GNU Radio SDR Framework for Bistatic Sensing Using 5G NR Zadoff-Chu and SSB Waveforms

R Krishna Kanth, Dr. Khawaja Wahab, Dr. Ali C. Gurbuz

Department of Electrical and Computer Engineering
North Carolina State University

GNU Radio Conference 2026

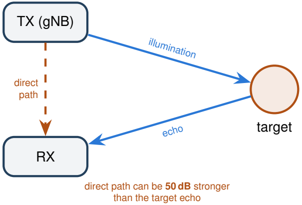
GRCon26
Raleigh, North Carolina

IMPRESS
INFORMATION PROCESSING AND SENSING

Why sense with 5G waveforms?

Integrated sensing and communications

- Reuse communication infrastructure for sensing i.e. no dedicated radar transmitter, spectrum or site
- Passive coherent location: detect targets using opportunistic signals



5G NR is a good illuminator

- Physical layer fully specified by 3GPP
- Synchronization signals are deterministic: a receiver can regenerate them without decoding user data
- Exactly what a matched filter needs

Same receiver architecture irrespective of TX signal - the hard part is doing it in real time.

The real-time problem

A sensing receiver must *continuously*:

1. suppress a direct-path signal orders of magnitude stronger than the echo,
2. matched-filter the residual,
3. reject static clutter,

... all while keeping pace with the sample stream.

- $f_s = 30.72\,\text{MS/s}$; $N_{ZC} = 16\,381$
- $\Rightarrow T_{PRI} = 0.533\,\text{ms}$
- $\Rightarrow \approx$ 1876 range profiles/s sustained

Why GNU Radio

- Streaming scheduler matches the problem
- Each stage becomes a reusable block
- Same chain runs in simulation and on hardware

Scope of this work

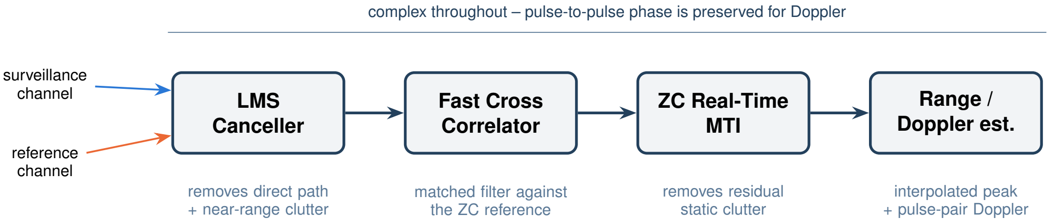
Cooperative bistatic testbed - transmitter under our control.

Not opportunistic sensing of a live commercial gNB.

Contributions

1. A complete **streaming sensing chain in GNU Radio**, as three reusable out-of-tree blocks running in real time at 30.72 MS/s:
   `LMS Canceller` → `Fast Cross Correlator` → `ZC Real-Time MTI`
2. A **waveform argument**: the standard SSB duty cycle is a few percent, so we radiate an extended Zadoff-Chu pilot continuously and show in simulation why it beats the full SSB burst
3. **Simulation characterisation** – drone target at four bistatic excess ranges (19.5–195.3 m), TCR above 35 dB
4. **Over-the-air validation**: a walking human tracked across a 38 m corridor, extended ZC compared against the 5G NR PSS

Processing chain



Each stage is one GNU Radio block. The same chain is used in simulation and over the air.

Stage 1 - adaptive cancellation

Complex LMS driven by the reference channel:

$$e[n] = y_{surv}[n] - \sum_{k=0}^{K-1} w_k[n]\, y_{ref}[n-k]$$

$$w_k[n+1] = w_k[n] + \mu\, y_{ref}[n-k]\, e^*[n]$$

What the tap count K means

- The filter converges to the stationary part of the surveillance channel over K delay bins
- A moving target carries time-varying phase, is poorly modelled by fixed weights, and survives

Two operating points

	Simulation	**Over the air**
K	1	5
μ	10^{-3}	10^{-7}
span	lag 0 only	$\approx$ first 20 m

- $K = 1$ in simulation leaves targets at $\tau_s \geq 2$ provably untouched
- $K = 5$ indoors also suppresses strong static returns near the antennas

Stages 2 and 3 - matched filter and clutter rejection

FFT matched filter

$$R[\tau] = \mathcal{F}^{-1}\{\mathcal{F}\{e[n]\} \cdot \mathcal{F}^*\{s[n]\}\}$$

- $N_{FFT} = 32\,768 \geq 2N_{ZC} - 1 \Rightarrow$ linear correlation
- Reference spectrum precomputed once
- Output kept complex - no magnitude taken

Exponential-average MTI

$$b_m[\tau] = (1-\alpha)b_{m-1}[\tau] + \alpha R_m[\tau]$$
$$\tilde{R}_m[\tau] = R_m[\tau] - b_m[\tau]$$

α must be matched to the target

$$f_{3dB} = \frac{\alpha}{2\pi T_{PRI}}$$

	α	f_{3dB}
Drone ($f_d \approx 160$ Hz)	0.10	29.9 Hz
Human ($f_d \approx 16$-24 Hz)	0.01	2.98 Hz

- $\alpha = 0.10$ would put a *walking human* below cutoff and attenuate it

Stage 4 - range and velocity estimation

Range:

- OTA testbed is quasi-monostatic (45 cm baseline), so the sum $\approx 2R$ and the target-range bin is $\Delta R = c/2B = 4.88\,\text{m}$
- Resolution is fixed by bandwidth; accuracy is improved by interpolating the peak

$$\delta = \frac{1}{2} \frac{|R[k-1]| - |R[k+1]|}{|R[k-1]| - 2|R[k]| + |R[k+1]|}$$

Single snapshot - no target motion required.

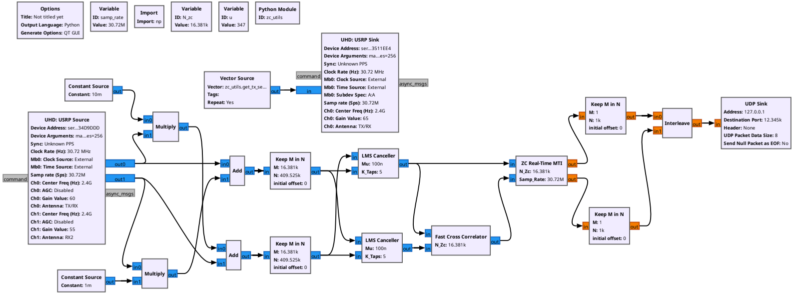
Velocity: pulse-pair estimator

$$\hat{f}_d = \frac{1}{2\pi T_{PRI}} \arg\left\{ \sum_m \tilde{R}_{m+1}[\tau^\star]\tilde{R}_m^*[\tau^\star] \right\}$$

- Doppler *resolution* over 3 pulses is poor ($\approx$39 m/s): two targets cannot be separated
- Doppler *accuracy* for one dominant target is a few Hz at realistic SNR

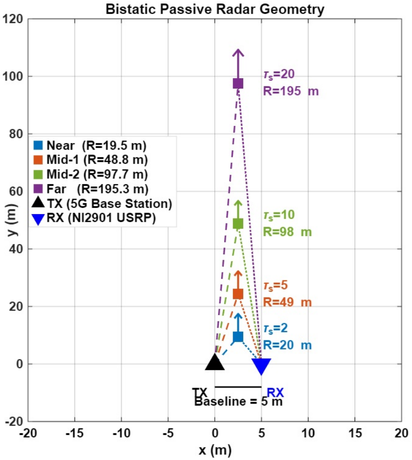
No coherent CPI over the air - by design.

GNU Radio implementation



- `LMS Canceller` runs first, at full rate
- Stream is decimated ahead of the correlator and MTI
- MTI output streamed over UDP for peak detection

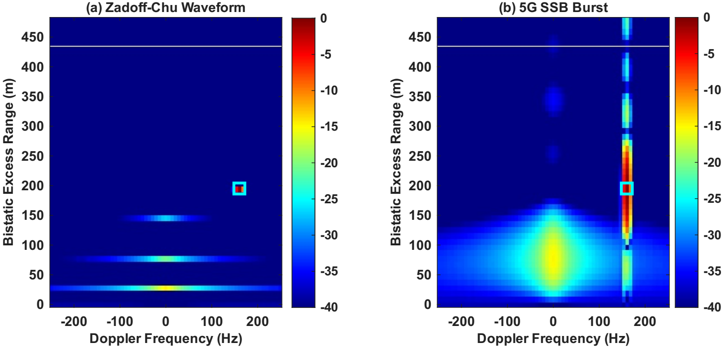
Simulation configuration



Parameter	Symbol	Value
Carrier	f_c	2.4 GHz
Sample rate	f_s	30.72 MS/s
ZC length / root	N_{ZC}, u	16 381 / 347
PRI	T_{PRI}	0.533 ms
Pulses per CPI	M_{CPI}	256
Direct-path ratio	DPR	50 dB
Drone RCS	σ	0.05 m^2
Drone speed	v	10 m/s

	Near	Mid-1	Mid-2	Far
τ_s	2	5	10	20
R_{bi} (m)	19.5	48.8	97.7	195.3

Why the ZC reference and not the full SSB



- **(a) ZC:** one clean target cell against a flat floor
- **(b) SSB:** same target, plus an OFDM-induced ridge across *all* range bins

Equal mean transmit power. The SSS and PBCH symbols are not CAZAC and the cyclic prefix adds periodic self-similarity - such a ridge would mask weaker returns at other ranges.

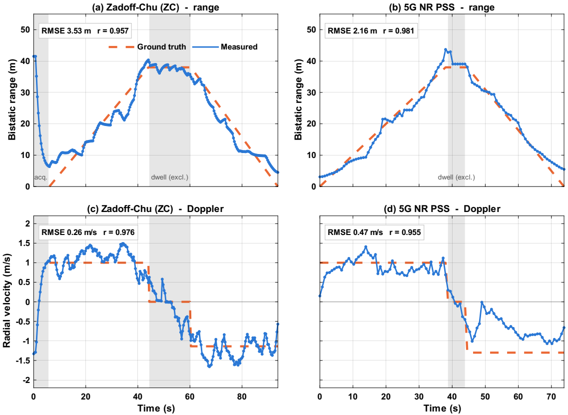
Over-the-air testbed

- Two NI USRP-2901: one transmits the continuous pilot, one is the two-channel sensing receiver
- Locked to a common **rubidium reference** - without it, LO drift appears as spurious Doppler
- Double Ridge Horn anetnnas on a 45 cm baseline along a **38 m** corridor
- Wired reference, with a controlled emulated impairment rather than an ideal replica

Experiment

One person walks to the far end, waits, walks back. Repeated for **extended ZC** and for the **5G NR PSS**.

Both waveforms track the walk end to end



- Measured range and velocity follow the constant-speed reference over the whole corridor. Range correlation > 0.95 for both waveforms
- Neither loses the target through the turn at the far end. Shaded spans (acquisition transient, far-end dwell) are excluded

Conclusions

- A complete bistatic sensing chain - LMS cancellation, FFT matched filtering, exponential-average MTI - runs **in real time at 30.72 MS/s** as three reusable GNU Radio out-of-tree blocks
- In simulation the chain recovers a drone target across **19.5-195.3 m** of bistatic excess range with **TCR above 35 dB**
- An extended Zadoff-Chu reference gives a markedly cleaner range-Doppler map than the full SSB burst at equal transmit power
- Over the air the chain tracks a walking human across a **38 m corridor** with both waveforms

Selected references

1. F. Liu *et al.*, “Integrated sensing and communications: toward dual-functional wireless networks for 6G and beyond,” *IEEE JSAC*, vol. 40, no. 6, pp. 1728–1767, 2022.
2. P. E. Howland, D. Maksimiuk and G. Reitsma, “FM radio based bistatic radar,” *IEE Proc. Radar, Sonar Navig.*, vol. 152, no. 3, pp. 107–115, 2005.
3. K. Abratkiewicz *et al.*, “SSB-based signal processing for passive radar using a 5G network,” *IEEE J. Sel. Topics Appl. Earth Obs. Remote Sens.*, vol. 16, pp. 3469–3484, 2023.
4. X. Lin *et al.*, “5G New Radio: unveiling the essentials of the next generation wireless access technology,” *IEEE Commun. Stand. Mag.*, vol. 3, no. 3, pp. 30–37, 2019.
5. B. Widrow and S. D. Stearns, *Adaptive Signal Processing*. Englewood Cliffs, NJ: Prentice-Hall, 1985.
6. N. J. Willis, *Bistatic Radar*, 2nd ed. SciTech Publishing, 2005.
7. GNU Radio Project, *GNU Radio: the free & open source radio ecosystem*, v3.10. `https://www.gnuradio.org`

Thank You

Any Questions?

R Krishna Kanth

krokkam@ncsu.edu

Department of Electrical and Computer Engineering
North Carolina State University

GRCon26
Raleigh, North Carolina

IMPRESS
INFORMATION PROCESSING AND SENSING