INSTITUTE FOR PHYSICAL AI @ BMI
The Charlot Lab

Technical Report TR-2026-13
Survey / Review · Preprint v1
7 July 2026

SPATIAL RF

Spatial RF: Spoof-Resistant Sensing by Cross-Spectrum Corroboration

Forgeability sets trust; only keyed-coherent bands can veto; silence lowers the bar rather than blinding the system.

David Jean Charlot, PhD

Dean of Physical AI · The Charlot Lab, Institute for Physical AI @ BMI

Correspondence: contact@physicalai-bmi.org · physicalai-bmi.org · The Charlot Lab: labs.physicalai-bmi.org/charlot
Interactive companion: physicalai-bmi.org/research/charlot-lab#topic-rf

Abstract. A single-band radio sensor is defeated by a single-band attack, which is the cheapest attack that exists. This report states a research position: a sensing fabric should span the whole usable spectrum and weight each band by how hard it is to forge, so that defeating the fabric requires forging a jointly consistent signature across every band at once. It reviews the primary sensing modalities the fabric composes — Wi-Fi channel-state information, millimeter-wave radar for vital signs and fall detection, through-barrier propagation, radio tomographic imaging over ambient links, authenticated ultra-wideband ranging, and physical-layer device fingerprinting — and the security results that motivate the design, chiefly distance-bounding and its known attacks. Section 2 states the review method. Section 3 gives a band portfolio and a forgeability-weighted trust model. Section 4 separates two authorities that are usually conflated: the authority to corroborate an event and the authority to veto one, and argues that only a keyed-coherent band should hold the second. Section 5 treats silence as a fault rather than a gap, so a dead or jammed node lowers the decision threshold and raises an alarm instead of blinding the system. Section 6 states the joint-consistency constraint that makes the fabric hard to defeat. Section 7 places the design beside through-barrier RF sensing. The design is described as a research programme, named Sentinel, with a public repository; no new experimental measurements are reported.

1. Introduction

Radio-frequency sensing has become capable enough to matter for safety. Commodity Wi-Fi radios read human motion and presence from channel-state information[1,2]; millimeter-wave radar measures respiration and heartbeat without contact[3] and detects falls[4,5]; radio links track motion through walls[6,7]. Where a sensor influences a physical decision, it becomes a target. An adversary who wants to hide an intrusion, suppress a fall alarm, or manufacture a phantom occupant does not need to defeat physics. He needs to defeat one receiver.

The economics are asymmetric and they favor the attacker. Almost every deployed RF sensor listens on one band with one phenomenology. A replayed Wi-Fi frame, a jammed sub-GHz link, a swept-tone injected into a radar's intermediate-frequency stage — each is a low-cost, single-band operation, and each is sufficient because the sensor has no second opinion. The defender pays for a whole sensor; the attacker pays for one band of it.

This report takes the position that the response is structural rather than incremental. If the cheapest attack is single-band, then sense across all bands, and price each band by how hard it is to forge. Low-trust ambient bands are allowed to corroborate an event but never to be the sole basis for asserting or denying one; a high-trust, keyed-coherent band, whose signature an attacker cannot synthesize without the key, is allowed to be decisive. A silent node is read as a fault, not a gap: it lowers the confidence the fabric requires and announces itself, rather than quietly removing a witness. Under this arrangement, to move the fabric's decision an adversary must produce a signature that is simultaneously consistent across bands with different physics, geometry, and timing, and that also carries valid cryptographic coherence on the bands that demand it. That joint object is physically incompatible with a remote single-band attack. The research effort that develops the fabric is named Sentinel.

2. Scope and method

This is a review and a research position. It surveys published RF-sensing modalities and the physical-layer security results that bear on their trustworthiness, and it proposes a fusion architecture on top of them. It reports no original experiments and no benchmark numbers; the trust model in Section 3 and the decision rules in Sections 4 through 6 are design specifications and conjectures, not measured results. Where a modality is mature the report says so, and where a claim is a design intention rather than a demonstration it is marked as such. The intent is to state the architecture precisely enough to be criticized and implemented, not to report that it has been validated. Reference implementations and the evolving specification are maintained in the open at github.com/dcharlot-physicalai-bmi/sentinel.

3. The band portfolio and a forgeability-weighted trust model

The fabric composes several bands, each contributing a different physical view of the same scene. Wi-Fi channel-state information gives dense, cheap motion and presence sensing from existing infrastructure[1,2]. Millimeter-wave radar contributes micro-Doppler signatures of respiration, heartbeat, and gait, and the fall events that follow from them[3,4,5,8]. Lower-frequency links, in and around the C-band and below, penetrate walls and furniture[7]. A mesh of ambient links, imaged as an ensemble rather than individually, reconstructs occupancy from

the shadowing a body casts across many paths, which is radio tomographic imaging[6]. Bluetooth Low Energy and sub-GHz perimeter radios add coarse proximity and long-range presence. Standing apart from all of these is authenticated ultra-wideband ranging, in which a keyed exchange measures time-of-flight that a relay or overshadowing attacker cannot shorten without breaking the protocol[9].

The organizing quantity is *forgeability*: the cost, to a remote adversary, of producing a receiver-side signal indistinguishable from the true one. A band's trust weight is a monotone function of that cost. Ambient bands that carry no authentication and can be replayed or injected sit low; radar micro-Doppler at range, which requires reproducing a distributed, moving scattering field rather than a single symbol, sits higher; a keyed-coherent ranging exchange, which binds the measurement to a secret, sits highest. Let each band b report a per-event corroboration $c_b(e) \in [0,1]$ and carry a trust weight w_b. The fabric's confidence in a candidate event e is the trust-weighted sum

$$S(e) \;=\; \sum_{b \in \mathcal{B}} w_b \, c_b(e), \qquad w_b \;=\; g\big(\kappa_b\big), \;\; g \text{ increasing},$$

where κ_b is the estimated forgeability cost of band b. Table 1 orders the portfolio by this weight and records the role each band is permitted to play, developed in Section 4. The weights are engineering estimates, not measurements; the point of writing them down is that they are auditable and can be revised against red-team evidence.

Table 1. The band portfolio, ordered by forgeability-derived trust. Roles are defined in Section 4: an ambient band may raise confidence but is never decisive; a keyed-coherent band may reject.

BAND / MODALITY	WHAT IT SENSES	TRUST (FORGEABILITY)	PERMITTED ROLE
UWB, keyed 802.15.4z-class ranging	authenticated time-of-flight, distance	High — bound to a secret	Corroborate + veto
mmWave FMCW radar	vitals, fall, gait micro-Doppler	Medium-high — hard to forge at range	Corroborate
C-band / sub-GHz through-barrier	motion behind walls	Medium — geometry-constrained	Corroborate
Mesh radio tomography	occupancy from link shadowing	Low-medium — needs many paths	Corroborate
Wi-Fi CSI	presence, motion	Low — replayable, unauthenticated	Corroborate
BLE / sub-GHz perimeter	proximity, long-range presence	Low — RSSI easily spoofed	Corroborate

Physical-layer device fingerprinting cuts across the table. Hardware imperfections leave a measurable signature in a transmitter's emissions, and both classical estimation and learned classifiers can identify a radio from them[10,11]. Fingerprinting raises the forgeability cost of

the ambient bands, because an injected frame must now also match the expected emitter's fingerprint, but it does not by itself confer veto authority: a sufficiently equipped adversary can approximate a fingerprint, whereas a keyed coherence check requires the secret.

4. Corroborate versus veto: only keyed-coherent bands can veto

The usual failure in multi-sensor fusion is to give every input the same kind of authority and merely weight it. That is unsafe under attack, because it lets an adversary who controls enough cheap bands overwhelm the sum. The fabric instead separates two authorities. The authority to *corroborate* is the power to raise confidence in an event; every band has it, in proportion to its weight. The authority to *veto* is the power to reject an event that the rest of the fabric believes, or to assert one on its own; the fabric grants it only to bands whose signatures are cryptographically bound and therefore cannot be manufactured remotely.

Concretely, a candidate event is admitted when the weighted evidence clears a threshold and no keyed band authentically contradicts it:

$$\mathrm{admit}(e) \iff \Big[\, S(e) \geq \Theta \,\Big] \;\wedge\; \Big[\, \nexists\, k \in \mathcal{K} :\; \mathrm{auth}_k \;\wedge\; c_k(\neg e) \geq \tau_k \,\Big],$$

where $\mathcal{K}$ is the set of keyed-coherent bands and $\mathtt{auth_k}$ marks a ranging exchange that passed its cryptographic check. Two properties follow by construction. First, ambient bands can only push `S(e)` upward; an adversary who floods Wi-Fi CSI or spoofs BLE proximity can add corroboration he does not deserve but cannot force the fabric to *deny* a real event, because denial requires an authenticated keyed contradiction he cannot produce. Second, no quantity of cheap corroboration substitutes for the keyed check when a decision is high-stakes: the threshold `Θ` for such decisions is set above what the ambient bands can sum to, so a real assertion still needs a high-trust witness. The design goal is that the least forgeable band is the one that gets to say no.

This structure has direct precedent in the security literature. Distance-bounding protocols were introduced precisely so that a verifier could establish an upper bound on its distance to a prover that a relay could not defeat[12], and the subsequent discovery of distance-hijacking attacks[13] and the pulse-reordering defenses that answer them[9] are exactly the analysis of when a keyed ranging band earns the authority the fabric assigns it. The lesson the fabric imports is that veto authority must be justified by an attack model, not assumed.

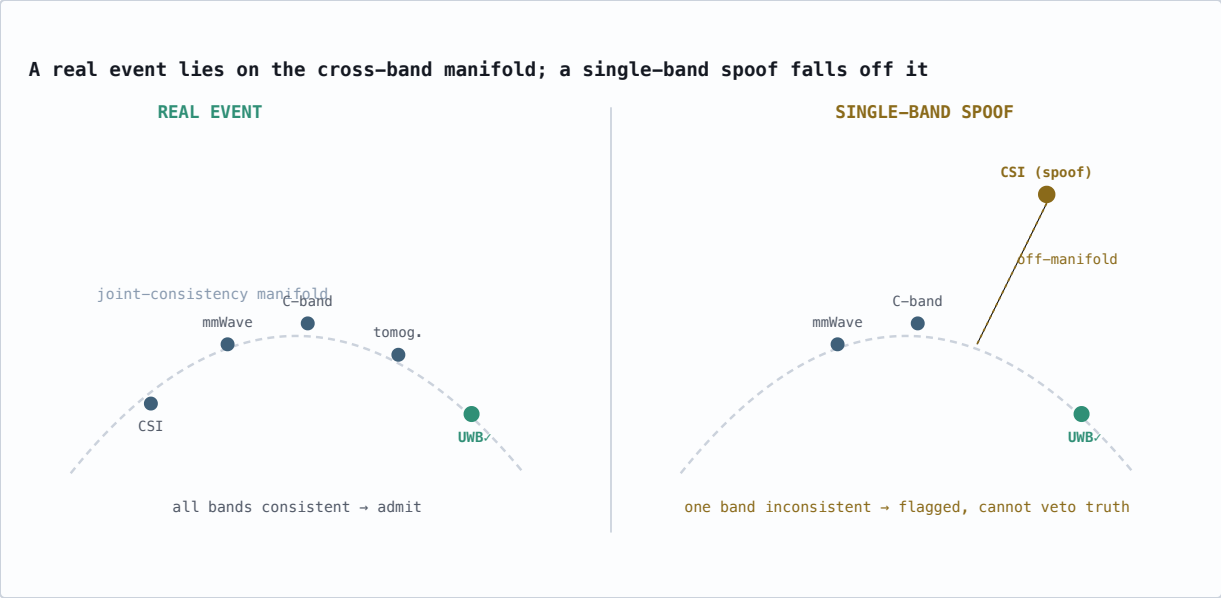

Figure 1. Schematic of the joint-consistency test. Left: a real event produces per-band readings that all lie near the manifold of physically realizable cross-band signatures, including a passing keyed UWB check, and the event is admitted. Right: an adversary who forges only the Wi-Fi CSI band produces a reading that is off the manifold relative to the honest bands and the keyed check, so the fabric flags the inconsistency; because CSI holds only corroboration authority, the spoof cannot deny the event the other bands support. Positions are illustrative. Interactive version: physicalai-bmi.org/research/charlot-lab.

5. Silence is a fault, not a gap

A conventional sensor that goes quiet is assumed to have nothing to report. That assumption is an attack surface: jamming a link, cutting power to a node, or pointing a directional antenna to overshadow one produces exactly the same quiet, and the system reads deliberate blinding as an all-clear. The fabric refuses that reading. A band that should be reporting and is not is treated as a fault, which has two consequences.

First, the missing band's weight is removed from the confidence budget, so the threshold the remaining bands must clear is lowered rather than left unmet:

$$\Theta' \;=\; \Theta \;-\; \sum_{b \in \mathcal{S}} w_b, \qquad \mathcal{S} = \{\, b : \; \mathrm{silent}(b) \,\},$$

so a dead or jammed node lowers the bar for the surviving witnesses instead of making the event unprovable. A body that a jammed Wi-Fi radio can no longer see is still admitted on radar and keyed ranging, at a threshold that no longer expects the Wi-Fi vote. Second, silence itself is an event. Loss of an expected band, especially the abrupt loss consistent with jamming or overshadowing, raises an alarm on its own channel; the fabric fails loud. The design intent, not yet a measured property, is that an adversary gains nothing by silencing a node, because silencing lowers the evidentiary bar and simultaneously reports the silence.

> Degradation is graceful and legible. Removing a node from the fabric moves it toward a smaller fabric with a lower threshold and a raised alarm, never toward a blind fabric that reports all-

clear. A system that cannot be quietly blinded forces an attacker into actions that are themselves detectable.

6. Why the fabric is hard to defeat

The security argument is a joint-consistency constraint. Every band observes the same physical scene through different physics: Wi-Fi CSI sees multipath perturbation, radar sees range and micro-Doppler, tomography sees link shadowing across a mesh, keyed UWB sees authenticated time-of-flight. For a real event these views are not independent; they are different projections of one geometry and one motion, and the set of jointly realizable readings forms a low-dimensional manifold in the product of the bands' measurement spaces. Detection can be posed as proximity to that manifold. Write the fabric's reading as a vector $x = (x_b)$ and let M be the realizable manifold; the fabric admits an event only when the honest bands are mutually consistent,

$$\operatorname{dist}\big(x,\, M\big) \;\le\; \epsilon \quad \text{and} \quad \operatorname{auth}_k \text{ holds for the keyed bands } k \in \mathcal{K}.$$

An adversary attacking one band controls one coordinate x_b. To avoid detection he must place the full vector back on M, which means his forged coordinate must be consistent with every other band's honest reading of the real scene, at the real geometry, timing, and Doppler — while the keyed coordinates must additionally carry valid cryptographic coherence he does not have. Forging one band is cheap; forging a coordinate that is jointly consistent with all the others and cryptographically coherent is the original expensive problem restored across the entire spectrum at once. The physics of the bands are not independently addressable by a remote transmitter, so the joint object is, for practical adversaries, physically incompatible with a single-band attack. This is a design argument, not a proof; its assumptions are that the bands are genuinely diverse in phenomenology, that the manifold is well estimated, and that at least one keyed band is present and healthy. Where those hold, the cost of defeating the fabric scales with the number of bands rather than remaining fixed at one.

7. Position and discussion

Spatial RF is a defensive counterpart to the Charlot Lab's through-barrier sensing work under OmniSense. Where OmniSense asks what a single radio band can perceive through walls and occlusion, drawing on the same tomographic and through-wall results surveyed here[6,7], Spatial RF asks how a set of such perceptions can be combined so that no one of them is a single point of failure. The two are complementary: the more capable each band becomes at seeing through the world, the more it matters that no single band can be made to lie unchallenged. The fusion architecture is agnostic to which bands are available and degrades, by the rule of Section 5, to whatever subset is healthy.

The report claims no validation. The trust weights, the corroborate-versus-veto split, the silence rule, and the manifold test are specifications to be implemented and attacked, and the honest expectation is that red-teaming will revise the weights and expose cases the manifold

model does not capture. The contribution is the framing: make forgeability the currency, separate corroboration from veto, treat silence as a fault, and require joint consistency. That framing is meant to be falsifiable, and the open repository exists so that it can be.

8. Conclusion

The cheapest attack on a sensor is a single-band attack, and single-band sensing invites it. Spatial RF proposes to remove the invitation by sensing across the whole spectrum, pricing each band by how hard it is to forge, letting low-trust ambient bands corroborate but never veto, reserving veto for keyed-coherent bands, and treating a silent node as a fault that lowers the bar and raises an alarm rather than a gap that blinds. Under this arrangement, defeating the fabric requires a jointly consistent, cryptographically coherent forgery across every band at once, which is physically incompatible with the cheap single-band attack the design was built to deny. The modalities the fabric composes are mature and well documented; the fabric itself is an early-stage research programme, Sentinel, offered here for scrutiny.

References

1. Y. Ma, G. Zhou, S. Wang. WiFi sensing with channel state information: a survey. *ACM Computing Surveys* 52(3), 2019. doi:10.1145/3310194.
2. D. Halperin, W. Hu, A. Sheth, D. Wetherall. Tool release: gathering 802.11n traces with channel state information. *ACM SIGCOMM Computer Communication Review* 41(1), 2011. doi:10.1145/1925861.1925870.
3. C. Li, V. M. Lubecke, O. Boric-Lubecke, J. Lin. A review on recent advances in Doppler radar sensors for noncontact healthcare monitoring. *IEEE Trans. Microwave Theory and Techniques* 61(5), 2013. doi:10.1109/TMTT.2013.2256924.
4. J. van Berlo, A. Elkelany, T. Ozcelebi, N. Meratnia. Millimeter wave sensing: a review of application pipelines and building blocks. *IEEE Sensors Journal* 21(9), 2021. doi:10.1109/JSEN.2021.3057450.
5. M. B. Akash, M. Shahria, et al. Elderly patient monitoring and fall detection using mmWave FMCW radar system. *2023 26th Int. Conf. on Computer and Information Technology (ICCIT)*, 2023. doi:10.1109/ICCIT60459.2023.10441619.
6. J. Wilson, N. Patwari. See-through walls: motion tracking using variance-based radio tomography networks. *IEEE Trans. Mobile Computing* 10(5), 2011. doi:10.1109/TMC.2010.175.
7. F. Adib, D. Katabi. See through walls with WiFi! *Proc. ACM SIGCOMM 2013*. doi:10.1145/2486001.2486039.
8. J. Lien, N. Gillian, M. E. Karagozler, P. Amihood, C. Schwesig, et al. Soli: ubiquitous gesture sensing with millimeter wave radar. *ACM Trans. Graphics* 35(4), 2016. doi:10.1145/2897824.2925953.
9. M. Singh, P. Leu, S. Capkun. UWB with pulse reordering: securing ranging against relay and physical-layer attacks. *Proc. Network and Distributed System Security Symposium (NDSS)*, 2019. doi:10.14722/ndss.2019.23109.
10. B. Danev, D. Zanetti, S. Capkun. On physical-layer identification of wireless devices. *ACM Computing Surveys* 45(1), 2012. doi:10.1145/2379776.2379782.
11. K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis, et al. ORACLE: optimized radio classification through convolutional neural networks. *IEEE INFOCOM 2019*. doi:10.1109/INFOCOM.2019.8737463.
12. S. Brands, D. Chaum. Distance-bounding protocols. *Advances in Cryptology — EUROCRYPT '93*, LNCS 765, 1994. doi:10.1007/3-540-48285-7_30.
13. C. Cremers, K. B. Rasmussen, B. Schmidt, S. Capkun. Distance hijacking attacks on distance bounding protocols. *2012 IEEE Symposium on Security and Privacy*. doi:10.1109/SP.2012.17.
14. J. Seo, T. Lee, J. Im, G.-I. Jee, et al. Efficient spoofing identification using baseline vector information of multiple receivers. *GPS Solutions* 22(4), 2018. doi:10.1007/s10291-018-0779-x.

AI-use disclosure. Preparation of this report used a large language model (Claude, Anthropic) for drafting and editing text, organizing the reviewed literature, and preparing the figures and the interactive companion. Cited references were checked to resolve to their sources. The author reviewed the content and is solely responsible for it. Consistent with ICMJE, COPE, and IEEE guidance, the model is a tool and is not credited as an author.

Institute for Physical AI @ BMI · The Charlot Lab
503 McKeever Rd, Arcola, TX 77583, USA
physicalai-bmi.org · contact@physicalai-bmi.org

Technical Report TR-2026-13 · Preprint v1