OpenWrt-Oriented Cooperative Multi-AP Wi-Fi Sensing with Reliability-Aware Fusion and QoS-Bounded Measurement Control

Volodymyr Pavlenko

Department of Electronic Computing Machines, Lviv Polytechnic National University, Lviv, Ukraine
volodymyr.v.pavlenko@lpnu.ua

Introduction

Cooperative Wi-Fi sensing across multiple access points is attractive for indoor monitoring because spatial diversity can reduce blind spots, stabilize detection when one wireless link fades, and move sensing closer to realistic controller-managed deployments than single-link laboratory demonstrations. In practice, however, multi-AP sensing is difficult to reproduce because different access points expose different chipsets, firmware branches, capture tools, packet-delivery behavior, timing quality, and sensing modalities. Prior cooperative Wi-Fi sensing work already shows the value of multi-link CSI fusion, AP-side CSI collection workflows such as CSI Sniffer, CSI transport reduction by compression methods such as EfficientFi and RSCNet, and coexistence-aware sensing traffic control in Slim-Sense and UniFi-style controller-managed operation. These studies solve important parts of the problem, but they usually treat fusion accuracy, measurement transport, and communication coexistence as separate concerns. They also do not define a single commodity-AP protocol that states how unreliable links are handled, how sensing remains inside controller-visible service budgets, and what another group must log to repeat the same policy. This work addresses that gap for OpenWrt-oriented deployments by defining a reproducibility-oriented workflow that makes per-link reliability assessment, controller-visible quality-of-service constraints, and a reproducibility manifest explicit in one protocol.

Methods

The workflow assumes N OpenWrt access points or OpenWrt-compatible AP nodes and one central coordinator reachable through the management plane. Each access point runs a lightweight local agent that converts raw Wi-Fi measurements into compact descriptors derived from received signal strength and, where hardware support exists, channel state information, while also reporting packet acceptance, temporal stability, timestamp consistency, and modality availability. The coordinator assigns a reliability score to each link, aggregates local descriptors with reliability-aware weighting, and exposes explicit measurement-budget controls over the active access-point subset, sensing modality, capture rate, and burst duration under configured limits on sensing airtime share, protected-flow throughput loss, and protected-flow latency inflation. For early validation, the protocol was instantiated in a small indoor setup using ESP32-C5 and ESP32-S3 sensing nodes, a primary prplOS-compatible dual-band AP node on 5 GHz channel 36, an additional 5 GHz helper

AP node, a dedicated 2.4 GHz helper AP on channel 6, Linux helper nodes, UDP CSI-summary capture, feature-window export, controller-decision logs, and SSH byte-stream protected-traffic traces collected by a laptop coordinator with two Wi-Fi adapters. The block protocol included warm-up, empty-room, static-presence, and motion periods. Each run also records a minimum manifest covering access-point role, chipset or sensing node, firmware or tool profile, radio configuration, sensing policy, topology role, synchronization evidence, and protected-traffic profile. The same run files are intended to be sufficient for a second laboratory to reconstruct the topology, radio state, sensing mode, controller policy, and protected-flow context without relying on hidden operator notes.

Results

The current result is a concrete workflow specification and evaluation contract rather than a finished large-scale benchmark. The method is designed to turn heterogeneous access-point-side measurements into a common coordinator-facing representation, proposes an operational rule for down-weighting or excluding unreliable links before fusion, and makes sensing and communication coexistence measurable through controller-side budget variables. The early validation had two limited purposes: to check that the capture/control evidence can be logged on hardware, and to sanity-check the fusion rule before larger experiments. In the indoor setup, the workflow captured live CSI-summary streams, feature windows, controller decisions, timing evidence, selected-node information, and protected-traffic traces under the stated block protocol. A synthetic three-link sanity-check comparison then illustrates the intended trade-off: reliability-weighted fusion raises a normalized stability index from 0.68 to 0.79 while keeping protected-flow throughput loss within a 3% service budget, increasing from 2.4% to 2.7%. This numeric example is not presented as a large-scale detection-accuracy result; it is used to verify that the proposed budget and reliability variables behave coherently before full testbed evaluation. The hardware pass also checked a practical failure mode emphasized by the workflow: if a link lacks usable CSI or shows unstable packet acceptance, the coordinator can keep that link visible in the manifest while excluding it from the fused descriptor. This keeps negative evidence available for audit instead of silently dropping failed AP observations. The workflow also defines a minimum manifest that reduces ambiguity during reproduction on another OpenWrt-oriented testbed.

Conclusions

The proposed workflow provides a structured and falsifiable deployment protocol for cooperative Wi-Fi sensing on commodity access-point infrastructure under realistic controller constraints. Relative to prior cooperative Wi-Fi sensing, CSI capture, compression, and coexistence-aware traffic-control studies, its practical value is to combine reliability-aware fusion, QoS-bounded measurement control, and reproducibility reporting in one OpenWrt-oriented baseline. This gives future OpenWrt testbed studies a common reference for what to log, what to budget, and how to compare cooperative policies fairly. The next step is broader quantitative experimentation on a real multi-access-point OpenWrt platform for binary presence or localization-style tasks under fixed service budgets. Accordingly, the work is positioned as a repeatable control and reporting baseline; later experiments will quantify task accuracy and service degradation under broader OpenWrt testbed conditions.

Wireless LAN (IEEE 802.11); Channel state information; Quality of service; Reliability; Verification and validation.

Conflict of Interest

The author declares no conflicts of interest.

Acknowledgments

This work draws on materials and intermediate results from the project “Intelligent Methods and Tools for Designing Modules for Autonomous Cyber-Physical Systems” (state registration No. 0124U002340, 2024–2028, Lviv Polytechnic National University).