AUDEAMUS GROUP, LLC

Wi-Fi Sensing & Privacy Weekly Brief

October 2, 2026 | Historical public-summary edition

HISTORICAL PUBLIC SUMMARY

Cross-room tracking sheds calibration — while sensing security catches up

September 25–October 2, 2026 · Three items met the relevance, date and evidence checks. New research: self-calibrating passive Wi-Fi tracking across walls and an LLM-controlled one-shot adaptation method for CSI sensing. Meaningful publication update: an open manuscript of a 2026 IEEE letter on authenticating sensing packets against spoofing. Meaningful standards and regulatory updates: none verified for inclusion. The week's strongest signal is that researchers are reducing two deployment costs—site calibration and labeled target data—while beginning to treat sensing signals as security-critical inputs; all three results still depend on bounded experiments or simulation.

01 / NEW · arXiv preprint · Wang et al. / 2026-09-28

Cross-Room Passive WiFi Tracking: Joint Estimation of Target Trajectory and Virtual Transmitter Location

Key finding. CoTrack jointly estimates a moving person’s trajectory and the location of a virtual transmitter using CSI-derived relative delay, angle, and Doppler measurements. This removes the need to know the transmitter’s physical position in advance, enabling passive cross-room tracking with less calibration. Across six line-of-sight and through-wall experiments, the system reports a median trajectory error of 1.14 meters and a median virtual-transmitter error of 0.47 meters.

Why it matters for Audeamus. Removing transmitter-location calibration is directly relevant to whole-home sensing, where one access point may serve receivers in several rooms and the dominant path through walls does not match direct geometry. The paper also analyzes when the joint estimate is identifiable and shows that motion diversity is an operational reliability condition.

Evidence limits. All six runs use one classroom, one walking target, Intel 5300 radios, a three-antenna receiver and 1-kHz CSI, with approximate room bounds supplied to the optimizer. Accuracy is still meter-scale; the virtual-transmitter reference is partly fitted using radar for evaluation, and pets, stationary presence, multiple people and unfamiliar homes are untested.

Read in full? Read in full. It tackles a real installation constraint with both theory and live cross-wall measurements, but the hardware and single-site protocol define a large productization gap.

Open original source

© 2026 Audeamus Group, LLC. All rights reserved. This report is the property of Audeamus Group, LLC and reflects solely its opinions. It is for informational purposes only and must not be relied upon as legal or investment advice. Third-party materials remain the property of their respective owners.

02 / NEW · arXiv preprint · Zhao et al. / 2026-09-25

CSI-Agent: LLM-Assisted Few-Shot Adaptation for Cross-Domain Wi-Fi CSI Sensing

Key finding. The paper recasts deployment-time adaptation as a class-by-class decision problem. An LLM sees structured diagnostic cards—not raw CSI—and chooses among bounded adaptation actions; a deterministic verifier can reject harmful choices. With one labeled target example per class, the system reports an average Macro-F1 of 0.489 across five device, user, environment, and compositional shifts, versus 0.323 for the strongest baseline.

Why it matters for Audeamus. Cross-home and cross-device failure is one of Wi-Fi sensing's largest commercial barriers. A short enrollment step plus constrained, auditable adaptation could lower per-home calibration cost, and similar results across four tested LLM planners suggest the gain is not tied to one model vendor.

Evidence limits. The evaluation replays four public datasets rather than deploying in occupied homes, assumes a closed label set and requires one labeled example for every class. The LLM selects from a hand-built action toolbox using aggregate query statistics; it does not discover new activities or prove safe long-term autonomy, and target Macro-F1 remains below 0.50 on average.

Read in full? Read in full. The agent is unusually constrained and well ablated, making this a useful deployment architecture even though the absolute cross-domain performance is not product-ready.

Open original source

© 2026 Audeamus Group, LLC. All rights reserved. This report is the property of Audeamus Group, LLC and reflects solely its opinions. It is for informational purposes only and must not be relied upon as legal or investment advice. Third-party materials remain the property of their respective owners.

Wi-Fi Sensing & Privacy Weekly Brief

October 2, 2026 | Historical public-summary edition

03 / UPDATE · Open manuscript of 2026 IEEE Wireless Communications Letters paper · Zerrari et al. / 2026-09-27

Backward-Compatible Tag-Based PHY Authentication for Secure WLAN Sensing

Key finding. Makes an open author manuscript available for an earlier 2026 IEEE letter. The design overlays a per-transmission secret tag on 802.11 OFDM sounding pilots, randomizes tagged subcarriers, and verifies the tag before accepting sensing input; the authors report more than 96% authentication at a 5% false-alarm rate in one simulated setting.

Why it matters for Audeamus. Wi-Fi sensing decisions can be spoofed because standard sounding sequences are public. Authenticating the measurement source without breaking unaware legacy receivers is relevant to alarm, access and health-monitoring products, and provides a concrete security mechanism for future WLAN-sensing profiles.

Evidence limits. The result is simulation-only under an 802.11ac channel model, not a new standard contribution or tested 802.11bf implementation. It assumes shared secret management, leaves signal-superposition and near-far attacks for future work, and still adds 0.52 dB channel-estimation error at the cited conservative legacy setting.

Read in full? Skim. The threat and compatibility tradeoff are important, but the short paper's evidence stops before hardware, protocol integration and adversarial testing.

Open original source

ARCHIVE NOTE

This edition preserves the dated public summary and original citations from Wi-Fi Sensing Review. It has been repackaged for the Audeamus Group archive; the historical claims have not been independently reverified during this formatting pass. No private desk analysis is included.

Original public Wi-Fi Sensing Review

© 2026 Audeamus Group, LLC. All rights reserved. This report is the property of Audeamus Group, LLC and reflects solely its opinions. It is for informational purposes only and must not be relied upon as legal or investment advice. Third-party materials remain the property of their respective owners.