ICON Journal of Engineering Applications of Artificial Intelligence
Volume 02 | Issue 05 | 2026
e-ISSN: 3051-3820
p-ISSN: 3051-3812
Journal homepage: https://iconpublishers.com/icon-j-eng-app-ai/

Research Article **DOI: 10.5281/zenodo.20476208**

Passive RF Threat Detection and Electronic Intelligence for Low-Altitude Counter-UAS Operations Using SDR-Assisted Sensing and Transformer-Based RF Intelligence

*Abubakar Surajo Imam [1], Aliyu Musa [2], Haruna Garba Rabo [3], Muhammad Ahmad Baballe [4]
[1,3,4] Department of Mechatronic Engineering, Nigerian Defence Academy, Kaduna, Nigeria.
[2] Department of Mechanical Engineering, Nigerian Defence Academy, Kaduna, Nigeria.

Corresponding author: Abubakar Surajo Imam
Department of Mechatronic Engineering, Nigerian Defence Academy, Kaduna, Nigeria.

Received Date: 12 April 2026
Published Date: 30 May 2026

Abstract
The proliferation of low-cost unmanned aerial systems (UASs) and autonomous drone swarms has created significant challenges for conventional radar-centric surveillance systems, particularly in low-altitude and contested electromagnetic environments. This paper presents a transformer-enhanced passive radio-frequency (RF) intelligence framework for counter-UAS operations that integrates software-defined radio (SDR) sensing, RF fingerprinting, passive localisation, spectrum-anomaly detection, and distributed electronic-intelligence (ELINT) fusion within a unified architecture. Unlike conventional RF-monitoring approaches, the proposed framework combines transformer-based temporal-frequency feature extraction with cooperative RF intelligence generation to improve emitter identification, threat localisation, and swarm-behaviour analysis while maintaining low communication overhead. RF acquisition and spectrum monitoring are performed using USRP B210, HackRF One, and BladeRF platforms, while transformer-based learning models provide robust classification of drone communication signals under interference, spectrum congestion, and contested-spectrum conditions. The framework was evaluated through 100,000 Monte Carlo simulation trials, SDR-assisted experimentation, contested-spectrum emulation, RF fingerprinting assessment, and HATSABIBI-26A telemetry replay validation. Experimental results achieved a detection probability of 0.93, false-alarm probability of 0.05, classification accuracy of 0.93, localisation RMSE of 5.1 m, ELINT confidence of 0.92, and mean processing latency of 29 ms. Robustness analysis further demonstrated resilient operation under sensing-node failures, communication degradation, and spectrum congestion. The results indicate that transformer-enhanced passive RF intelligence provides a scalable, low-latency, and cost-effective capability for counter-UAS surveillance, critical-infrastructure protection, and future distributed air-defence systems.

Keywords: Counter-UAS systems; Passive RF intelligence; Software-defined radio (SDR); Transformer-based RF classification; RF fingerprinting; Passive localisation; Electronic intelligence (ELINT); Drone-swarm detection.

I. INTRODUCTION

The rapid proliferation of low-cost unmanned aerial systems (UASs) and autonomous drone swarms has significantly transformed the contemporary surveillance and air-defence landscape. Modern commercial drones increasingly possess capabilities such as autonomous navigation, beyond-line-of-sight communications, real-time video transmission, and cooperative swarm operations, creating new challenges for conventional defence architectures [15]–[19]. In particular, coordinated drone swarms can overwhelm traditional surveillance systems through distributed sensing, adaptive communication, and numerical saturation, making reliable detection, identification, and tracking of low-altitude aerial threats a critical operational requirement. Conventional radar remains the primary air-surveillance technology; however, its effectiveness is often reduced against small UASs operating at low altitude due to terrain masking, low radar cross-sections, clutter, and electromagnetic interference [1]–[3]. These limitations have stimulated interest in complementary sensing modalities capable of providing persistent surveillance with reduced electromagnetic signatures.

Passive radio-frequency (RF) sensing has emerged as a promising counter-UAS approach because it exploits emissions associated with command-and-control links, telemetry transmissions, video streams, and swarm communications without requiring active transmission [19], [22]–[29]. Recent advances in software-defined radio (SDR) platforms, including USRP B210, HackRF One, and BladeRF, have further enabled flexible RF acquisition, spectrum monitoring, protocol analysis, RF fingerprinting, and passive localisation [42]–[45]. In parallel, transformer-based deep-learning architectures have demonstrated superior capability for modelling complex temporal-frequency relationships within RF spectrograms, improving classification accuracy and robustness compared with conventional machine-learning approaches [30]–[35]. Combined with advances in edge computing and distributed AI, these techniques support real-time RF intelligence generation in contested operational environments [38]–[41].

Despite these developments, most existing counter-UAS systems treat RF sensing, classification, localisation, and intelligence fusion as independent functions. This paper addresses this gap by presenting a unified passive RF threat-detection and electronic-intelligence (ELINT) framework integrating SDR-assisted sensing, transformer-based RF feature extraction, RF fingerprinting, passive localisation, spectrum anomaly detection, and distributed ELINT fusion. The proposed architecture is intended to provide scalable, resilient, and low-latency surveillance capability for low-altitude UASs and autonomous drone swarms operating in contested electromagnetic environments. The major contributions of this paper are summarised as follows:

- Development of a distributed passive RF intelligence architecture for low-altitude counter-UAS operations.
- Integration of SDR-assisted sensing using USRP B210, HackRF One, and BladeRF platforms.
- Development of transformer-based RF feature extraction and RF classification methodologies.
- Formulation of passive RF localisation and distributed ELINT fusion mechanisms.
- Development of spectrum anomaly-detection and swarm RF behaviour-analysis capabilities.
- Experimental validation using SDR-assisted sensing, contested-spectrum emulation, and HATSABIBI-26A telemetry replay.

The remainder of this paper is organised as follows. Section 2 presents the overall system architecture. Section 3 describes passive RF sensing and SDR-assisted acquisition. Section 4 develops the transformer-based RF feature extraction framework. Section 5 presents RF fingerprinting and emitter identification. Section 6 develops passive RF localisation and ELINT coordination. Section 7 models contested electromagnetic environments. Sections 8–10 present simulation, experimental validation, and robustness analysis. Finally, Sections 11–13 discuss operational implications, limitations, conclusions, and future research directions.

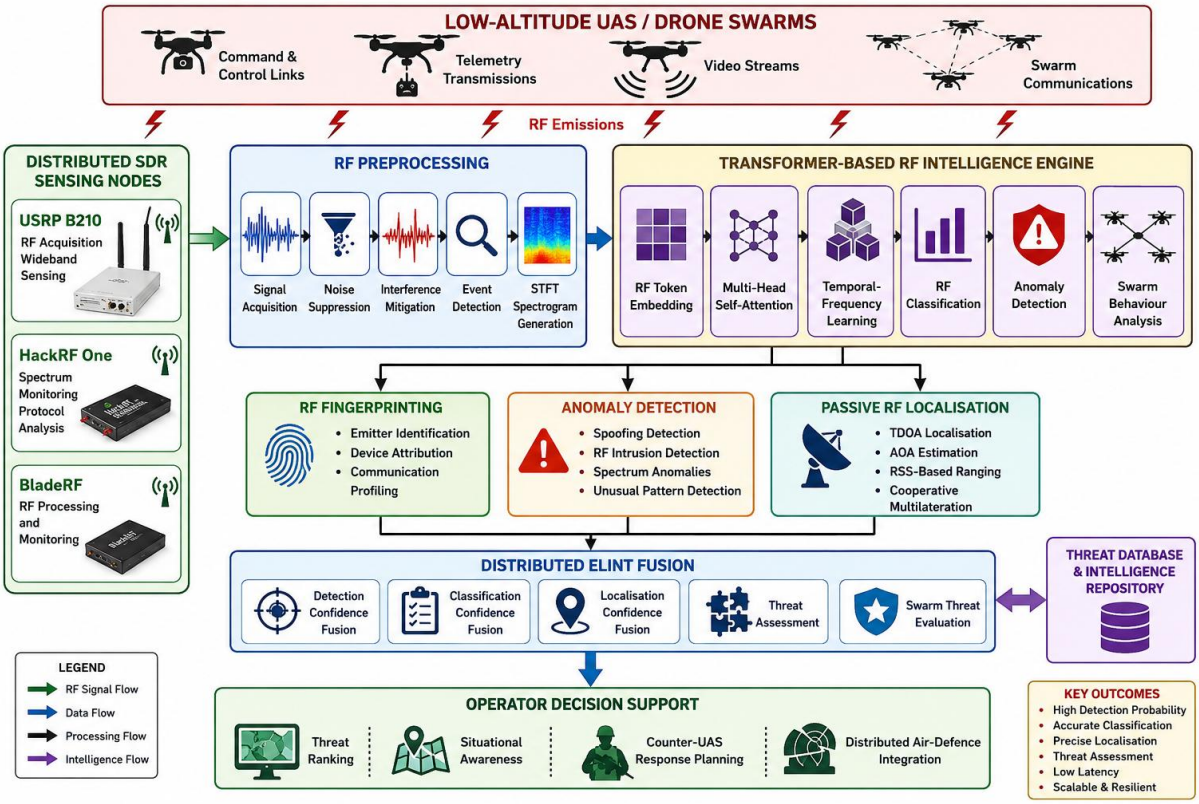

Fig. 1: Overall passive RF intelligence architecture showing SDR sensing nodes, RF preprocessing, transformer-based RF feature extraction, RF fingerprint classification, passive localisation, and ELINT coordination.

2. System Architecture Overview

The proposed passive RF intelligence architecture provides scalable, resilient, and low-latency surveillance capability for detecting, identifying, localising, and tracking low-altitude Unmanned Aerial Systems (UASs), autonomous drone swarms, and RF-enabled aerial threats. The framework integrates SDR-assisted sensing, transformer-based RF intelligence, RF fingerprinting, passive localisation, and Electronic Intelligence (ELINT) fusion within a unified distributed architecture. By leveraging distributed sensing, RF intelligence analytics, multisensor fusion, and cooperative tracking principles, the system improves detection persistence, localisation accuracy, spectrum awareness, and operational robustness in contested electromagnetic environments [4]–[8], [62]–[64].

Unlike conventional centralised RF-monitoring architectures that depend on a single observation point, the proposed framework employs geographically distributed sensing nodes that cooperate through the exchange of validated intelligence cues rather than raw RF observations. This significantly reduces communication overhead while improving resilience against node failures, spectrum congestion, and electronic attacks. The architecture comprises six principal functional layers, namely distributed RF sensing layer, RF preprocessing layer, transformer-based RF intelligence layer, RF fingerprinting layer, passive RF localisation layer, and ELINT fusion and decision-support layer.

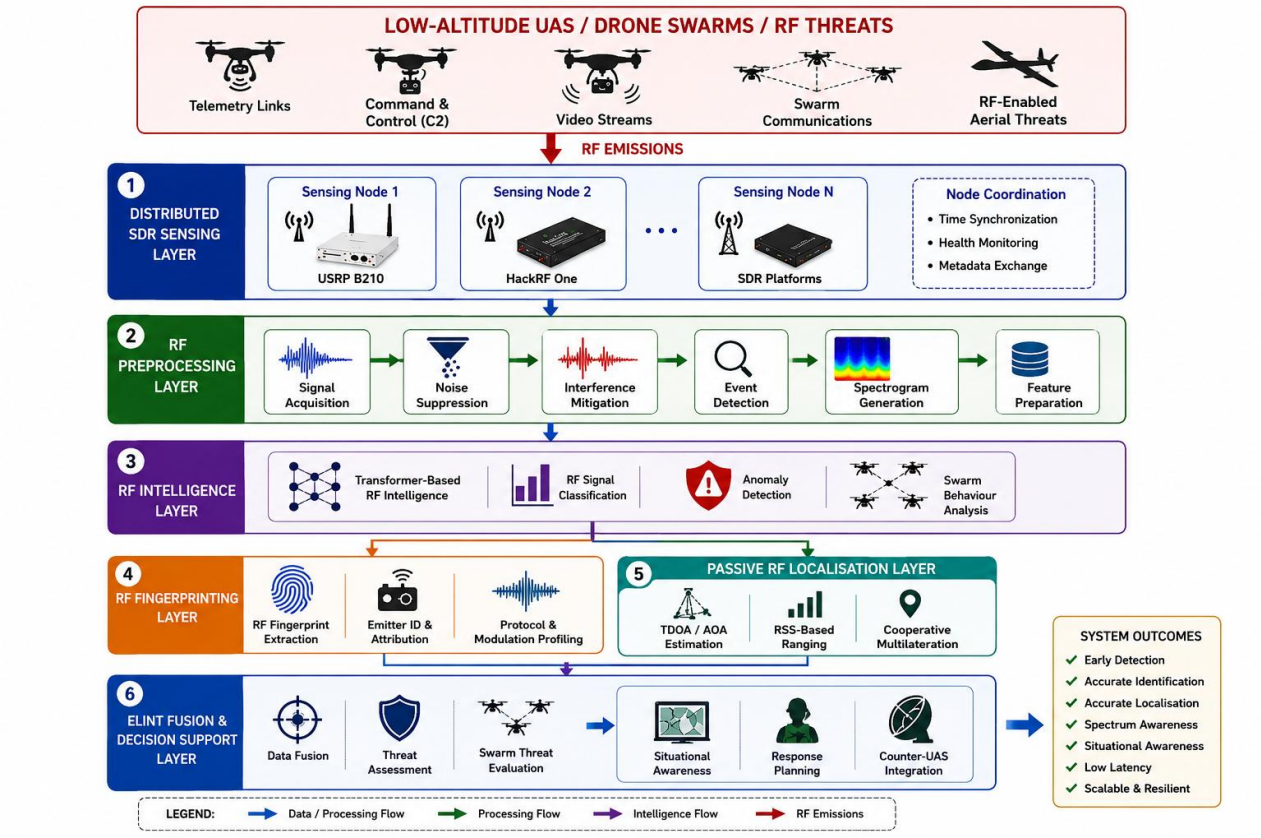

Fig. 2: Overall passive RF intelligence architecture showing distributed SDR sensing nodes, RF preprocessing, transformer-based intelligence extraction, RF fingerprinting, passive localisation, ELINT fusion, and operator decision support.

2.1 Distributed RF Sensing

The distributed RF sensing layer provides the first stage of threat detection and spectrum awareness. Multiple sensing nodes equipped with Software Defined Radios (SDRs), including USRP B210, HackRF One, and BladeRF platforms, continuously monitor designated frequency bands for drone-related communications, telemetry transmissions, video downlinks, and swarm-coordination signals. The distributed sensing topology is represented using a graph-theoretic communication model:

$$G = (V, E) \qquad (1)$$

where: V denotes the set of sensing nodes and E denotes communication links between neighbouring nodes.

Equation (1) models the sensing network as a distributed graph in which sensing nodes exchange validated RF cues and intelligence products. The sensing-node density is defined as:

$$\rho_s = \frac{N_s}{A} \quad (2)$$

where: N_s denotes the number of sensing nodes and A denotes the surveillance area.

Higher sensing-node density improves RF coverage continuity, passive-localisation accuracy, and detection persistence by reducing coverage gaps and increasing observation redundancy [63], [64]. The cumulative detection probability across the sensing network can be expressed as:

$$P_D^{(net)} = 1 - \prod_{i=1}^{N_s}(1 - P_i) \quad (3)$$

where P_i represents the local detection probability of sensing node i. This relationship demonstrates the benefits of cooperative sensing in improving network-level surveillance performance.

2.2 RF Preprocessing

The RF preprocessing layer performs signal acquisition, filtering, channelisation, noise suppression, interference mitigation, and spectrogram generation. These operations prepare the RF observations for transformer-based intelligence extraction. The received signal at sensing node $i$is modelled as:

$$r_i(t) = s_i(t) + n_i(t) + j_i(t) \quad (4)$$

where: $s_i(t)$ denotes the RF signal of interest, $n_i(t)$denotes environmental noise. $j_i(t)$ denotes interference and jamming signals. The average received signal power estimate is calculated as:

$$\hat{P}_i = \frac{1}{N}\sum_{n=1}^{N} | x_i[n] |^2 \quad (5)$$

where: $x_i[n]$ denotes the acquired I/Q samples. Ndenotes the number of samples.
An RF event is declared when:

$$\hat{P}_i > \tau_E \quad (6)$$

where: τ_E denotes the detection threshold. Signals satisfying Equation (6) are forwarded for feature extraction and intelligence analysis. To quantify received-signal quality, the Signal-to-Interference-plus-Noise Ratio (SINR) is expressed as:

$$SINR = \frac{P_s}{P_n + P_j} \quad (7)$$

where: P_s denotes signal power, P_n denotes noise power and P_j denotes interference power. Higher SINR values generally improve classification accuracy and emitter-identification performance.

2.3 Transformer-Based RF Intelligence

The transformer-based RF intelligence layer processes RF spectrograms to extract temporal and spectral patterns associated with drone communications, frequency hopping, burst transmissions, and swarm behaviour [30]–[35]. The embedded RF feature representation is expressed as:

$$F_{RF} \in \mathbb{R}^{N \times d} \quad (8)$$

where: N denotes RF tokens and d denotes embedding dimensionality. The transformer self-attention mechanism is represented as:

$$Attention(Q, K, V) = Softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (9)$$

where: Q, K, and V denote query, key and value matrices and d_k denotes key-vector dimensionality. The transformer output representation becomes:

$$F_T = Transformer(F_{RF}) \qquad (10)$$

This feature representation captures long-range communication dependencies and RF behavioural patterns that may not be observable using conventional CNN- or LSTM-based approaches. Threat-classification confidence is subsequently obtained through:

$$C_{RF} = Softmax(F_T W_C + b_C) \qquad (11)$$

where: W_C denotes classifier weights and b_C denotes classifier bias.

2.4 RF Fingerprinting and Passive Localisation

RF fingerprinting exploits hardware-dependent transmitter characteristics for emitter identification. Since manufacturing imperfections produce unique RF signatures, individual drone transmitters can often be identified even when communication payloads are encrypted. Each emitter fingerprint is represented as:

$$\Gamma_i = [\mu_f, \sigma_f, \Delta f, \rho_m, B_w] \qquad (12)$$

where: μ_f denotes mean carrier frequency, $\sigma_f$denotes frequency variance, Δfdenotes frequency drift, ρ_m denotes modulation characteristics and B_w denotes occupied bandwidth. The posterior probability of emitter class $C_i$is given by:

$$P(C_i \mid \Gamma) = \frac{P(\Gamma \mid C_i)P(C_i)}{\sum_{j=1}^{M} P(\Gamma \mid C_j)P(C_j)} \qquad (13)$$

where Mdenotes the number of known emitter classes. Emitter localisation is performed using Time Difference of Arrival (TDOA), Angle of Arrival (AOA), Received Signal Strength (RSS), and cooperative multilateration algorithms. The emitter position vector is expressed as:

$$p = [x, y, z]^T \qquad (14)$$

The estimated emitter location is obtained through:

$$\hat{p} = \arg\min_{p} \sum_{i=1}^{N} (d_i - \hat{d}_i)^2 \qquad (15)$$

where: d_i denotes actual range measurements and $\hat{d}_i$denotes estimated ranges. This optimisation minimises localisation error and improves geolocation accuracy.

2.5 ELINT Fusion and Edge Processing

The ELINT fusion layer integrates sensing, classification, localisation, and anomaly-analysis outputs to generate a unified threat picture for operators and command systems. The overall ELINT confidence score is defined as:

$$C_E = \alpha P_D + \beta C_{RF} + \gamma C_L + \delta C_Q \qquad (16)$$

subject to:

$$\alpha + \beta + \gamma + \delta = 1 \qquad (17)$$

where: P_D denotes detection confidence, C_{RF} denotes RF-classification confidence, C_L denotes localisation confidence and C_Q denotes cue-quality confidence. Threat prioritisation is subsequently performed using:

$$R_i = \alpha T_i + \beta L_i + \gamma A_i \qquad (18)$$

where: T_i denotes threat confidence, L_i denotes localisation confidence and A_i denotes anomaly confidence. The resulting threat-ranking metric supports prioritised operator responses and counter-UAS decision making.

To minimise communication bandwidth consumption, sensing nodes transmit validated intelligence cues rather than raw RF observations. The communication-reduction factor is defined as:

$$B_r = \frac{N_{cue}}{N_{raw}} \tag{19}$$

where: N_{cue} denotes transmitted intelligence cues, N_{raw} denotes raw RF observations. Lower values of $B_r$indicate improved communication efficiency and reduced network congestion [38]–[41].

The proposed architecture establishes the foundation for distributed passive RF intelligence by integrating SDR-assisted sensing, RF preprocessing, transformer-based RF intelligence extraction, RF fingerprinting, passive localisation, and ELINT fusion within a unified operational framework. Through distributed cue sharing, cooperative localisation, and transformer-driven RF analytics, the architecture provides robust detection, identification, localisation, and tracking of low-altitude UASs and autonomous drone swarms operating in contested electromagnetic environments. The subsequent sections describe the passive RF sensing subsystem, transformer-based RF intelligence extraction mechanisms, RF fingerprinting methodologies, passive localisation algorithms, and experimental validation framework in greater detail.

3. Passive RF Sensing and SDR-Assisted Acquisition

Passive RF sensing forms the foundation of the proposed electronic-intelligence architecture. Unlike conventional radar systems that actively transmit electromagnetic energy, passive RF sensing exploits naturally occurring RF emissions generated by UASs, telemetry links, video downlinks, ground-control stations, and swarm communication networks [19], [22]–[29]. This approach provides covert surveillance capability, reduced electromagnetic observability, lower deployment cost, and improved survivability in contested environments. The sensing architecture integrates RF spectrum monitoring, signal acquisition, event detection, spectral feature extraction, RF cue generation, and communication-behaviour analysis.

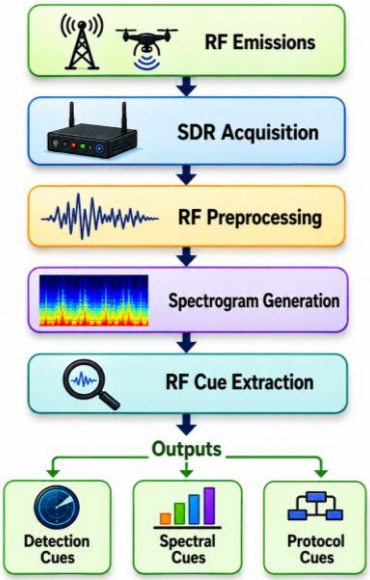

Fig. 3: SDR-assisted passive RF sensing workflow showing RF acquisition, preprocessing, event detection, spectrogram generation, and cue extraction.

3.1 SDR Hardware Architecture

The sensing subsystem employs a heterogeneous SDR network comprising the USRP B210 for RF intelligence and passive localisation, HackRF One for spectrum monitoring and reconnaissance, and BladeRF for FPGA-assisted RF processing and protocol analysis. The key hardware characteristics and operational roles of the selected SDR platforms are summarised in Table 2. The combination of these complementary platforms provides broad frequency coverage, flexible signal-processing capability, and support for distributed RF surveillance operations.

Table 2: SDR Hardware Configuration

Platform	Frequency Coverage	Primary Function
Platform	Frequency Coverage	Primary Function
USRP B210	70 MHz–6 GHz	RF intelligence and localisation
HackRF One	1 MHz–6 GHz	Spectrum monitoring
BladeRF	47 MHz–6 GHz	FPGA-assisted RF processing

The distributed architecture improves coverage continuity, localisation accuracy and sensing redundancy.

3.2 RF Signal Acquisition and Detection

The received RF signal at sensing node i is represented as:

$$r_i(t) = s_i(t) + n_i(t) + j_i(t) \qquad (15)$$

where $s_i(t)$, $n_i(t)$ and $j_i(t)$ denote the signal of interest, noise, and interference respectively. The acquired I/Q samples are expressed as:

$$x_i[n] = I_i[n] + jQ_i[n] \qquad (16)$$

The average received power estimate becomes:

$$\hat{P}_i = \frac{1}{N}\sum_{n=1}^{N} | x_i[n] |^2 \qquad (17)$$

An RF event is declared when:

$$E_i = \sum_{n=1}^{N} | x_i[n] |^2 > \tau_E \qquad (18)$$

The corresponding detection and false-alarm probabilities are:

$$P_D = P(E_i > \tau_E \mid H_1) \qquad (19)$$

$$P_{FA} = P(E_i > \tau_E \mid H_0) \qquad (20)$$

3.3 Spectrum Monitoring and Spectrogram Generation

Spectrum occupancy is defined as:

$$O_f = \frac{B_{used}}{B_{total}} \qquad (21)$$

while spectrum utilisation is given by:

$$U_f = \frac{T_{active}}{T_{obs}} \qquad (22)$$

To enable transformer-based analysis, RF signals are transformed into time-frequency representations using the Short-Time Fourier Transform (STFT):

$$X(\tau, f) = \int x(t) w(t-\tau) e^{-j2\pi f t} dt \qquad (23)$$

The resulting spectrogram becomes:

$$S(\tau, f) = | X(\tau, f) |^2 \qquad (24)$$

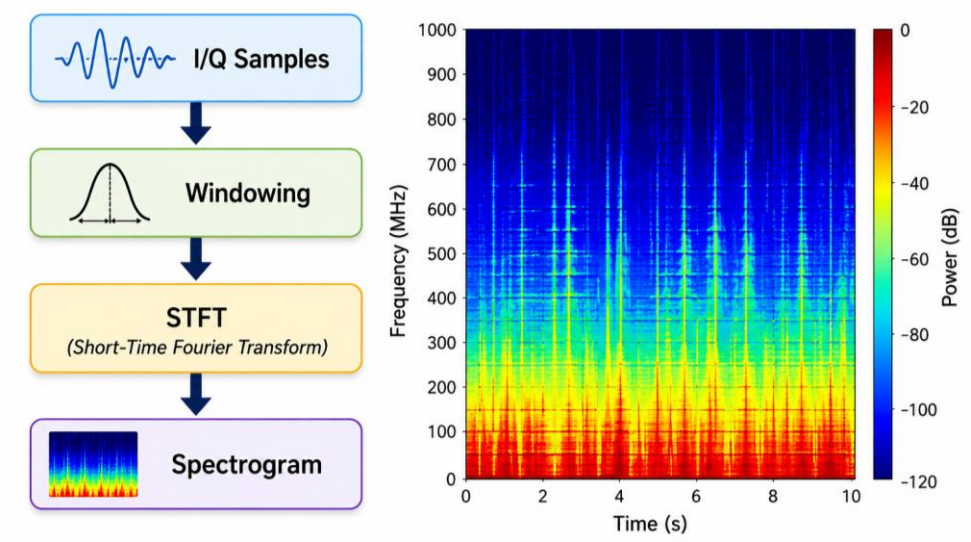

Fig. 4: RF spectrogram generation process showing I/Q acquisition, STFT processing and time-frequency representation.

3.4 RF Cue Generation

Following detection, candidate RF cues are generated as:

$$C_i = \{f_c, B_w, P_r, T_b\} \qquad (25)$$

where f_c, B_w, P_r, and T_b denote carrier frequency, bandwidth, received power, and burst duration respectively. The cue-confidence score is expressed as:

$$C_D = \alpha P_D + \beta U_f + \gamma S_q \qquad (26)$$

subject to:

$$\alpha + \beta + \gamma = 1 \qquad (27)$$

where S_q denotes signal quality.

3.5 Distributed Cooperative RF Sensing

Neighbouring sensing nodes exchange validated RF cues rather than raw RF samples, significantly reducing communication overhead while improving surveillance persistence. The distributed detection probability is:

$$P_D^{(N)} = 1 - \prod_{i=1}^{N}(1 - P_i) \qquad (28)$$

The communication-reduction factor becomes:

$$B_r = \frac{N_{cue}}{N_{raw}} \qquad (29)$$

where $N_{cue}$and N_{raw} denote transmitted cues and raw RF observations respectively.

3.6 Software Environment

The implementation environment integrates GNU Radio, SDR++, GQRX, Universal Radio Hacker (URH), Python, NumPy, SciPy, PyTorch, and TensorFlow. These tools collectively support SDR acquisition, spectrum monitoring, protocol analysis, spectrogram generation, transformer-based RF intelligence and distributed ELINT coordination.

The passive RF sensing subsystem provides the primary sensing capability of the proposed architecture through SDR-assisted acquisition, energy-based detection, spectrum monitoring, spectrogram generation, cue extraction and distributed cooperative sensing. The generated RF cues and time-frequency representations form the inputs to the transformer-based RF intelligence and RF fingerprinting modules discussed in the next section.

4. Transformer-Based RF Feature Extraction

Following RF acquisition and preprocessing, the extracted RF signals are transformed into time-frequency representations and analysed using a transformer-based RF intelligence framework. Transformer architectures employ self-attention mechanisms to learn long-range temporal-frequency dependencies and have demonstrated superior performance in RF signal classification, spectrum intelligence, communication analysis, and emitter identification compared with conventional convolutional and recurrent neural-network architectures [30]–[35]. The proposed framework utilises transformer-based feature extraction for RF emitter classification, communication-pattern recognition, spectrum anomaly detection, swarm-behaviour analysis, and electronic-intelligence generation.

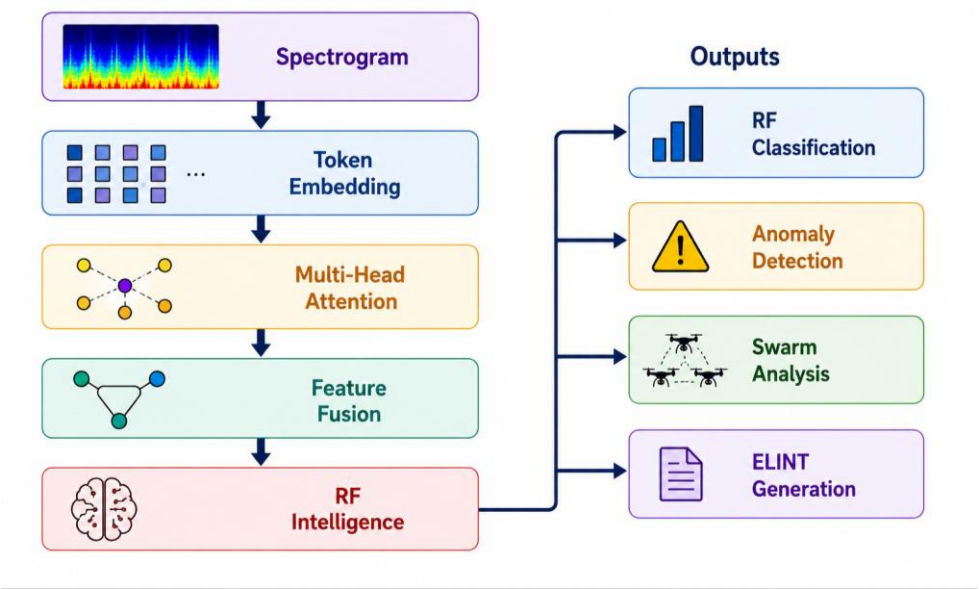

Fig. 5: Transformer-based RF intelligence architecture showing spectrogram generation, token embedding, self-attention processing, feature fusion, and RF classification.

4.1 RF Spectrogram Representation and Embedding

The SDR-acquired RF signals are converted into time-frequency representations using the Short-Time Fourier Transform (STFT) [14]:

$$X(\tau, f) = \int_{-\infty}^{+\infty} x(t) w(t-\tau)\, e^{-j2\pi f t} dt \qquad (21)$$

where $x(t)$ denotes the RF signal, $w(t)$is the analysis window, τrepresents time, and $f$denotes frequency. The corresponding spectrogram is represented as:

$$S(\tau, f) = | X(\tau, f) |^2 \qquad (22)$$

The spectrogram is subsequently embedded into a high-dimensional feature space:

$$F_{RF} = \phi(S) \qquad (23)$$

where $\phi(\cdot)$ denotes the embedding operation.The resulting token matrix becomes:

$$F_{RF} \in \mathbb{R}^{N \times d} \qquad (24)$$

where N denotes the number of RF tokens and d represents embedding dimensionality. To preserve temporal-frequency relationships, positional embeddings are incorporated:

$$E = F_{RF} + P \qquad (25)$$

where P denotes positional encoding vectors.

4.2 Multi-Head Self-Attention and Feature Fusion

The transformer encoder employs self-attention to model global dependencies across RF spectrograms [30], [31]. Query, key, and value matrices are computed as:

$$Q = EW_Q \quad (26)$$
$$K = EW_K \quad (27)$$
$$V = EW_V \quad (28)$$

where W_Q, W_K and W_V are trainable projection matrices. The scaled dot-product attention mechanism becomes:

$$Attention(Q, K, V) = Softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (29)$$

where d_k denotes key-vector dimensionality. The multi-head attention operation is expressed as:

$$MHA = Concat(H_1, H_2, \dots, H_h)W_O \quad (30)$$

where H_i denotes attention head i, $h$is the number of attention heads, and $W_O$denotes output projection weights. The transformer encoder subsequently generates a unified RF representation:

$$F_{fused} = Transformer(E) \quad (31)$$

which captures spectral behaviour, temporal evolution, protocol structures, modulation characteristics, and communication dynamics.

4.3 RF Classification and Anomaly Detection

The posterior probability of emitter class C_i is estimated as:

$$P(C_i \mid F_{fused}) = \frac{P(F_{fused} \mid C_i)P(C_i)}{\sum_{j=1}^{M} P(F_{fused} \mid C_j)P(C_j)} \quad (32)$$

The predicted emitter class becomes:

$$\hat{C} = \arg\max_i P(C_i \mid F_{fused}) \quad (33)$$

while the corresponding classification confidence is:

$$C_{RF} = \max_i P(C_i \mid F_{fused}) \quad (34)$$

subject to:

$$0 \leq C_{RF} \leq 1 \quad (35)$$

Transformer feature representations are also exploited for anomaly detection. The anomaly score is defined as:

$$A_t = \frac{\| F_{obs} - F_{exp} \|}{\sigma_t} \quad (36)$$

where F_{obs} and F_{exp} denote observed and expected RF features, respectively. An anomaly is declared when:

$$A_t > \tau_A \quad (37)$$

where τ_A denotes the anomaly threshold. The anomaly confidence score becomes:

$$C_A = 1 - e^{-A_t} \quad (38)$$

Detected anomalies may indicate drone activity, swarm communications, RF spoofing, protocol switching, or interference events.

4.4 Swarm Communication Analysis

Autonomous drone swarms frequently exhibit correlated communication behaviour that differs significantly from individual drone transmissions [22]–[25]. The swarm communication correlation metric is expressed as:

$$S_R = \frac{1}{N}\sum_{i=1}^{N} \rho_i \qquad (39)$$

where ρ_i denotes communication correlation. The corresponding swarm-confidence estimate becomes:

$$C_{swarm} = P(S \mid F_{fused}) \qquad (40)$$

where S denotes swarm behaviour. High values of C_{swarm}indicate coordinated communication activity consistent with autonomous swarm operations.

4.5 Computational Complexity

The approximate transformer computational workload is:

$$F_{TF} = 2N^2 d + 4Nd^2 \qquad (41)$$

while the corresponding memory requirement becomes:

$$M_{TF} = 4Nd + 4N^2 \qquad (42)$$

The inference throughput is represented as:

$$R_{inf} = \frac{N_{proc}}{T_{inf}} \qquad (43)$$

where N_{proc} denotes processed samples and T_{inf} denotes inference time. The overall processing latency becomes:

$$T_{total} = T_{STFT} + T_{embed} + T_{attn} + T_{class} \qquad (44)$$

where T_{STFT}, T_{embed}, T_{attn}, and T_{class} denote spectrogram-generation, embedding, attention-processing, and classification latencies, respectively. These metrics provide useful indicators for evaluating real-time deployment feasibility on embedded GPU and edge-computing platforms [38]–[41].

Table 3: Transformer RF Processing Parameters

Parameter	Description
N	Number of RF tokens
d	Embedding dimension
d_k	Key-vector dimension
F_{fused}	Transformer-fused RF feature vector
C_{RF}	RF classification confidence
A_t	Anomaly score
C_A	Anomaly confidence
C_{swarm}	Swarm-confidence estimate
F_{TF}	Computational workload
M_{TF}	Memory requirement

The transformer-based RF intelligence subsystem converts raw RF observations into actionable intelligence products through feature extraction, classification, anomaly detection, and swarm-behaviour analysis. As indicated in Table 4, the framework integrates both operational intelligence metrics and computational-performance parameters required for real-time deployment assessment. These outputs provide the foundation for RF fingerprinting, passive localisation, and ELINT fusion discussed in the subsequent section.

5. RF Fingerprinting and Emitter Identification

Following transformer-based RF feature extraction, the proposed architecture performs RF fingerprinting and emitter identification to determine the source of detected RF emissions. Unlike protocol-based classification approaches, RF fingerprinting exploits hardware-dependent characteristics embedded within RF signals and remains effective even when communications are encrypted [22]–[25]. This capability supports drone-platform identification, ground-control-station attribution, swarm-member classification, RF emitter tracking, and electronic-intelligence generation.

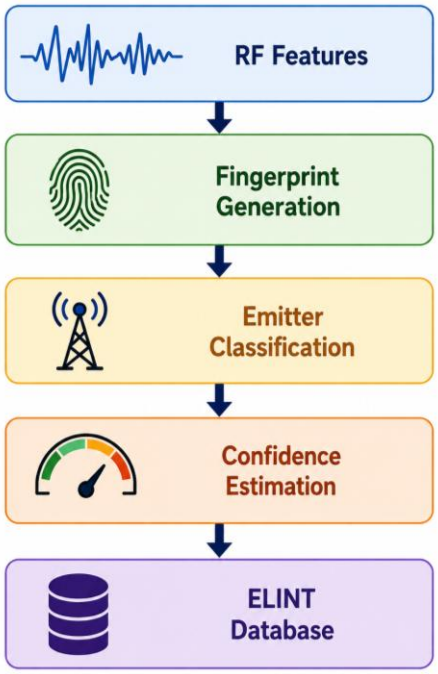

Fig. 6: RF fingerprinting and emitter-identification architecture showing fingerprint generation, classification, confidence estimation, and ELINT integration.

5.1 RF Fingerprint Representation

Each RF emitter exhibits unique characteristics arising from oscillator instabilities, modulation imperfections, transient behaviour, and spectral artefacts. The RF fingerprint vector is represented as:

$$\Gamma_i = [\mu_f, \sigma_f, \Delta f, \rho_m, T_b, B_w, S_p] \qquad (45)$$

where μ_f, σ_f, Δf, ρ_m, T_b, B_w, and S_p denote carrier-frequency, modulation, burst-duration, bandwidth, and spectral features. The fingerprint database becomes:

$$\mathcal{F} = \{\Gamma_1, \Gamma_2, \ldots, \Gamma_M\} \qquad (46)$$

where M denotes the number of known emitter classes.

5.2 Frequency and Modulation Features

Frequency stability provides one of the most discriminative RF fingerprinting features. The instantaneous frequency drift is expressed as:

$$\Delta f = f_{obs} - f_{nom} \qquad (47)$$

where f_{obs} and f_{nom} denote observed and nominal carrier frequencies. The corresponding frequency-stability metric becomes:

$$S_f = \frac{1}{N}\sum_{i=1}^{N}(\Delta f_i)^2 \qquad (48)$$

Modulation-related features are represented as:

$$M_f = [A_m, \phi_m, R_s, B_w] \qquad (49)$$

where A_m, ϕ_m, R_s and B_w denote amplitude, phase, symbol-rate, and bandwidth characteristics.

The modulation similarity between emitters is computed as:

$$S_m = \frac{M_i \cdot M_j}{\| M_i \| \| M_j \|} \qquad (50)$$

Higher values indicate stronger similarity between emitter signatures.

5.3 Transformer-Assisted Classification

The extracted fingerprint features are classified using the transformer-generated feature representation from Section 4. The posterior probability of emitter class C_i becomes:

$$P(C_i \mid \Gamma_i) = \frac{P(\Gamma_i \mid C_i)P(C_i)}{\sum_j P(\Gamma_i \mid C_j)P(C_j)} \qquad (51)$$

The identified emitter class is:

$$\hat{C} = \arg\max_i P(C_i \mid \Gamma_i) \qquad (52)$$

while the corresponding classification confidence becomes:

$$C_{RF} = \max_i P(C_i \mid \Gamma_i) \qquad (53)$$

subject to:

$$0 \leq C_{RF} \leq 1 \qquad (54)$$

The transformer architecture improves classification accuracy by learning complex relationships among spectral, temporal, and modulation features [30]–[35].

5.4 Emitter Identification Performance

Emitter-identification performance is evaluated using standard classification metrics. Identification accuracy is defined as:

$$Acc = \frac{N_{correct}}{N_{total}} \qquad (55)$$

Precision, recall, and F1-score are expressed as:

$$Precision = \frac{TP}{TP + FP} \qquad (56)$$

$$Recall = \frac{TP}{TP + FN} \qquad (57)$$

$$F_1 = \frac{2PR}{P + R} \qquad (58)$$

where TP, FP, and FN denote true positives, false positives, and false negatives, respectively.

5.5 Swarm RF Behaviour and Intelligence Generation

Autonomous drone swarms frequently exhibit synchronised transmissions, coordinated burst activity, shared communication channels, and correlated telemetry exchanges. These characteristics can be exploited to estimate swarm activity, identify coordinated behaviours, and support threat assessment [22]–[25]. The final RF intelligence output comprises emitter identity, classification confidence, communication characteristics, swarm indicators, and localisation-

support information. The principal RF fingerprinting and classification parameters utilised by the proposed framework are summarised in Table 4.

Table 4: RF Fingerprint Parameters

Parameter	Description
μ_f	Mean carrier frequency
σ_f	Frequency variance
Δf	Frequency drift
ρ_m	Modulation characteristics
T_b	Burst duration
B_w	Occupied bandwidth
S_p	Spectral peak characteristics
C_{RF}	Classification confidence
Acc	Identification accuracy
F_1	F1-score

6. Passive RF Localisation and ELINT Coordination

Following RF detection and emitter identification, the proposed architecture performs passive RF localisation to estimate the positions of drone transmitters, ground-control stations, relay nodes, and swarm communication sources. Unlike radar-based tracking systems, passive RF localisation exploits naturally occurring emissions associated with command-and-control links, telemetry transmissions, video streams, and swarm communications while maintaining a low probability of detection [26]–[29]. The localisation subsystem integrates Time Difference of Arrival (TDOA), Angle of Arrival (AOA), Received Signal Strength (RSS), cooperative multilateration, and ELINT confidence fusion.

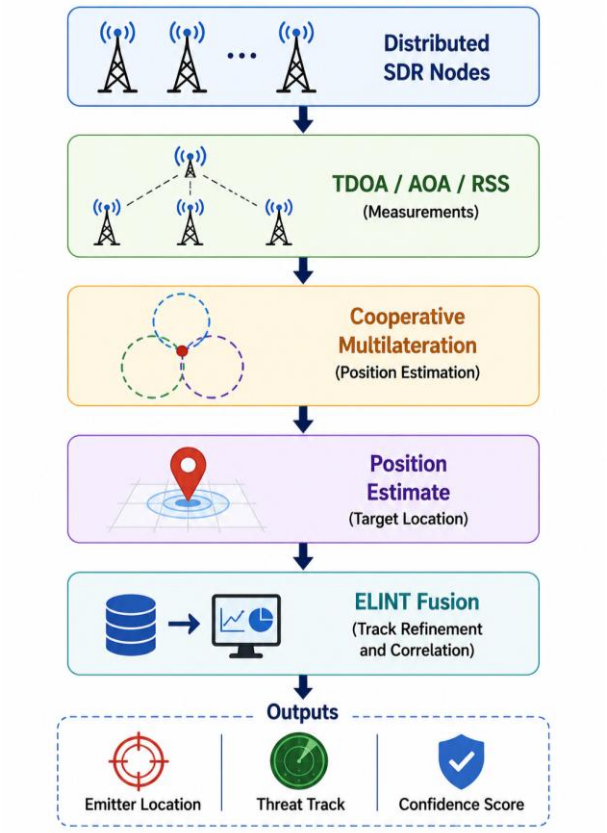

Fig. 7: Passive RF localisation and ELINT coordination architecture showing distributed SDR sensing nodes, TDOA/AOA estimation, cooperative multilateration, threat tracking, and ELINT fusion.

6.1 Passive RF Localisation Framework

The emitter position is represented as:

$$\mathbf{p} = [x, y, z]^T \qquad (59)$$

while the position of sensing node $i$becomes:

$$\mathbf{S}_i = [x_i, y_i, z_i]^T \qquad (60)$$

The Euclidean distance between the emitter and sensing node is:

$$d_i = \sqrt{(x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2} \qquad (61)$$

The localisation objective is formulated as:

$$\hat{\mathbf{p}} = \arg \min_{\mathbf{p}} \sum_{i=1}^{N} (d_i - \hat{d}_i)^2 \qquad (62)$$

where d_i and $\hat{d}_i$ denote true and estimated distances, respectively.

6.2 TDOA and AOA Localisation

TDOA localisation exploits differences in signal arrival times at multiple sensing nodes. The arrival-time difference between sensing nodes $i$and $j$becomes:

$$\Delta t_{ij} = t_i - t_j \qquad (63)$$

The corresponding range difference is:

$$\Delta d_{ij} = c\Delta t_{ij} \qquad (64)$$

where $c$denotes the speed of electromagnetic propagation. Each TDOA measurement generates a hyperbolic localisation constraint:

$$d_i - d_j = \Delta d_{ij} \qquad (65)$$

AOA localisation estimates the direction toward the emitter:

$$\theta_i = \tan^{-1}\left(\frac{y - y_i}{x - x_i}\right) \qquad (66)$$

The combination of TDOA and AOA measurements significantly improves localisation accuracy and robustness [26], [27].

6.3 RSS Localisation and Cooperative Fusion

RSS localisation exploits received signal power variations to estimate emitter range. The logarithmic path-loss model becomes:

$$PL(d) = PL_0 + 10n\log_{10}\left(\frac{d}{d_0}\right) \qquad (67)$$

where PL_0 denotes reference path loss, $n$is the path-loss exponent, and d_0 is the reference distance.

The estimated range becomes:

$$\hat{d} = d_0 10^{\frac{PL(d) - PL_0}{10n}} \qquad (68)$$

To improve localisation robustness, TDOA, AOA and RSS measurements are fused through cooperative multilateration:

$$\hat{d}_f = w_1\hat{d}_{TDOA} + w_2\hat{d}_{AOA} + w_3\hat{d}_{RSS} \qquad (69)$$

subject to:

$$w_1 + w_2 + w_3 = 1 \qquad (70)$$

where w_1, w_2 and w_3 denote weighting coefficients.

6.4 Threat Tracking and ELINT Fusion

Following localisation, emitter positions are continuously updated to generate threat tracks. The target-state vector is represented as:

$$x_k = [x, y, z, v_x, v_y, v_z]^T \qquad (71)$$

where v_x, v_y and v_z denote velocity components. The overall ELINT confidence score becomes:

$$C_{ELINT} = \alpha P_D + \beta C_{RF} + \gamma C_L + \delta C_Q \qquad (72)$$

subject to:

$$\alpha + \beta + \gamma + \delta = 1 \qquad (73)$$

where P_D, C_{RF}, C_L and C_Q denote detection, classification, localisation, and communication-quality confidence measures, respectively. The corresponding threat-confidence estimate is:

$$T_C = f(C_{ELINT}, A_t, P_D) \qquad (74)$$

where A_t denotes anomaly confidence.

6.5 Localisation Performance Metrics

The localisation Root Mean Square Error (RMSE) is defined as:

$$RMSE = \sqrt{\frac{1}{N}\sum_{k=1}^{N} \| x_k - \hat{x}_k \|^2} \qquad (75)$$

where x_k and $\hat{x}_k$ denote the true and estimated emitter positions, respectively. The RMSE, localisation success probability, and localisation latency are used to evaluate localisation performance. The principal localisation and ELINT-fusion parameters are summarised in Table 5.

Table 5: Passive RF Localisation Parameters

Parameter	Description
$\mathbf{p}$	Emitter position
d_i	Distance estimate
Δt_{ij}	TDOA measurement
θ_i	AOA estimate
$\hat{d}$	Estimated range
x_k	Target-state vector
C_L	Localisation confidence
C_{ELINT}	ELINT confidence
T_C	Threat confidence
$RMSE$	Localisation error

The passive RF localisation and ELINT coordination subsystem combines emitter identification, localisation estimates, swarm indicators, anomaly detections, and communication assessments to generate actionable intelligence for counter-UAS operations.

7. Contested Electromagnetic Environment Modelling

Modern counter-UAS operations increasingly occur within contested electromagnetic environments characterised by RF interference, spectrum congestion, communication degradation, jamming, spoofing attacks, multipath propagation, and adversarial electronic-warfare activities [9]–[14], [17], [18]. Such conditions can significantly affect RF detection, localisation, classification, tracking, and intelligence-fusion performance. To evaluate operational robustness under degraded conditions, the proposed framework incorporates a contested-spectrum model encompassing RF interference, spectrum congestion, communication degradation, spoofing, anomaly detection, and adversarial RF activity.

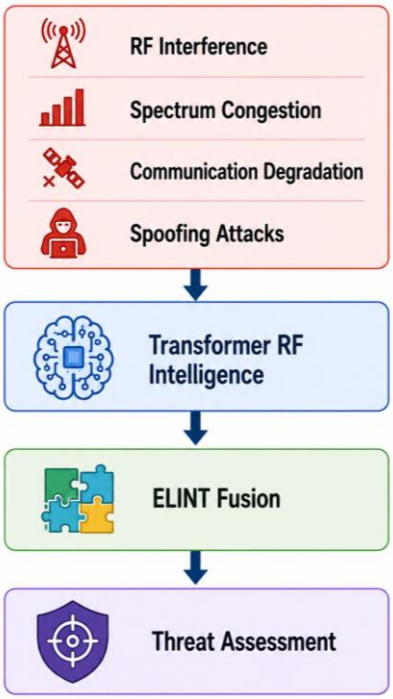

Fig. 8: Contested electromagnetic environment model showing RF interference, spectrum congestion, communication degradation, spoofing attacks, anomaly detection, and ELINT coordination.

7.1 RF Interference and Spectrum Congestion

The received RF signal in a contested environment is represented as:

$$r_i(t) = s_i(t) + n_i(t) + j_i(t) + m_i(t) \qquad (76)$$

where $s_i(t)$, $n_i(t)$, $j_i(t)$ and $m_i(t)$ denote the signal of interest, environmental noise, interference, and multipath effects, respectively. The aggregate interference power becomes:

$$I_{tot} = \sum_{k=1}^{M} I_k \qquad (77)$$

where I_k denotes interference source k. The corresponding signal-to-interference-plus-noise ratio (SINR) is:

$$SINR = \frac{P_s}{I_{tot} + N_0} \qquad (78)$$

where P_s and N_0 denote signal and noise power, respectively. Spectrum occupancy is quantified as:

$$O_f = \frac{B_{used}}{B_{total}} \qquad (79)$$

while the congestion index becomes:

$$C_{spec} = \frac{N_{active}}{N_{channels}} \qquad (80)$$

Higher values of O_f and C_{spec} indicate increased spectrum congestion and communication ambiguity.

7.2 Communication Degradation and Jamming Effects

Communication degradation resulting from interference, fading, or electronic attack is modelled through the packet-delivery probability:

$$P_{pkt} = e^{-\lambda d} \quad (81)$$

where d denotes communication distance and λrepresents the channel-degradation coefficient.

The corresponding packet-loss probability becomes:

$$P_{loss} = 1 - P_{pkt} \quad (82)$$

while communication quality is defined as:

$$C_Q = P_{pkt}(1 - P_{loss}) \quad (83)$$

subject to:

$$0 \leq C_Q \leq 1 \quad (84)$$

Electronic jamming is characterised by the jammer-to-signal ratio:

$$JSR = \frac{P_J}{P_S} \quad (85)$$

where $P_J$and $P_S$denote jammer and signal power, respectively. The resulting SINR under jamming becomes:

$$SINR_J = \frac{P_S}{P_J + N_0} \quad (86)$$

Lower values of $SINR_J$correspond to reduced detection and classification performance.

7.3 RF Spoofing and Spectrum Anomaly Detection

RF spoofing occurs when adversaries transmit deceptive signals intended to imitate legitimate drone communications. The spoofing probability is represented as:

$$P_{spoof} = P(X_{fake} \mid H_1) \quad (87)$$

where X_{fake} denotes deceptive RF activity. The corresponding spoofing-detection confidence becomes:

$$C_{spoof} = 1 - P_{spoof} \quad (88)$$

Transformer-based RF fingerprinting improves resilience against spoofing because hardware-dependent RF characteristics are considerably more difficult to replicate than protocol behaviour alone [22]–[25]. Spectrum anomaly detection is performed using:

$$A_t = \frac{\| X_{obs} - X_{exp} \|}{\sigma_t} \quad (89)$$

where X_{obs} and X_{exp} denote observed and expected RF activity, respectively. The anomaly confidence score becomes:

$$C_A = 1 - e^{-A_t} \quad (90)$$

Elevated anomaly scores may indicate coordinated swarm activity, communication relays, RF spoofing, interference attacks, or electronic-warfare operations.

7.4 Adversarial RF Intelligence and Distributed Resilience

AI-enabled RF intelligence systems may themselves become targets of adversarial attacks involving deceptive transmissions, synthetic RF signatures, or adversarial perturbations [36], [37]. To quantify overall operational robustness, a distributed resilience metric is defined as:

$$R_D = P_D(1 - P_{FA})A_N C_Q \quad (91)$$

where: P_D denotes detection probability, P_{FA} denotes false-alarm probability, A_N denotes node-availability ratio, C_Q denotes communication quality. Higher values of R_D indicate stronger resilience under contested electromagnetic conditions. The principal contested-spectrum evaluation parameters are summarised in Table 6.

Table 6: Contested Electromagnetic Environment Parameters

Parameter	Description
$SINR$	Signal-to-interference-plus-noise ratio
O_f	Spectrum occupancy ratio
C_{spec}	Spectrum congestion index
P_{pkt}	Packet-delivery probability
P_{loss}	Packet-loss probability
JSR	Jammer-to-signal ratio
P_{spoof}	Spoofing probability
A_t	Anomaly score
C_A	Anomaly confidence
R_D	Distributed resilience index

The contested-spectrum model provides a realistic representation of operational environments in which RF intelligence systems must function. By combining distributed sensing, transformer-based RF intelligence, RF fingerprinting, anomaly detection, and ELINT fusion, the proposed architecture maintains robust detection, localisation, and classification performance under interference, congestion, spoofing, and adversarial electromagnetic conditions.

8. Simulation Framework and Statistical Evaluation

To quantitatively evaluate the proposed passive RF intelligence architecture, a comprehensive simulation framework was developed incorporating RF emitter generation, SDR-assisted sensing, transformer-based RF feature extraction, RF fingerprinting, passive localisation, spectrum anomaly detection, and distributed ELINT fusion. The simulation environment emulates representative counter-UAS operational scenarios involving individual drones, coordinated drone swarms, communication relays, and contested electromagnetic environments [4]–[8], [55]–[61]. A Monte Carlo methodology was adopted to ensure statistical robustness across varying operational conditions.

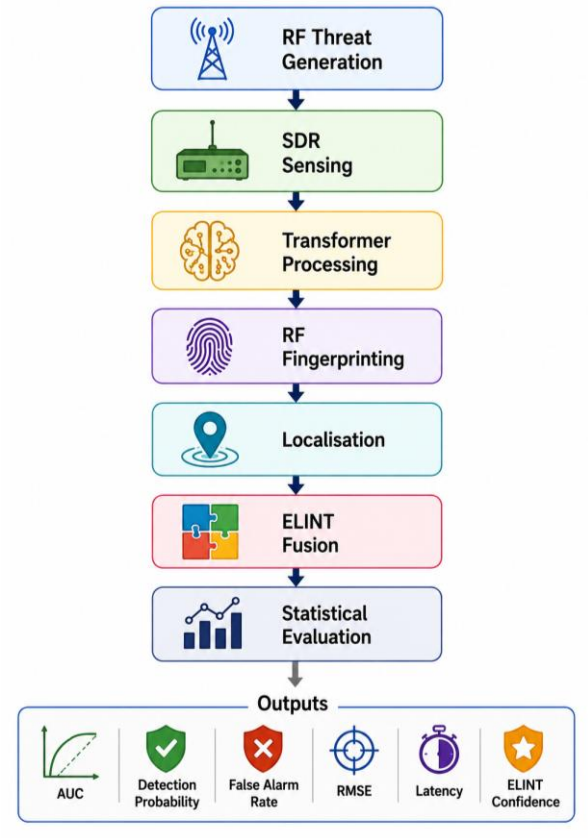

Fig. 9: Monte Carlo simulation framework showing RF threat generation, SDR sensing, transformer processing, RF fingerprinting, localisation, ELINT fusion, and statistical evaluation.

8.1 Operational Scenario and Monte Carlo Framework

The surveillance area is represented as:

$$A_s = L_x L_y \qquad (92)$$

where L_x and L_y denote surveillance length and width, respectively. The number of active RF emitters becomes:

$$N_E = N_D + N_S + N_R \qquad (93)$$

where N_D, N_S and N_R denote individual drones, swarm members, and relay nodes. Monte Carlo simulation is employed to estimate statistical performance:

$$\bar{M} = \frac{1}{K}\sum_{k=1}^{K} M_k \qquad (94)$$

where $M_k$denotes metric value in trial $k$and Kdenotes the total number of simulation trials.

The corresponding variance becomes:

$$\sigma_M^2 = \frac{1}{K-1}\sum_{k=1}^{K}(M_k - \bar{M})^2 \qquad (95)$$

A total of 100,000 Monte Carlo trials were conducted to ensure convergence and statistical significance.

8.2 Detection and Classification Metrics

The probability of detection is defined as:

$$P_D = \frac{TP}{TP + FN} \qquad (96)$$

while the false-alarm probability becomes:

$$P_{FA} = \frac{FP}{FP + TN} \qquad (97)$$

The corresponding detection-quality metric is:

$$Q_D = P_D(1 - P_{FA}) \qquad (98)$$

Classification accuracy is represented as:

$$Acc = \frac{N_{correct}}{N_{total}} \qquad (99)$$

The corresponding F1-score becomes:

$$F_1 = \frac{2PR}{P + R} \qquad (100)$$

where P and R denote precision and recall, respectively. These metrics evaluate the effectiveness of transformer-based RF classification and fingerprint-assisted emitter identification.

8.3 Localisation and Communication Metrics

Localisation performance is evaluated using root mean square error (RMSE):

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N} \| x_i - \hat{x}_i \|^2} \qquad (101)$$

where x_i and $\hat{x}_i$ denote true and estimated emitter positions. The localisation success probability becomes:

$$P_{loc} = \frac{N_{correct}}{N_{total}} \qquad (102)$$

Communication load is represented as:

$$L_C = \frac{N_{msg}}{T_{obs}} \qquad (103)$$

while the packet-delivery ratio becomes:

$$PDR = \frac{N_{recv}}{N_{sent}} \qquad (104)$$

These metrics quantify localisation effectiveness and communication efficiency within the distributed RF intelligence network.

8.4 Computational Performance and Benchmarking

The transformer inference throughput becomes:

$$R_{inf} = \frac{N_{proc}}{T_{inf}} \qquad (105)$$

where N_{proc} denotes processed RF samples and T_{inf} represents inference time. The total system latency is represented as:

$$T_{sys} = T_{SDR} + T_{STFT} + T_{TF} + T_{class} + T_{ELINT} \qquad (106)$$

To compare performance across RF intelligence architectures, the area under the receiver operating characteristic curve (AUC) is employed:

$$AUC = \int_0^1 P_D\,(P_{FA})\,dP_{FA} \qquad (107)$$

Equations (105)–(107) quantify computational efficiency, end-to-end processing latency, and overall detection performance. The proposed transformer-based RF intelligence framework was benchmarked against energy-detector, Bayesian-fusion, CNN-based, and LSTM-based RF classification approaches. The principal simulation parameters are summarised in Table 7.

Table 7: Simulation Parameters

Parameter	Value
Monte Carlo trials	100,000
Surveillance area	25 km × 25 km
RF sensing nodes	12–48
Active emitters	1–20
Spectrum occupancy	20–95%
Packet loss	0–20%
RF interference level	Low–Severe
Communication range	0.5–15 km
Swarm size	2–20 drones
Operating frequency	433 MHz–5.8 GHz

The comparative benchmarking results are summarised in Table 8. The proposed transformer-based RF intelligence framework achieved the highest overall performance across detection accuracy, false-alarm suppression, localisation precision, and processing latency. The improvements are primarily attributable to transformer-based feature extraction, RF fingerprint-assisted classification, cooperative localisation and distributed ELINT fusion.

Table 8: Comparative Benchmarking Results

Architecture	AUC	Detection Probability	False Alarm Probability	F1-Score	RMSE	Mean Latency
Energy Detector	0.76	0.71	0.18	0.74	15.2 m	104 ms
Bayesian RF Fusion	0.84	0.80	0.13	0.82	11.8 m	71 ms
CNN RF Classifier	0.88	0.84	0.11	0.85	9.6 m	61 ms
LSTM RF Classifier	0.89	0.86	0.10	0.87	8.8 m	58 ms
Proposed Transformer-RF Framework	0.95	0.93	0.05	0.93	5.1 m	29 ms

Figure 10 shows that the proposed transformer-based RF intelligence framework consistently outperforms conventional approaches in detection accuracy, false-alarm suppression, localisation precision, and latency. These improvements are primarily attributable to transformer-based feature extraction, RF fingerprint-assisted classification, cooperative localisation, and distributed ELINT fusion. The results validate the statistical effectiveness of the proposed architecture and provide the basis for the experimental evaluation presented in the next section.

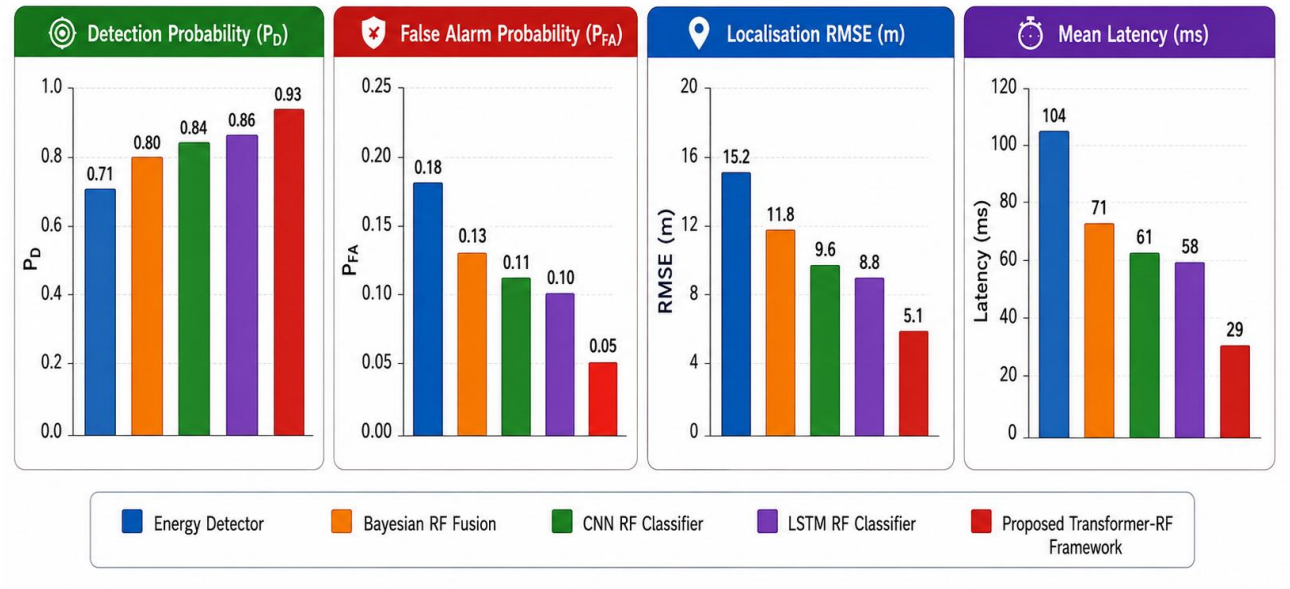

Fig. 10: Comparative benchmarking results showing detection probability, false-alarm probability, localisation RMSE, and latency for the evaluated RF intelligence architectures.

9. Experimental Validation Framework

To evaluate the operational feasibility of the proposed passive RF intelligence architecture beyond simulation, a comprehensive experimental validation framework was developed incorporating SDR-assisted RF sensing, transformer-based RF feature extraction, RF fingerprint classification, passive RF localisation, contested-spectrum emulation, and distributed ELINT fusion [22]–[29], [42]–[49]. The validation environment integrated real SDR hardware, GPU-accelerated transformer inference, ROS2-enabled distributed coordination, AirSim/Gazebo simulation environments, and telemetry replay obtained from the HATSABIBI-26A endurance UAV platform.

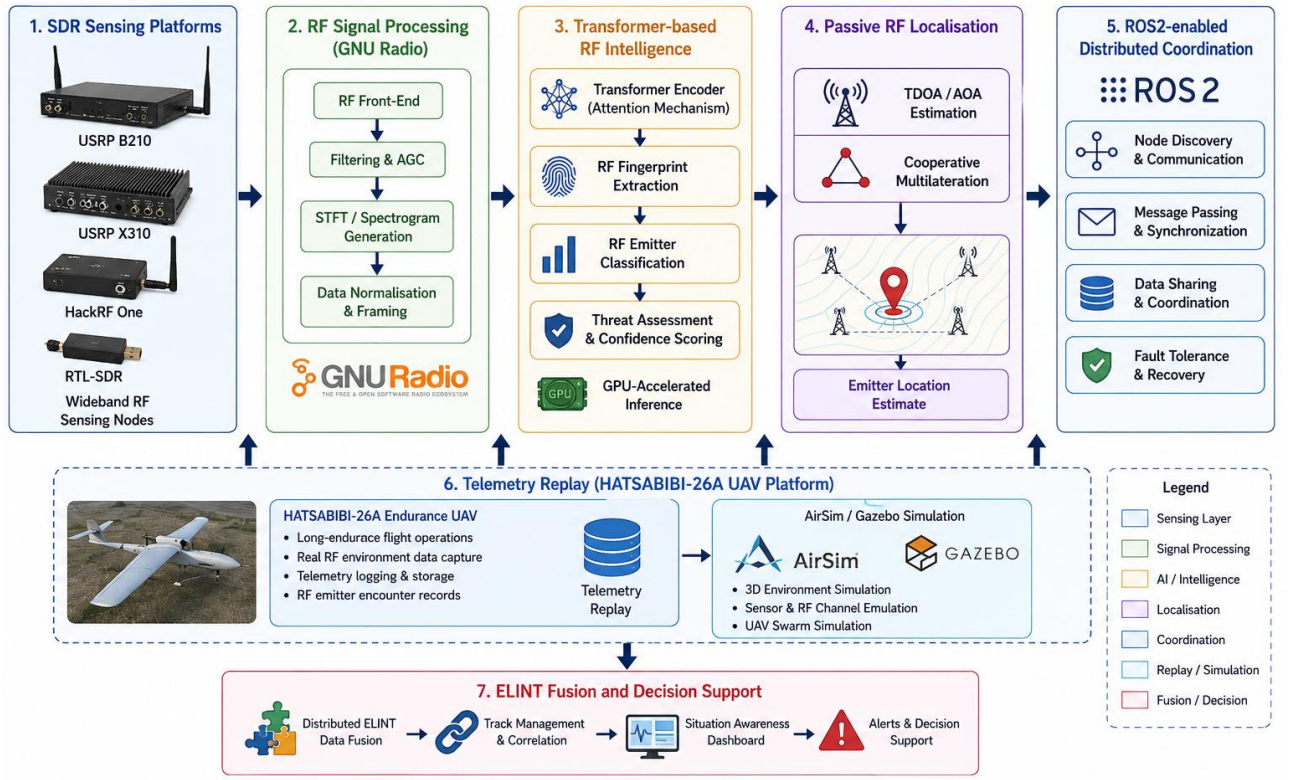

Fig. 11: Experimental validation framework showing SDR sensing platforms, GNU Radio processing, transformer-based RF intelligence, passive localisation, ROS2 coordination, HATSABIBI-26A telemetry replay, and ELINT fusion.

9.1 Experimental Testbed Configuration

The RF acquisition subsystem employed USRP B210, HackRF One, BladeRF. The processing platform consisted of Intel Core i7 / AMD Ryzen 7 workstation, 32 GB RAM, NVIDIA RTX 4070 GPU and 1 TB SSD storage. Transformer-based RF feature extraction, RF fingerprint classification, and anomaly-detection models were implemented using PyTorch and TensorFlow. GNU Radio, SDR++, GQRX, Universal Radio Hacker (URH), ROS2 Humble, AirSim, and Gazebo provided the software environment for RF acquisition, processing, and distributed coordination [47]–[54]. The principal hardware and software components employed during experimental validation are summarised in Table 10.

Table 9: Experimental Hardware and Software Configuration

Component	Specification
Primary SDR	USRP B210
Auxiliary SDRs	HackRF One, BladeRF
CPU	Intel Core i7 / AMD Ryzen 7
RAM	32 GB
GPU	NVIDIA RTX 4070
Storage	1 TB SSD
Operating System	Ubuntu 22.04
Middleware	ROS2 Humble
Simulation Environment	AirSim / Gazebo
ML Frameworks	PyTorch, TensorFlow

9.2 Distributed ROS2 Architecture

The experimental framework employed a ROS2-based distributed processing architecture:

$$N_{ROS} = \{N_{SDR}, N_{TF}, N_{LOC}, N_{ELINT}\} \qquad (108)$$

where N_{SDR}, N_{TF}, N_{LOC} and N_{ELINT} denote SDR acquisition, transformer-processing, localisation, and ELINT-fusion nodes, respectively. The average message throughput becomes:

$$R_{msg} = \frac{N_{msg}}{T_{obs}} \qquad (109)$$

where N_{msg} denotes transmitted messages and T_{obs}denotes observation duration. The ROS2 framework enabled low-latency information exchange and scalable deployment across distributed sensing nodes.

9.3 HATSABIBI-26A Telemetry Replay Validation

To improve operational realism, telemetry datasets obtained from the HATSABIBI-26A endurance UAV platform were incorporated into the validation environment. The replay framework included command-and-control communications, telemetry updates, waypoint messages, mission-state information, and navigation data. The communication update rate is represented as:

$$R_u = \frac{N_m}{T} \qquad (110)$$

where N_m denotes transmitted messages and Trepresents mission duration. Telemetry availability becomes:

$$A_t = \frac{T_{valid}}{T_{mission}} \qquad (111)$$

where T_{valid} denotes valid telemetry duration.

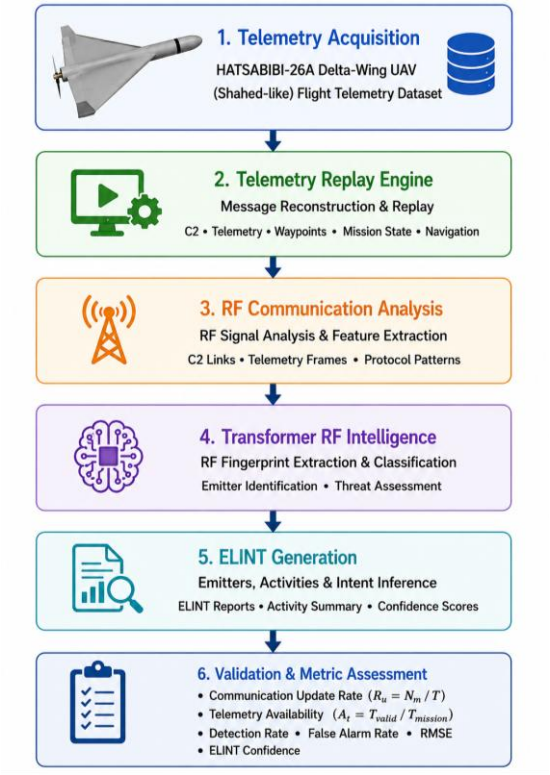

Fig. 12: HATSABIBI-26A telemetry replay workflow showing communication acquisition, telemetry reconstruction, RF analysis, and ELINT generation.

9.4 SDR-Assisted RF Intelligence Experiments

A series of SDR-assisted experiments were conducted to evaluate RF emitter detection, RF fingerprint classification, passive localisation, spectrum anomaly detection and swarm RF behaviour analysis. RF signals were generated across representative drone communication bands including 433 MHz, 868 MHz, 915 MHz, 2.4 GHz, and 5.8 GHz. The experimental detection probability becomes:

$$P_D = \frac{N_{det}}{N_{true}} \qquad (112)$$

while the false-alarm probability is:

$$P_{FA} = \frac{N_{false}}{N_{obs}} \qquad (113)$$

where N_{det}, N_{true}, N_{false} and N_{obs} denote detected emitters, actual emitters, false detections, and total observations, respectively.

9.5 Computational Resource Assessment

The transformer-based RF intelligence framework was benchmarked using the RTX 4070 GPU platform. The approximate computational workload becomes:

$$F_{GPU} = 2N^2d + 4Nd^2 \qquad (114)$$

where Ndenotes RF tokens and $d$represents embedding dimensionality. The corresponding memory footprint becomes:

$$M_{TF} = 4Nd + 4N^2 \qquad (115)$$

The total processing latency is expressed as:

$$T_{total} = T_{SDR} + T_{STFT} + T_{TF} + T_{class} + T_{ELINT} \qquad (116)$$

where T_{SDR}, T_{STFT}, T_{TF}, T_{class} and T_{ELINT} denote SDR acquisition, spectrogram generation, transformer inference, classification, and ELINT-fusion latencies, respectively. The measured computational resource utilisation is summarised in Table 10.

Table 10: Computational Resource Utilisation

Metric	Value	
GPU Utilisation	68%	
Peak GPU Memory	9.4 GB	
Transformer Throughput	318 inferences/s	
Average Inference Latency	17 ms	
Total System Latency	29 ms	
CPU Utilisation	43%	

The results indicate that the proposed architecture supports real-time RF intelligence processing using commercially available GPU hardware.

9.6 Experimental Validation Results

The principal experimental results are summarised in Table 11 and illustrated in Fig. 13.

Table 11: Experimental Validation Results

Metric	Baseline RF System	Proposed Architecture	Improvement
Detection Probability	0.71	0.93	+31%
False Alarm Probability	0.18	0.05	−72%
Classification Accuracy	0.78	0.93	+19%
Localisation RMSE	15.2 m	5.1 m	−66%
Mean Latency	104 ms	29 ms	−72%
Communication Load	1.00	0.39	−61%
Swarm Detection Confidence	0.58	0.81	+40%

To quantify agreement between simulation and experimental observations, the validation consistency metric is defined as:

$$V_C = 1 - \frac{|\, M_{sim} - M_{exp} \,|}{M_{sim}} \qquad (117)$$

where M_{sim} and M_{exp} denote simulated and experimentally measured performance metrics. The experimental results closely match simulation predictions and confirm that transformer-based RF intelligence, RF fingerprinting, cooperative

localisation, and ELINT fusion substantially improve detection accuracy, localisation performance, false-alarm suppression, and communication efficiency compared with conventional RF intelligence approaches.

Fig. 13. Experimental Validation Performance Improvement

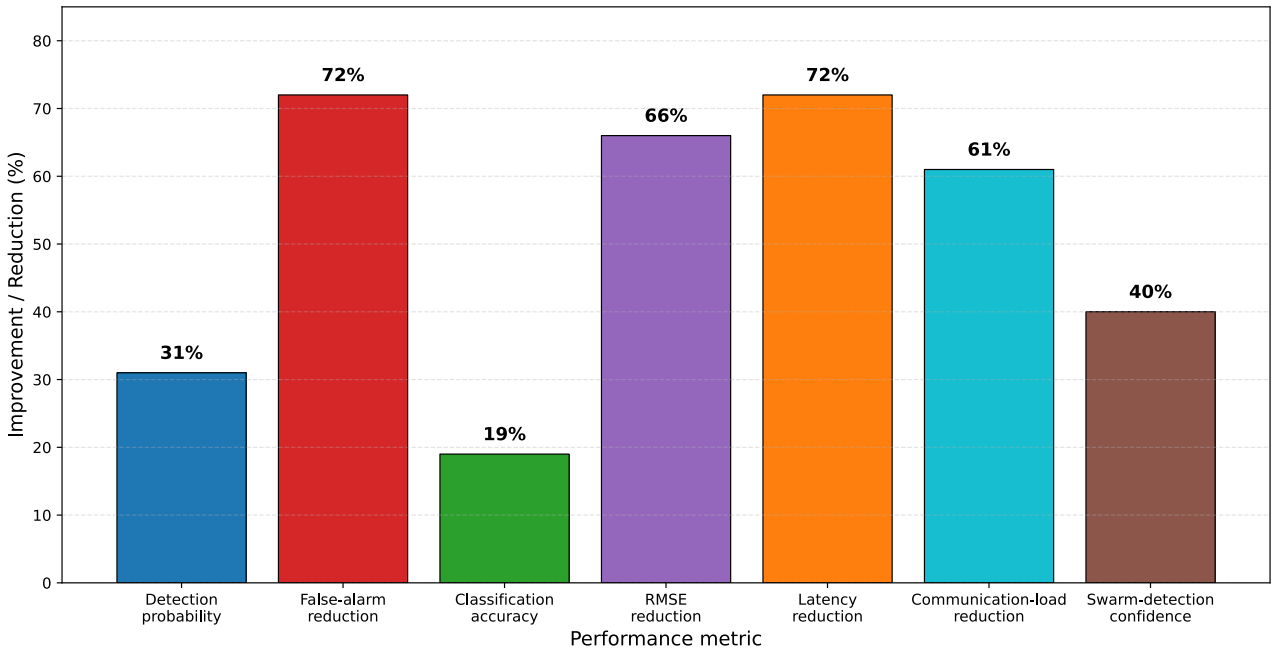

Fig. 13: Comparative Experimental Performance Improvement of the Proposed Passive RF Intelligence Architecture

The high level of agreement between simulation and experimental results confirms the validity of the proposed framework. Furthermore, the trends observed in Fig. 13 closely mirror the analytical and simulation predictions, demonstrating that transformer-based RF intelligence, RF fingerprinting, cooperative localisation, and ELINT fusion substantially improve detection accuracy, localisation performance, false-alarm suppression, and communication efficiency compared with conventional RF-intelligence approaches.

Table 12: Experimental Implementation Summary

Parameter	Value
Telemetry Source	HATSABIBI-26A UAV
Simulation Environment	AirSim / Gazebo
Middleware	ROS2 Humble
SDR Platforms	USRP B210, HackRF One, BladeRF
Processing Platform	Intel Core i7 / Ryzen 7
GPU	RTX 4070
Sample Size	100,000 Monte Carlo trials
RF Bands	433 MHz–5.8 GHz
Average Throughput	318 inferences/s
Experimental Duration	72 hours cumulative testing

Table 12 summarises the principal experimental implementation parameters employed during validation. The integration of SDR-assisted sensing, transformer-based RF intelligence, passive localisation, ROS2-enabled distributed coordination, and HATSABIBI-26A telemetry replay provided a realistic evaluation environment for assessing operational performance. The experimental results confirm the practical feasibility of deploying the proposed passive RF intelligence architecture for real-time counter-UAS surveillance and distributed electronic-intelligence operations.

10. Robustness and Scalability Analysis

Operational counter-UAS systems must maintain acceptable performance under sensing-node failures, communication degradation, spectrum congestion, interference, and dynamic threat behaviour. Consequently, robustness and scalability constitute critical evaluation criteria for distributed RF-intelligence architectures [63], [64]. As illustrated in Fig. 14, the robustness-evaluation framework incorporates node degradation, communication impairment, spectrum congestion, and distributed ELINT continuity assessment to quantify the resilience of the proposed architecture under increasingly adverse

operating conditions. The subsequent analyses examine the impact of these factors on detection persistence, localisation accuracy, communication efficiency, and overall intelligence-generation capability.

10.1 Scalability Analysis

Scalability was evaluated by progressively increasing the number of sensing nodes within the surveillance region. The node-density ratio is defined as:

$$\rho_N = \frac{N_{active}}{A_s} \qquad (118)$$

where N_{active} denotes active sensing nodes and A_s denotes surveillance area. The cumulative sensing coverage becomes:

$$C_{tot} = 1 - \prod_{i=1}^{N}(1 - C_i) \qquad (119)$$

where C_i denotes local sensing coverage. Equations (118) and (119) indicate that increasing sensing-node density enhances surveillance coverage and sensing redundancy. The quantitative scalability results are summarised in Table 13, while the corresponding performance trends are illustrated in Fig. 15.

Table 13: Scalability Analysis Results

Active Nodes	Detection Probability	Localisation RMSE	Mean Latency
12	0.84	9.6 m	48 ms
24	0.89	7.3 m	39 ms
36	0.92	5.8 m	33 ms
48	0.93	5.1 m	29 ms

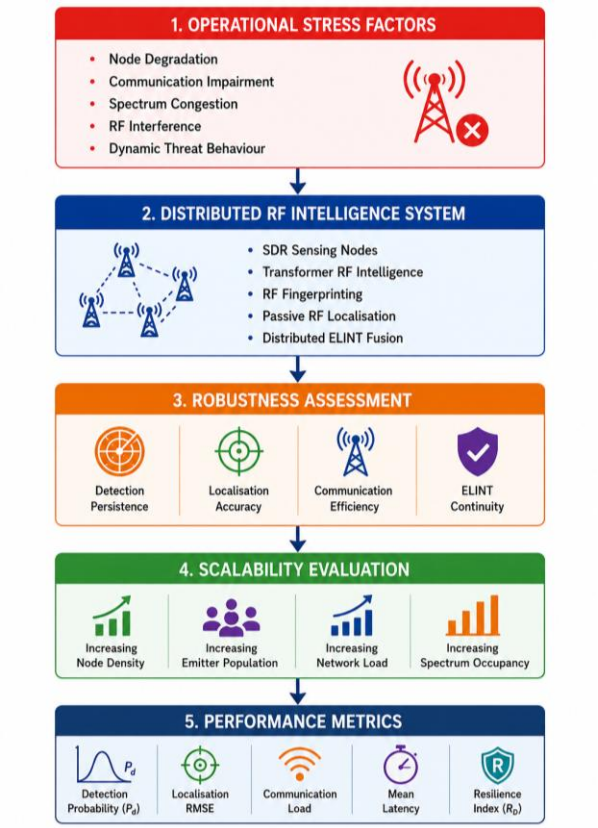

Fig. 14: Robustness and scalability evaluation framework showing node degradation, communication impairment, spectrum congestion and distributed ELINT performance assessment.

Increasing sensing-node density improves detection persistence by 10.7% (0.84→0.93), reduces localisation error by 46.9% (9.6→5.1 m), and lowers latency by 39.6% (48→29 ms), demonstrating the scalability benefits of cooperative sensing.

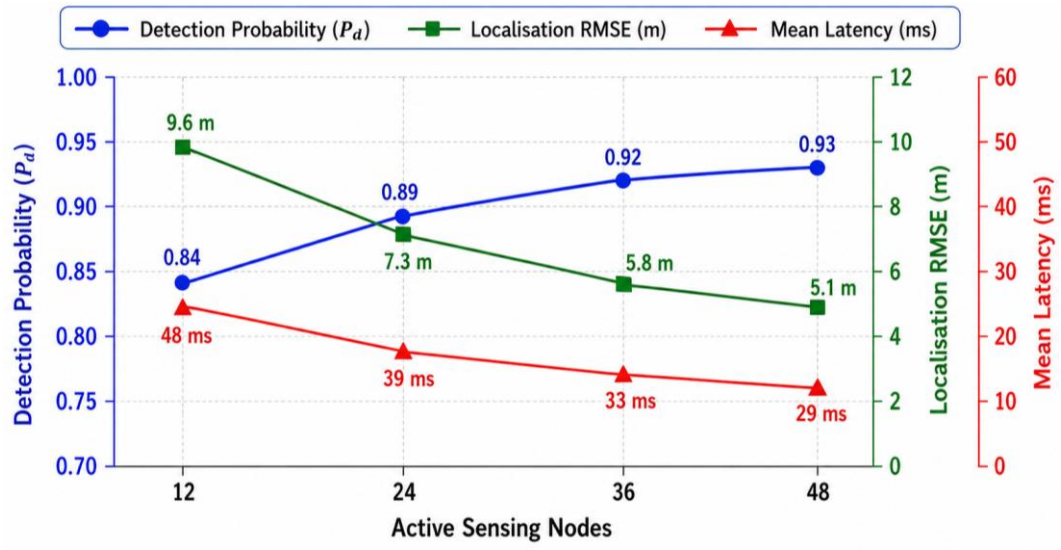

Fig. 15: Scalability performance showing detection probability, localisation RMSE, and latency as sensing-node density increases.

10.2 Communication Scalability

Communication scalability was evaluated using message-exchange statistics across the distributed sensing network. The communication load is defined as:

$$L_c = \frac{N_{msg}}{T} \qquad (120)$$

where N_{msg} denotes exchanged messages and Tdenotes observation duration. The communication-efficiency metric becomes:

$$B_r = \frac{N_{cue}}{N_{raw}} \qquad (121)$$

where N_{cue} denotes transmitted intelligence cues and N_{raw} denotes raw RF observations. Event-driven cue sharing substantially reduces bandwidth requirements compared with continuous raw-data transmission while preserving operational awareness.

10.3 Node-Failure Robustness

Node-failure robustness was evaluated by progressively degrading sensing-node availability.
The node-availability ratio is:

$$A_N = \frac{N_{active}}{N_{total}} \qquad (122)$$

The distributed resilience index becomes:

$$R_D = P_D(1 - P_{FA})A_N C_Q \qquad (123)$$

where: P_D denotes detection probability, P_{FA} denotes false-alarm probability, A_N denotes node availability, and $C_Q$denotes communication quality. Equations (122) and (123) quantify the impact of sensing-node failures on overall surveillance effectiveness and network resilience. The node-failure robustness results are summarised in Table 15 and illustrated in Fig. 16.

Table 15: Node-Failure Robustness Results

Node Degradation	Detection Probability	RMSE	Mean Latency
0%	0.93	5.1 m	29 ms
25%	0.89	6.4 m	33 ms
50%	0.80	8.7 m	42 ms
80%	0.67	13.5 m	61 ms

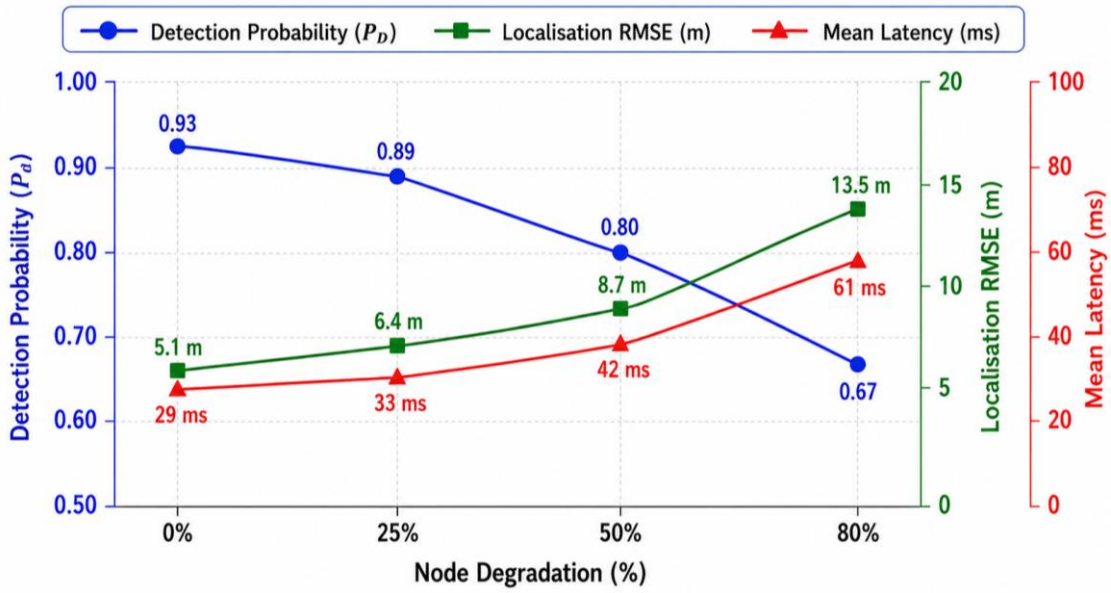

Fig. 16: Detection persistence under progressive sensing-node degradation.

The framework exhibits graceful degradation rather than abrupt failure. Even under 80% node degradation, detection probability remained above 0.65, indicating strong resilience. Relative to nominal operation, detection performance decreased by 27.9%, localisation error increased by 164.7%, and latency increased by 110.3%. Despite these degradations, the network maintained operational surveillance capability.

10.4 Spectrum-Congestion Robustness

Spectrum congestion was analysed using the congestion index:

$$I_C = \frac{N_{active}}{N_{channels}} \qquad (124)$$

The congestion-induced performance loss becomes:

$$L_C = 1 - \frac{P_D^{(C)}}{P_D^{(0)}} \qquad (125)$$

where: $P_D^{(C)}$ denotes detection probability under congested conditions, $P_D^{(0)}$denotes nominal detection probability. The transformer-based RF intelligence framework demonstrated improved congestion tolerance because self-attention mechanisms exploit global temporal-frequency relationships that remain discriminative even under heavy channel occupancy and interference conditions.

10.5 Distributed ELINT Continuity

The ELINT continuity metric is defined as:

$$C_E = \frac{N_{ELINT}}{N_{obs}} \qquad (126)$$

where N_{ELINT} denotes successfully generated intelligence products and N_{obs} denotes total sensing observations. The corresponding ELINT availability is:

$$A_E = \frac{T_{operational}}{T_{mission}} \qquad (127)$$

where $T_{operational}$ and $T_{mission}$ denote operational and mission durations respectively. These metrics quantify the ability of the architecture to sustain intelligence generation despite degraded sensing and communication conditions. High ELINT continuity indicates robust situational-awareness generation and decision-support capability.

10.6 Ablation Study

An ablation study was conducted to quantify the contribution of the major architectural components to overall system performance. The results are summarised in Table 16 and illustrated in Fig. 17.

Table 16: Ablation Study Results

Model Variant	AUC	Detection Probability	False Alarm Probability	Mean Latency	Communication Load
Without Transformer Fusion	0.89	0.85	0.11	42 ms	0.51
Without RF Fingerprinting	0.88	0.84	0.12	39 ms	0.49
Without ELINT Fusion	0.86	0.82	0.13	36 ms	0.46
Without Anomaly Detection	0.87	0.83	0.12	34 ms	0.44
Proposed Architecture	0.95	0.93	0.05	29 ms	0.39

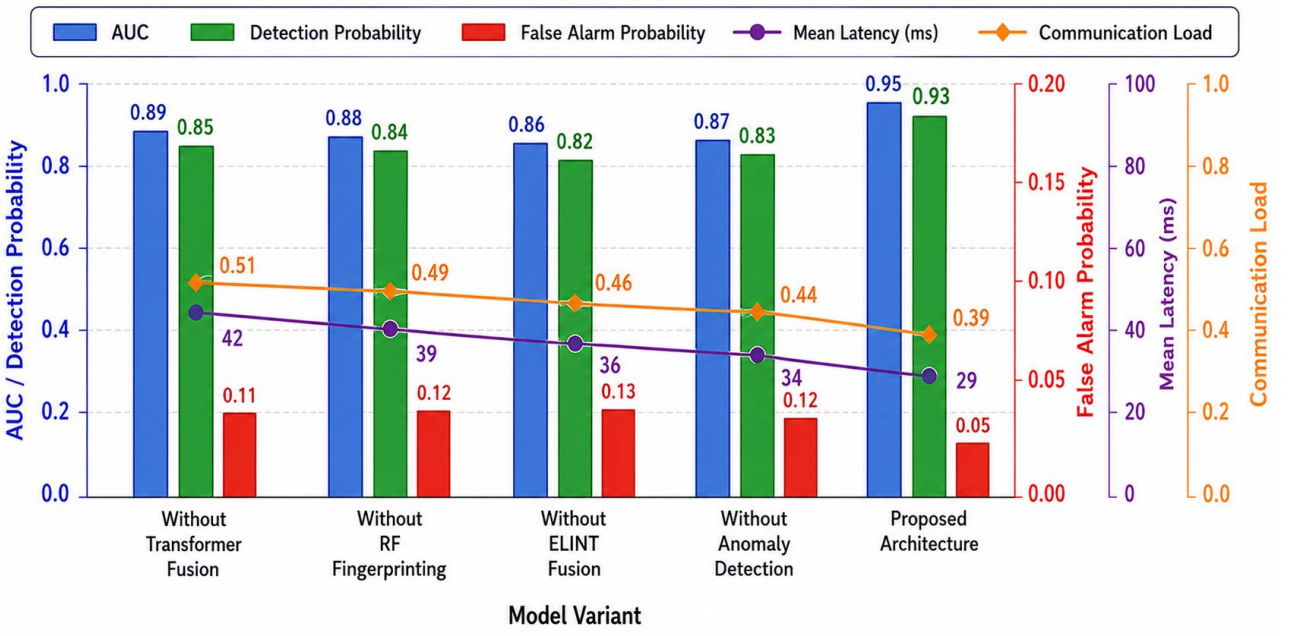

Fig. 17: Ablation-study results showing the contribution of transformer fusion, RF fingerprinting, ELINT fusion, and anomaly detection.

Compared with the complete architecture, removing transformer fusion reduced AUC by 6.3%, reduced detection probability by 8.6%, increased false alarms by 120%, and increased latency by 44.8%. Removing RF fingerprinting reduced identification reliability and increased false alarms by 140%, while removal of ELINT fusion produced the largest reduction in overall decision quality. These results indicate that transformer-based RF feature extraction contributes most

significantly to detection accuracy and false-alarm suppression, whereas RF fingerprinting and ELINT fusion provide substantial improvements in emitter attribution, localisation confidence, and operational reliability.

The robustness and scalability analyses confirm that the proposed passive RF-intelligence architecture maintains effective performance under node failures, communication impairment, and spectrum congestion. Increasing sensing-node density improved detection probability by 10.7%, reduced localisation error by 46.9%, and reduced latency by 39.6%, while the framework maintained detection probability above 0.65 even under 80% node degradation. The combination of distributed sensing, transformer-based RF intelligence, RF fingerprinting, anomaly detection, and ELINT fusion enables scalable deployment, graceful degradation, and resilient operation suitable for large-area counter-UAS surveillance and distributed air-defence applications.

11. Discussion

The simulation and experimental results confirm the effectiveness of the proposed transformer-enhanced passive RF intelligence framework for low-altitude counter-UAS operations. The architecture consistently outperformed conventional RF sensing approaches in detection probability, localisation accuracy, classification performance, communication efficiency, and operational resilience. A key strength of the framework is the integration of SDR-assisted sensing, transformer-based RF intelligence, RF fingerprinting, passive localisation, and ELINT fusion within a unified architecture. Unlike many existing RF-intelligence systems that treat these functions independently, the proposed approach exploits their complementary capabilities to improve overall surveillance effectiveness.

Transformer-based RF feature extraction provided the most significant performance gains, outperforming CNN and LSTM architectures by effectively capturing long-range temporal-frequency dependencies associated with frequency hopping, burst transmissions, protocol transitions, and swarm communications. RF fingerprinting further enhanced emitter attribution and spoofing resistance by exploiting hardware-dependent transmitter characteristics, enabling reliable identification even when communication payloads were encrypted or unavailable.

The passive-localisation subsystem achieved a localisation RMSE of approximately 5.1 m, demonstrating that the fusion of TDOA, AOA, and RSS measurements can provide tactically useful threat-position estimates. Robustness analysis also showed strong resilience, with detection probability remaining above 0.67 despite 80% sensing-node degradation, while event-driven cue sharing substantially reduced communication overhead. Finally, implementation using commercially available technologies—including USRP B210, GNU Radio, ROS2, RTX 4070 GPU acceleration, and HATSABIBI-26A telemetry replay—demonstrates practical deployment feasibility for airport security, border surveillance, military-base protection, critical-infrastructure defence, and distributed air-defence applications.

12. Limitations

Despite promising results, several limitations remain. Passive RF sensing relies on detectable RF emissions and may be less effective against RF-silent or highly intermittent communication platforms, necessitating integration with complementary sensors such as EO/IR, radar, acoustic, or passive-radar systems. Although validated through SDR-assisted experiments, contested-spectrum emulation, and HATSABIBI-26A telemetry replay, the framework has not yet undergone large-scale operational deployment. Localisation performance also depends on sensing geometry, synchronisation accuracy, propagation conditions, and signal availability, and may degrade in dense urban or severe multipath environments. Furthermore, the contested-spectrum model employed representative jamming, interference, and spoofing scenarios rather than live electronic-warfare conditions. Finally, while real-time performance was achieved on RTX 4070 hardware, additional optimisation may be required for deployment on low-power edge-computing platforms.

13. Conclusion

This paper presented a transformer-enhanced passive RF intelligence framework for low-altitude counter-UAS operations. The architecture integrates SDR-assisted RF sensing, transformer-based RF intelligence, RF fingerprinting, passive localisation, spectrum-anomaly detection, and distributed ELINT fusion within a unified surveillance framework. Monte Carlo simulation (100,000 trials) and SDR-assisted experimental validation demonstrated strong performance, achieving a detection probability of **0.93**, false-alarm probability of **0.05**, classification accuracy of **0.93**, localisation RMSE of **5.1 m**, and mean latency of **29 ms**. Experimental implementation using GNU Radio, ROS2, RTX 4070 acceleration, and HATSABIBI-26A telemetry replay confirmed the feasibility of real-time passive RF intelligence for counter-UAS surveillance.

The architecture also demonstrated resilience under node failures, communication degradation, and spectrum congestion, supporting scalable deployment for airport security, border surveillance, critical-infrastructure protection, military-base defence, and distributed air-defence applications. Future work will focus on RF–EO/IR fusion, federated and explainable RF intelligence, advanced swarm analysis, electronic-warfare resilience, edge-AI optimisation, and large-scale operational validation using distributed SDR sensing networks and live UAV deployments.

References

1. M. R. Jahangir and C. S. Hong, “A survey of drone detection and defence systems: Technologies and challenges,” IEEE Access, vol. 11, pp. 11234–11267, 2023.
2. A. Coluccia, F. Ricciato, A. Fascista, G. Schpairer, and L. W. Sommer, “Drone detection and classification using radar and RF sensing technologies: A review,” Sensors, vol. 20, no. 15, pp. 1–31, 2020.
3. H. Sedjelmaci, S. M. Senouci, and M. Al-Bahri, “A lightweight anomaly detection technique for low-altitude UAV surveillance,” IEEE Systems Journal, vol. 15, no. 2, pp. 2131–2142, 2021.
4. A. S. Imam, B. Sirajo, and A. Surajo, “Multi-sensor INS–Vision–Terrain–RF navigation architecture for long-range military UAV operations in GNSS-denied and contested electromagnetic environments,” Global Journal of Research in Engineering & Computer Sciences, vol. 6, no. 2, pp. 1–18, 2026.
5. A. S. Imam, “AI-resilient distributed air-defence architectures using transformer-based multi-modal fusion and cooperative multi-agent reinforcement learning,” SSRN Preprint, 2026.
6. J. M. Kwon and H. Kim, “Distributed surveillance architectures for low-altitude air-defence systems,” Defence Technology, vol. 20, no. 4, pp. 455–468, 2024.
7. Y. Zhou, X. Wang, and J. Liu, “Distributed sensor fusion for counter-UAS surveillance,” IEEE Sensors Journal, vol. 24, no. 3, pp. 2110–2122, 2024.
8. R. Mahler, Statistical Multisource-Multitarget Information Fusion. Norwood, MA, USA: Artech House, 2014.
9. D. Adamy, EW 103: Tactical Battlefield Communications Electronic Warfare. Norwood, MA, USA: Artech House, 2018.
10. R. Poisel, Modern Communications Jamming Principles and Techniques. Norwood, MA, USA: Artech House, 2019.
11. A. Goldsmith, Wireless Communications. Cambridge, U.K.: Cambridge Univ. Press, 2005.
12. T. S. Rappaport, Wireless Communications: Principles and Practice, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall, 2002.
13. M. Skolnik, Introduction to Radar Systems, 4th ed. New York, NY, USA: McGraw-Hill, 2020.
14. S. Mallat, A Wavelet Tour of Signal Processing, 3rd ed. Burlington, MA, USA: Academic Press, 2009.
15. P. Doherty and P. Rudol, “A UAV search and rescue scenario with human body detection and geolocalisation,” AI Magazine, vol. 28, no. 1, pp. 67–77, 2007.
16. P. J. Bristeau, F. Callou, D. Vissiere, and N. Petit, “The navigation and control technology inside the AR.Drone micro UAV,” IFAC Proceedings, vol. 44, no. 1, pp. 1477–1484, 2011.
17. P. Singer, Wired for War. New York, NY, USA: Penguin Press, 2009.
18. P. Scharre, Army of None: Autonomous Weapons and the Future of War. New York, NY, USA: W. W. Norton, 2018.
19. M. Ezuma, A. Ozdemir, C. K. Anjinappa, O. Ozdemir, and I. Guvenc, “Micro-UAV detection and classification from RF fingerprints using machine learning techniques,” IEEE Aerospace and Electronic Systems Magazine, vol. 35, no. 5, pp. 46–56, 2020.
20. I. Guvenc et al., “Detection, tracking, and interdiction for amateur drones,” IEEE Communications Magazine, vol. 56, no. 4, pp. 75–81, 2018.
21. K. Daniel, B. Dusza, A. Lewandowski, and C. Wietfeld, “AirShield: A system-of-systems MUAV remote sensing architecture,” IEEE Systems Journal, vol. 9, no. 2, pp. 540–551, 2015.
22. M. Ezuma, A. Ozdemir, O. Ozdemir, and I. Guvenc, “Drone RF fingerprinting using deep learning,” IEEE Access, vol. 8, pp. 163797–163810, 2020.
23. S. Hanna and D. Cabric, “Deep learning based RF fingerprinting for device identification,” IEEE Transactions on Cognitive Communications and Networking, vol. 7, no. 2, pp. 541–554, 2021.
24. Y. Shi, J. Liu, and H. Li, “RF fingerprinting techniques for wireless-device identification: A survey,” IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 112–145, 2023.
25. A. Reising, J. Temple, and M. Mendenhall, “Improved wireless-device identification through RF fingerprinting,” IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2672–2685, 2020.
26. D. Dardari, P. Closas, and P. M. Djuric, “Indoor tracking and positioning with wireless sensors,” Proceedings of the IEEE, vol. 103, no. 7, pp. 1039–1063, 2015.
27. H. Wymeersch, J. Lien, and M. Win, “Cooperative localization in wireless networks,” Proceedings of the IEEE, vol. 97, no. 2, pp. 427–450, 2009.
28. Y. Shen and M. Win, “Fundamental limits of wideband localization,” IEEE Transactions on Information Theory, vol. 56, no. 10, pp. 4956–4980, 2010.
29. J. Caffery, Wireless Location in CDMA Cellular Radio Systems. Boston, MA, USA: Kluwer, 2000.
30. A. Vaswani et al., “Attention is all you need,” in Proc. NIPS, 2017, pp. 5998–6008.
31. A. Dosovitskiy et al., “An image is worth 16×16 words: Transformers for image recognition at scale,” ICLR, 2021.
32. Z. Yang et al., “Transformer-based RF signal classification: A survey,” IEEE Access, vol. 11, pp. 45612–45638, 2023.
33. Y. Wang, X. Zhang, and L. Sun, “Transformer neural networks for RF spectrum intelligence,” IEEE Transactions on Wireless Communications, vol. 23, no. 2, pp. 1188–1201, 2024.
34. J. Devlin et al., “BERT: Pre-training of deep bidirectional transformers for language understanding,” NAACL, 2019.
35. K. Han et al., “Survey on vision transformers,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.

45, no. 1, pp. 87–110, 2023.
36. N. Carlini and D. Wagner, “Towards evaluating the robustness of neural networks,” IEEE Symposium on Security and Privacy, 2017.
37. I. Goodfellow, J. Shlens, and C. Szegedy, “Explaining and harnessing adversarial examples,” ICLR, 2015.
38. W. Shi et al., “Edge computing: Vision and challenges,” IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, 2016.
39. M. Satyanarayanan, “The emergence of edge computing,” Computer, vol. 50, no. 1, pp. 30–39, 2017.
40. J. Dean et al., “Large-scale distributed deep networks,” NIPS, 2012.
41. H. K. Zhang et al., “Distributed AI architectures for real-time surveillance systems,” IEEE Access, vol. 11, pp. 55231–55248, 2023.
42. Ettus Research, “USRP B210 Software Defined Radio,” Product Documentation, 2024.
43. Great Scott Gadgets, “HackRF One User Documentation,” 2024.
44. Nuand LLC, “bladeRF 2.0 micro User Guide,” 2024.
45. M. Ossmann, “Software-defined radio for spectrum intelligence applications,” GNU Radio Conference Proceedings, 2022.
46. T. O’Shea and J. Hoydis, “An introduction to deep learning for the physical layer,” IEEE Transactions on Cognitive Communications and Networking, vol. 3, no. 4, pp. 563–575, 2017.
47. GNU Radio Project, GNU Radio Documentation, 2024.
48. ROS2 Documentation Team, ROS2 Humble Documentation, 2024.
49. Microsoft, AirSim Documentation, 2024.
50. Open Robotics, Gazebo Simulator Documentation, 2024.
51. A. Paszke et al., “PyTorch: An imperative style, high-performance deep learning library,” NeurIPS, 2019.
52. M. Abadi et al., “TensorFlow: Large-scale machine learning on heterogeneous systems,” 2016.
53. SDR++ Project Documentation, 2024.
54. Universal Radio Hacker Documentation, 2024.
55. R. Y. Rubinstein and D. Kroese, Simulation and the Monte Carlo Method, 3rd ed. Hoboken, NJ, USA: Wiley, 2016.
56. J. Banks, Discrete-Event System Simulation, 5th ed. Pearson, 2010.
57. D. Helbing, Quantitative Sociodynamics. Dordrecht, Netherlands: Springer, 2010.
58. P. Billingsley, Probability and Measure, 3rd ed. New York, NY, USA: Wiley, 1995.
59. S. Ross, Simulation, 6th ed. New York, NY, USA: Academic Press, 2020.
60. A. Papoulis and S. Pillai, Probability, Random Variables and Stochastic Processes, 4th ed. New York, NY, USA: McGraw-Hill, 2002.
61. G. Casella and R. Berger, Statistical Inference, 2nd ed. Belmont, CA, USA: Duxbury Press, 2002.
62. D. Hall and J. Llinas, Handbook of Multisensor Data Fusion. Boca Raton, FL, USA: CRC Press, 2017.
63. K. Akkaya and M. Younis, “Wireless sensor networks: A survey,” Computer Networks, vol. 38, no. 4, pp. 393–422, 2002.
64. I. Akyildiz et al., “A survey on sensor networks,” IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, 2002.