

Robust Drone-to-Drone Communications for Innovative Air Mobility: Physical-Layer Threat Assessment and Antenna-Based Mitigation

Lukas Schalk, Miguel A. Bellido-Manganell, Andrés Biedma-Pérez, Yusuf Çolak

German Aerospace Center (DLR), Institute of Communications and Navigation

1 Introduction

Innovative Air Mobility (IAM) envisages high-density operations in urban environments, which require safe and scalable traffic management concepts. Within these, separation can no longer rely on ground infrastructure and radar coverage alone; it depends on aircraft directly and continuously informing each other about their position and intent. This makes the drone-to-drone communication link a safety-critical element of the IAM system. The drone-to-drone communications system DroneCAST (Drone Communications and Surveillance Technology), developed by the German Aerospace Center (DLR), enables such a direct exchange between unmanned aerial vehicles. Jamming or spoofing at the physical layer, however, is enough to degrade cooperative situational awareness or inject false position information into it. Ground-based interference is especially relevant, as IAM operates at low altitude where jammers are easy to deploy and hard to avoid.

This work makes three contributions. First, it presents a physical-layer threat-and-risk analysis specific to drone-to-drone broadcast communications in the context of IAM, rating seven threats by severity and likelihood under a defined attacker model. Second, it maps these threats onto countermeasures in a layered resilience framework, identifying antenna-based spatial filtering as one of the few mitigations addressing the most probable threats without requiring additional spectrum, waveform changes, or the certification burden of learning-based methods. Third, it designs and evaluates such a countermeasure: a compact circularly polarized patch antenna meeting the bandwidth requirement of the DroneCAST drone-to-drone communications link, and a four-element array that suppresses two ground-based jammers arriving simultaneously from different directions while preserving air-to-air coverage.

2 Attack Scenarios and Countermeasures

The analysis assumes an external attacker without cryptographic credentials or physical access to the aircraft, operating through radio-frequency interference, passive interception, signal impersonation, or manipulation of satellite navigation signals. The resulting threats are listed in Table 1. Severity is taken as the maximum impact across communication availability, navigation availability and integrity, signal authenticity, situational awareness, confidentiality, and operational continuity, because a threat can be safety-critical even if it affects only one dimension. Likelihood is derived from feasibility factors such as attacker proximity, equipment availability, required waveform knowledge, and timing precision. Attacks based on jamming emerge as the most probable threats, since they require moderate equipment and little waveform knowledge, whereas spoofing of navigation signals is the most severe, because the aircraft may trust and subsequently broadcast a false position.

Table 1: Physical-layer threats for DroneCAST with severity (S) and likelihood (L), rated 1–5.

ID	Category	Threat description	Severity	Likelihood
T1	Link availability	Constant / barrage jamming	4	4
T2	Link availability	Reactive jamming	4	3
T3	Link availability	Selective / protocol-aware jamming	4	2
T4	Navigation availability	Jamming of satellite navigation signals	4	4
T5	Navigation integrity	Spoofing of satellite navigation signals	5	2
T6	Signal authenticity	Radio-frequency spoofing / signal impersonation	4	3
T7	Confidentiality	Passive eavesdropping	3	5

No single countermeasure addresses all threats. Frequency hopping, spread-spectrum transmission, robust physical-layer design, and link redundancy primarily protect link availability. Multi-constellation reception and sensor fusion address navigation attacks. Physical-layer authentication and privacy-aware message design address authenticity and confidentiality. Combined in a layered resilience framework following a perception-decision-action structure, they remain subject to the weight, energy, latency, and certifiability constraints of unmanned aerial vehicles. Among them, antenna-based spatial filtering is an attractive alternative, as it improves the signal-to-interference-plus-noise ratio without additional spectrum or waveform changes.

3 Evaluation of the Antenna-Based Countermeasure

The evaluated countermeasure is a compact circularly polarized patch antenna, used both as an individual radiator and as the building block of an array. Circular polarization reduces the polarization-mismatch losses caused by changes in the relative orientation of the drones, while the low-profile geometry facilitates integration into the aircraft platform. Arranged as an array, the elements provide the spatial degrees of freedom required to enhance reception from the intended drone and to suppress interference arriving from the jammer direction.

The element, designed for the 5 GHz DroneCAST band on a RO4003C substrate of thickness h , is shown in Fig. 1(a). Circular polarization is generated by the unequal cuts C_x and C_y introduced at opposite corners of the patch, which excite two orthogonal modes with the required phase difference around the operating frequency. Four slots are incorporated into the patch to tune the resonance and the axial ratio; for clarity, the length $L_{\text{slot}2}$, the width $W_{\text{slot}2}$, and the orientation angle α_2 are indicated only for slot 2 in Fig. 1(a), although the same parameterization applies to all four slots. The antenna is fed by a coaxial probe at $(x_{\text{feed}}, y_{\text{feed}})$ on a ground plane of dimensions $L_{\text{GND}} \times W_{\text{GND}}$.

The red region in Fig. 1 marks the range where the axial ratio remains below 3 dB, which constitutes the most restrictive antenna requirement. This circular-polarization bandwidth, centered at 5 GHz, comfortably exceeds the required 40 MHz. Within the complete shaded band the antenna also remains well matched, with $|S_{11}| < -20$ dB in Fig. 1(b), and exhibits a stable realized gain of 6.7 dB in Fig. 1(c). The element therefore satisfies the bandwidth requirement of the DroneCAST air-to-air link and is suitable for subsequent integration into the array. The optimized antenna dimensions are summarized in Table 2.

Figure 2 evaluates the proposed array in the presence of two ground-based jammers, corresponding to threat T1. The four circularly polarized patch antennas are mounted at the corners of the drone and mechanically tilted 15° downward, towards the region from which interference is expected to arrive. The two jammers are placed at the same distance from the receiver and transmit with equal power, but have different azimuth and elevation angles. As shown in Fig. 2(a), the beamforming solution preserves broad air-to-air coverage while reducing the array response in both jammer directions. The corresponding horizontal and vertical cuts in Fig. 2(b) and Fig. 2(c) confirm the formation of spatial nulls towards J1 and J2, respectively. The results demonstrate that the proposed four-element architecture can simultaneously suppress interference arriving from multiple directions.

4 Conclusion

This work rates the physical-layer threats relevant to drone-to-drone communication in Innovative Air Mobility and demonstrates antenna-based spatial processing as a countermeasure. The proposed circularly polarized patch antenna exceeds the required 40 MHz bandwidth and reduces sensitivity to changes in the relative orientation of the drones, while its compact geometry enables a four-element array. Beamforming preserves air-to-air coverage while nulling two equal-power jammers, forming one layer of the broader framework needed to address the full threat set. Future work will combine spatial filtering with robust physical-layer design and resilience of positioning, navigation, and timing.

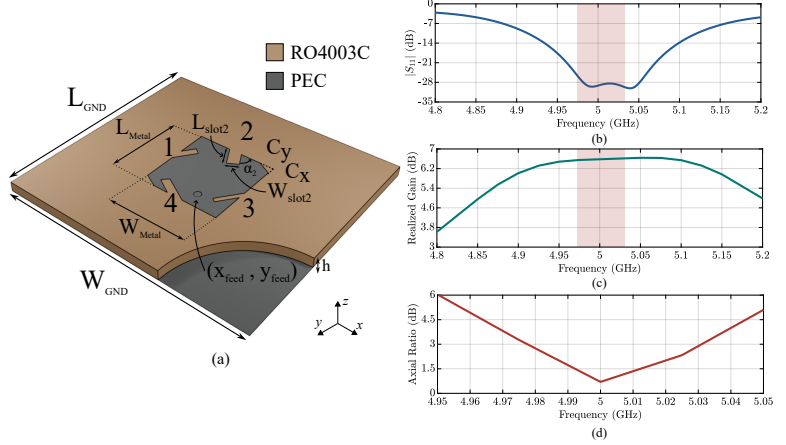


Figure 1: Circularly polarized patch antenna: (a) geometry, (b) reflection coefficient, (c) realized gain, (d) axial ratio. The red region marks the bandwidth limited by the axial-ratio requirement.

Table 2: Dimensions of the circularly polarized patch antenna. Linear dimensions in mm, angular in degrees.

Parameter	Value	Parameter	Value	Parameter	Value
L_{GND}	42.30	W_{GND}	38.44	α_{s1}	52.86
L_{metal}	13.42	W_{metal}	13.90	α_{s2}	53.76
X_{feeding}	2.87	Y_{feeding}	0.42	α_{s3}	48.98
C_x	1.19	C_y	2.27	α_{s4}	28.16
L_{slot1}	4.16	W_{slot1}	0.73	L_{slot3}	5.58
L_{slot2}	3.18	W_{slot2}	1.23	W_{slot3}	1.49
L_{slot4}	2.98	W_{slot4}	1.95		

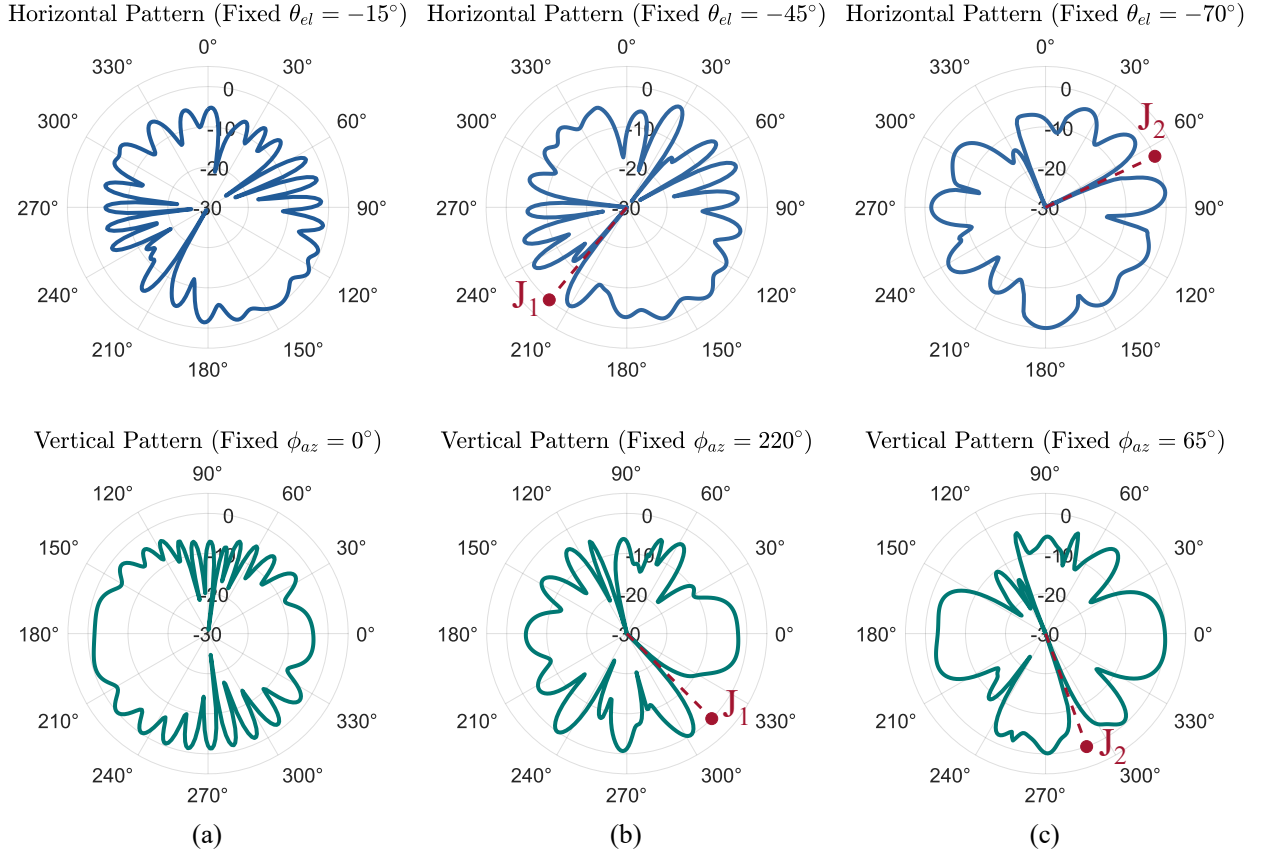


Figure 2: Array-based interference mitigation: (a) radiation pattern after beamforming, and pattern cuts through (b) jammer J1 and (c) jammer J2. The four elements are mounted at the drone corners, tilted 15° downward.