loss. This high level isolates hardware effects; it does not test sensitivity at an NTN operating point, which is a natural next step on the same bench.

Cancellation depth is the ratio, in dB, of the largest map value within ± 1.5 delay bins and ± 15 Hz of the direct path before and after cancellation. With the `ota_sense` configuration (Blackman–Harris window, two CLEAN components), single-point depth was 38.71 ± 3.84 dB with one radio in loopback and 34.75 ± 4.46 dB with two. Figure 6 comes from an offline MATLAB replay of the same receiver, which reproduces these depths within 0.05 dB. A *matched simulation* repeats the two-host experiment without radios: same scene, waveform, and 8-tap filter, the measured clock offset of -1.28×10^{-9} between the two oscillators, and noise set to the captured peak-to-noise ratio. It reaches 37.6 ± 3.1 dB, between the two hardware values, so the radios are not the main cause.

Controlled simulation separates the causes (Figure 6a). With a 24-tap interpolator and the blade switched off, single-point CLEAN reaches 71.0 dB. Either the 8-tap filter (40.0 dB) or the blade alone (41.5 dB) limits depth to about 40 dB. The blade sits at 0.4 m of excess path, inside the direct path's delay bin, so part of the "residue" is a real echo; the filter's response, which varies with fractional delay, is the other part.

Two additions diagnose these on the captures. The first removes the direct path's phase in each symbol, the common phase error (CPE) that oscillator phase noise puts on every subcarrier. The second, after CLEAN, fits and subtracts on each subcarrier a term at the direct path's Doppler, approximating the combined response of the filter, radios, cables, and splitter as constant within a dwell. With both, the *response-aware canceller* reaches 72.7 ± 9.3 dB on two hosts, 70.7 ± 7.9 dB with one radio, and 70.7 ± 8.2 dB in the matched simulation. Its depth falls from about 80 to 60 dB over the 28 dwells (Figure 6b) on hardware and in the matched simulation, but not with the 24-tap filter, so the large spreads reflect a trend more than scatter. The captures start at closest approach, where the range rate is zero; by the last dwell it is 250 m/s, and the fractional delay moves 0.6 sample within a dwell, while the per-subcarrier term assumes a constant response. Because the common-phase step also removes slow-time modulation at the direct path's delay, the blade included, this canceller locates the residue; it is not a receiver for objects at that range, and since it fits and scores the same dwell, its depth is a diagnostic upper bound. In the same replay it cut false detections in a target-absent capture from 4.20 to 1.28 per dwell, close to the nominal one.

6.2. Payload-Aided Example

References alone use 8.1% of the occupied REs, giving up 10.9 dB of coherent energy, and the DMRS on every other subcarrier adds grating sidelobes in delay. Comparing references is one flag (`-variant reference-only`, `payload-aided`, or `genie`). On the bench rung with the SGP4 pass and $E_s/N_0 = 10$ dB, a moving -25 dB object stood 9.6 dB above its CFAR threshold with references only, 13.0 dB payload-aided, and 13.1 dB with the genie. The payload-aided map gains the full 10.9 dB in peak-to-noise ratio (26.5 to 37.4 dB), but the margin rises only 3.4 dB: the direct path is not cancelled in this example, so once noise is low the CFAR threshold is set by deterministic sidelobes. At 40 dB E_s/N_0 the margins saturate at 10.6 and 13.5 dB. Decision errors cost little: the uncoded symbol error rate is 0.4% at 10 dB.

On hardware, a 30 s conducted capture carried a ladder of four moving paths at -25 , -30 , -35 , and -40 dB and a static path at 1050 m. Replayed through the GNU Radio

blocks, the payload-aided receiver associated the -25 dB path in 230 of 299 dwells (76.9%) within one delay bin and 10 Hz, with errors of -4.2 ± 4.0 m and 0.9 ± 0.5 Hz. The weaker paths were not detected, the static path was suppressed as clutter, and a matched target-absent capture gave no association in 299 dwells. False detections remain high: 1,442 in the ladder capture (4.8 per dwell), 1,163 of them at multiples of 50 Hz, and 894 (3.0 per dwell) in the target-absent capture, 688 on the same comb. They come from direct-path residue and the frame structure, not from targets.

7. Future Work

The testbed models only a common reference error, in which carrier and sample clock move together; a transparent satellite payload adds a carrier offset with no matching delay drift. An impairment block for carrier offset, phase noise, and amplifier nonlinearity, and a clock tracker in `grid_sense`, come next. On the receiver side: the response-aware canceller in the live blocks, stronger rejection of the 50 Hz comb, and decoder-aided references; on the emulator side, a longer filter. Extending the channel over several synchronized USRPs would allow multistatic and multi-antenna receivers, and emulating several satellites with handover would let a receiver track an object across passes. A non-repeating payload or live gNB source, radiated tests, 20 MHz hardware runs, and a broader payload-aided evaluation are left to a continuation study.

8. Conclusion

gr-ntnisac lets an experimenter test an NTN sensing receiver in simulation and on real radios before a satellite trial, scored against commanded path truth with the same code throughout. One channel rule, range as the only kinematic input, covers moving and rotating targets, 3GPP multipath, and common reference error. On conducted hardware, cancellation reached 34.8 dB, close to the 37.6 dB of a matched simulation, and controlled simulation traced the limit to the emulator's 8-tap filter and an unresolved blade echo. A payload-aided receiver detected a -25 dB path in 76.9% of conducted dwells, while standing false detections from residue and the 50 Hz comb remain the main receiver limitation. This is the purpose of the tool: to make differences between simulation and hardware visible, repeatable, and attributable.

References

- [1] Fan Liu, Yuanhao Cui, Christos Masouros, Jie Xu, Tony Xiao Han, Yonina C. Eldar, and Stefano Buzzi. Integrated sensing and communications: Toward dual-functional wireless networks for 6G and beyond. *IEEE J.*

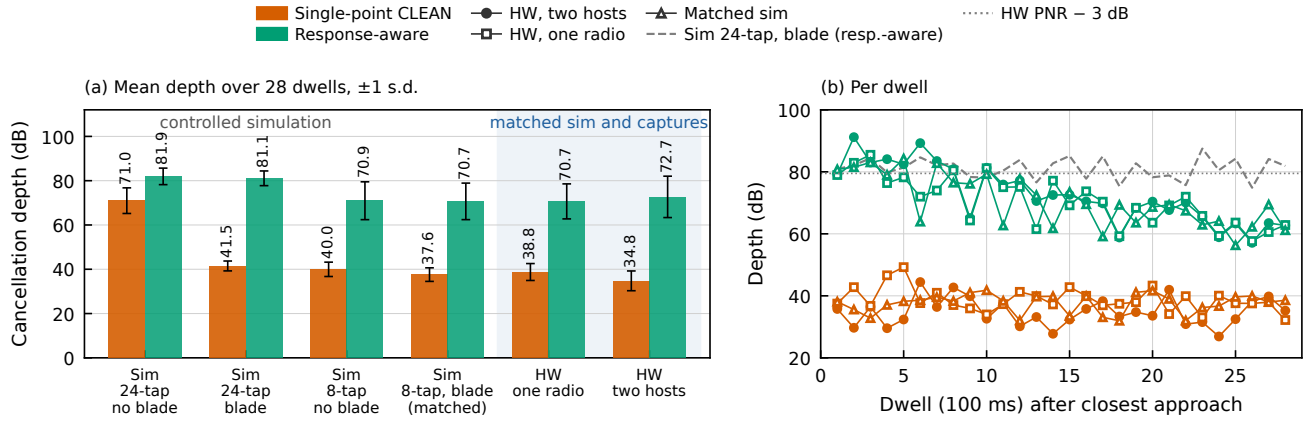


Figure 6. Direct-path cancellation depth: (a) by configuration, (b) per dwell. Response-aware: CPE (common phase error) correction, CLEAN, and a per-subcarrier term.

- Sel. Areas Commun.*, 40(6):1728–1767, 2022. doi: 10.1109/JSAC.2022.3156632.
- [2] 3GPP. Service requirements for integrated sensing and communication; stage 1. TS 22.137, 3GPP, 2024. V19.1.0.
- [3] Next G Alliance. Integrated sensing and communications readiness report, phase I. Report, ATIS, September 2025. https://nextgalliance.org/white_papers/integrated-sensing-and-communication-s-readiness-report-phase-i/.
- [4] Li You, Yongxiang Zhu, Xiaoyu Qiang, Christos G. Tsinos, Wenjin Wang, Xiqi Gao, and Björn Ottersten. Ubiquitous integrated sensing and communications for massive MIMO LEO satellite systems. *IEEE Internet Things Mag.*, 7(4): 30–35, 2024. doi: 10.1109/IOTM.001.2300201.
- [5] Rodrigo Blázquez-García, Diego Cristallini, Martin Ummenhofer, Viktor Seidel, Jörg Heckenbach, and Daniel O’Hagan. Capabilities and challenges of passive radar systems based on broadband low-earth orbit communication satellites. *IET Radar, Sonar & Navig.*, 18(1):78–92, 2024. doi: 10.1049/rsn2.12446.
- [6] Karol Abratkiewicz, Adam Księżyk, Marek Płotka, Piotr Samczyński, Jacek Wszolek, and Tomasz P. Zieliński. SSB-based signal processing for passive radar using a 5G network. *IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens.*, 16:3469–3484, 2023. doi: 10.1109/JSTARS.2023.3262291.
- [7] Marek Wypich and Tomasz P. Zieliński. Experimental evaluation of 5G NR OFDM-based passive radar exploiting reference, control, and user data. *Sensors*, 26(4), 2026. doi: 10.3390/s26041317. Art. no. 1317.
- [8] Piotr Samczyński, Karol Abratkiewicz, Marek Płotka, Tomasz P. Zieliński, Jacek Wszolek, Sławomir Hausman, Piotr Korbel, and Adam Księżyk. 5G network-based passive radar. *IEEE Trans. Geosci. Remote Sens.*, 60, 2022. doi: 10.1109/TGRS.2021.3137904. Art. no. 5108209.
- [9] Zhiwen Zhou, Chaoyue Zhang, Xiaoli Xu, and Yong Zeng. OpenISAC: An open-source real-time experimentation platform for OFDM-ISAC. *IEEE Internet Things J.*, 13(17): 41254–41269, 2026. doi: 10.1109/IJOT.2026.3710751.
- [10] Eric Blossom. GNU Radio: Tools for exploring the radio frequency spectrum. *Linux J.*, June 2004. No. 122.
- [11] 3GPP. Study on new radio (NR) to support non-terrestrial networks. TR 38.811, 3GPP, 2020. V15.4.0.
- [12] 3GPP. Study on channel model for frequencies from 0.5 to 100 GHz. TR 38.901, 3GPP, 2026. V19.4.0.
- [13] J. Andrew Zhang, Fan Liu, Christos Masouros, Robert W. Heath, Zhiyong Feng, Le Zheng, and Athina Petropulu. An overview of signal processing techniques for joint communication and radar sensing. *IEEE J. Sel. Topics Signal Process.*, 15(6):1295–1315, 2021. doi: 10.1109/JSTSP.2021.3113120.
- [14] Soham Dhiren Desai. NTN ISAC: Hardware-in-the-loop 5G NR sensing over an emulated LEO channel. https://github.com/soham12112/NTN_ISAC_GRCON26, 2026.
- [15] The MathWorks, Inc. 5G Toolbox. <https://www.mathworks.com/products/5g.html>, 2026. Accessed Oct. 2026.
- [16] 3GPP. NR; physical channels and modulation. TS 38.211, 3GPP, 2026. V19.3.0.
- [17] William C. Jakes, Jr., editor. *Microwave Mobile Communications*. Wiley, 1974.
- [18] Christian Sturm and Werner Wiesbeck. Waveform design and signal processing aspects for fusion of wireless communications and radar sensing. *Proc. IEEE*, 99(7):1236–1259, 2011. doi: 10.1109/JPROC.2011.2131110.
- [19] 3GPP. NR; radio resource control (RRC); protocol specification. TS 38.331, 3GPP, 2026. V19.4.0.

- [20] 3GPP. NR; NR and NG-RAN overall description; stage 2. TS 38.300, 3GPP, 2026. V19.4.0.
- [21] R. P. Perry, R. C. DiPietro, and R. L. Fante. SAR imaging of moving targets. *IEEE Trans. Aerosp. Electron. Syst.*, 35(1):188–200, 1999. doi: 10.1109/7.745691.
- [22] Christian R. Berger, Bruno Demissie, Jörg Heckenbach, Peter Willett, and Shengli Zhou. Signal processing for passive radar using OFDM waveforms. *IEEE J. Sel. Topics Signal Process.*, 4(1):226–238, 2010. doi: 10.1109/JSTSP.2009.2038977.
- [23] Dominique Poullin. Passive detection using digital broadcasters (DAB, DVB) with COFDM modulation. *IEE Proc. Radar, Sonar Navig.*, 152(3):143–152, 2005. doi: 10.1049/ip-rsn:20045017.
- [24] James E. Palmer, H. Andrew Harms, Stephen J. Searle, and Linda M. Davis. DVB-T passive radar signal processing. *IEEE Trans. Signal Process.*, 61(8):2116–2126, 2013. doi: 10.1109/TSP.2012.2236324.
- [25] J. A. Högbom. Aperture synthesis with a non-regular distribution of interferometer baselines. *Astron. Astrophys. Suppl. Ser.*, 15:417–426, 1974.
- [26] Krzysztof Kulpa. The CLEAN type algorithms for radar signal processing. In *Proc. Microw., Radar Remote Sens. Symp. (MRRS)*, pages 152–157, 2008. doi: 10.1109/MRRS.2008.4669567.
- [27] Martin Ester, Hans-Peter Kriegel, Jörg Sander, and Xiaowei Xu. A density-based algorithm for discovering clusters in large spatial databases with noise. In *Proc. 2nd Int. Conf. Knowl. Discovery Data Mining (KDD)*, pages 226–231, 1996.
- [28] Mark A. Richards. *Fundamentals of Radar Signal Processing*. McGraw-Hill, 2nd edition, 2014.
- [29] Wahab Khawaja, Ahmed Manavi Alam, and Ali C. Gurbuz. A two-stage 5G NR ISAC framework for coarse-to-fine UAV detection and tracking. In *Proc. IEEE Int. Symp. Spectrum Innovation (DySPAN)*, pages 1–8, 2026. doi: 10.1109/DySPAN69846.2026.11571167.