# Feasibility Study: IP-Based Mesh Wi-Fi Infrastructure with Anti-Jamming Features for Long-Distance Control and Video Transmission

Prepared for Expert / PhD Review

October 8, 2025

**Abstract**

This study evaluates the feasibility of an IP-based wireless mesh that carries (i) narrowband control/telemetry over long distances and (ii) wideband video/data at shorter to mid ranges, with explicit anti-jamming mechanisms. We outline a dual-layer, multi-band architecture combining Sub-GHz narrowband links with 5.8 GHz Wi-Fi backhaul, propose spectrum-agile countermeasures, and summarize candidate hardware/software. The goal is to solicit scholarly review on technical risks, regulatory constraints, and research opportunities.

## 1 Objectives

- Dual-layer design:
  - **Layer 1 (Control)**: narrowband, high link budget, long range; carries command/telemetry and coordination beacons.
  - **Layer 2 (Video/Data)**: wideband 5.8 GHz mesh for high throughput (e.g., HD video).
- Anti-jamming: spectrum sensing, adaptive hopping, side-channel coordination.
- End-to-end IP compatibility (802.11s/batman-adv, WPA3/WireGuard).
- Preference for COTS components; pathway to SDR/FPGA miniaturized front ends.

## 2 System Architecture

### 2.1 Topology Overview

- **Primary Backhaul (5.8 GHz, Wi-Fi 6/6E)**: e.g., Qualcomm QCN9074 class radios, 20–40 MHz channels, 802.11s mesh; video/data, RoIP.
- **Secondary Control Link (Sub-GHz, e.g., 865–868 MHz)**: 802.11ah (Wi-Fi HaLow) or SDR-based narrowband; control, failsafe, coordination. Duty-cycle/EIRP per local regulation.
- **Inter-band Coordination**: fast channel switch via 802.11h CSA; side-channel beacons on Sub-GHz when 5.8 GHz is impaired.

### 2.2 Data Flow

1. **Control/Telemetry**: prioritized on Sub-GHz; robust MCS and small bandwidth.
2. **Video/Data**: prioritized on 5.8 GHz mesh; rate control, aggregation, FEC as needed.
3. **Resilience**: when jamming/interference detected, push CSA + routing updates via Sub-GHz; maintain encrypted tunnels across hops.

## 3 Anti-Jamming Strategy

### 3.1 Detection

- PHY/MAC metrics: CCA busy, PER, retries, RSSI/Noise floor drift.
- Periodic spectrum snapshots (ath11k/ath12k survey) and/or passive SDR probe.

### 3.2 Decision and Response

- Compare against baseline noise models; declare impairment if thresholds exceeded.
- Execute coordinated channel hopset update (802.11h CSA), announced on Sub-GHz side-channel.

### 3.3 Recovery

- Preserve WireGuard/IPsec tunnels across frequency change.
- Validate link via packet loss and RTT; gradually restore MCS and frame aggregation.

## 4 Hardware Feasibility

### 4.1 Backhaul and Control Radios

- **5.8 GHz Mesh**: QCN9074/IPQ-class modules; OpenWrt/QSDK support.
- **Sub-GHz Control**: 802.11ah modules *or* SDR transceivers configured for narrowband.

### 4.2 SDR/FPGA With Tunable RF Front Ends

Modern SDR transceivers integrate mixers, fractional-N synthesizers, and data converters in small SMD packages, exposing digital I/Q to an FPGA:

- **ADI AD9361**: 70 MHz–6 GHz tuning, on-chip synthesizers, 12-bit ADC/DAC; compact package; FPGA interface.
- **Lime LMS7002M**: 100 kHz–3.8 GHz tuning; dual-TX/RX; integrated LO/filters; FPGA interface.
- **Qorvo RFFC2072** (reconfigurable converter): 5×5 mm QFN, fractional-N PLL + VCO + high-linearity mixer for agile LO/IF translation.

These parts enable compact, tunable front ends that can fit small UAV enclosures while providing flexible band selection under FPGA control.

### 4.3 Spectrum Sensing

- Low-cost SDR probe (e.g., RTL-SDR, LimeSDR Mini) to provide out-of-band monitoring for jamming/interference classification.

## 5 Software Stack

- **OS/Firmware**: OpenWrt/QSDK with ath11k/ath12k.
- **Mesh**: 802.11s with `batman-adv` or `OLSR`.
- **Security**: WPA3-SAE; overlay tunnels (WireGuard) for session continuity.
- **Anti-Jam Daemon**: userspace agent (C/C++/Python) that reads survey/SDR inputs, computes hop decisions, signals CSA, tracks recovery KPIs.
- **SDR Control**: GNU Radio or FPGA gateware to tune Sub-GHz link parameters (BW, LO, gain, filters).

## 6 Regulatory and Practical Constraints (India Example)

- **5.8 GHz** (5.825–5.875 GHz): unlicensed outdoor Wi-Fi with EIRP/DFS compliance.
- **865–868 MHz**: SRD band; ERP and duty-cycle limits apply (often $\leq$ 1% duty cycle). Continuous control may require licensing.
- Airworthiness, EMC, and power budgeting for UAV payloads.

## 7 Risk and Mitigation

- **Jamming sophistication** $\rightarrow$ multi-modal detection, hopsets, spatial diversity, Sub-GHz keep-alive.
- **Payload power/size** $\rightarrow$ prefer integrated SDR+FPGA SoMs; aggressive power states.
- **Complexity** $\rightarrow$ staged MVP (fixed hopset, manual triggers) before full autonomy.
- **Regulatory** $\rightarrow$ pre-consultation; fallback to permitted bandwidth/duty cycles; logging.

## 8 Bill of Materials (Major Items)

| Function | Candidate | Notes |
|---|---|---|
| 5.8 GHz mesh backhaul | Qualcomm QCN9074 class | Wi-Fi 6, 4x4; OpenWrt/QSDK; 20–40 MHz channels. |
| Sub-GHz control link | 802.11ah module or SDR | Narrowband control; high link budget; duty-cycle aware. |
| Integrated SDR transceiver | ADI AD9361 / Lime LMS7002M | Tunable SMD RF front end; I/Q to FPGA; small footprint. |
| Reconfigurable converter | Qorvo RFFC2072 | 5×5 mm QFN; PLL+VCO+mixer; agile LO/IF. |

| | | |
|---|---|---|
| FPGA/SoM | Zynq/Artix or similar | Baseband, SDR control, glue logic. |
| LNA / IF amp / PA | COTS RF stages | Gain/noise/linearity budget per link budget. |
| Switching/filters | RF switches, SAW/LC | Band selection and out-of-band rejection. |
| Spectrum probe | RTL-SDR / LimeSDR Mini | Passive monitoring; jammer classification. |
| Enclosure/thermal | Custom UAV-grade | Isolation, airflow, vibration. |
| Power system | DC/DC, EMI filters | Clean rails for RF + digital domains. |

## 9 Prototype & Test Plan

### 9.1 MVP 1: Bench

- OpenWrt node (QCN9074), Sub-GHz SDR node, wired control PC.
- Anti-jam daemon triggers channel switch on induced interference.
- Validate tunnel continuity and recovery time.

### 9.2 MVP 2: Field

- Two to four mesh nodes on tripods/UAV test rack.
- Video over 5.8 GHz; control over Sub-GHz; scripted RF impairment (noise/jammer).
- KPIs: hop execution time, packet loss, PSNR for video, control latency, energy per bit.

## 10 Open Research Questions (for PhD Review)

1. Optimal cross-layer policy for detecting and classifying jamming vs. congestion in real time.
2. Fast, reliable inter-band coordination with minimal control overhead.
3. SDR/FPGA co-design for miniature, low-power, tunable RF front ends on UAV payloads.
4. Learning-based channel/route selection under mobility and interference.
5. Security analysis of frequency-agile meshes (linkability, traffic analysis resistance).

## 11 Conclusion

A hybrid multi-band mesh is feasible with COTS Wi-Fi backhaul and a Sub-GHz control side-channel. SDR/FPGA-based tunable RF front ends enable compact form factors while preserving agility. Key success factors are robust anti-jamming logic, careful RF design, regulatory alignment, and staged validation.

## Appendix: Expert Review Checklist

Please comment on:

1. **RF Link Budget**: margins for control vs. video at target distances; antenna choices.

2. **Front-End Linearity/Noise**: SDR/FPGA choice, filter plan, duplexing.
3. **Jamming Model**: detection features, thresholds, false positives.
4. **Hopset Design**: channel pool size, dwell times, coordination latency.
5. **Security**: tunnel continuity, key management across hops.
6. **Power/Thermal**: expected draw per node; cooling on UAV.
7. **Regulatory**: duty-cycle/EIRP assumptions and compliance path.