Secure 3D Drone Localization using Active Watermarked Ranging and Adaptive Swarm Optimization Against AI-Enabled Anchor Spoofing

Vishal Krishna Singh, Neeraj Jain, Chhaya Singh, Nada Alzaben, Rajkumar Singh Rathore and Chaminda Hewage

***Abstract*—Consumer drones and smart IoT devices are increasingly deployed in applications such as autonomous delivery, surveillance, environmental monitoring, indoor asset tracking, and smart-home services. Reliable localization is essential for autonomous navigation, geofencing, return-to-home operation, context-aware services, and safety-critical positioning in these resource-constrained connected devices. However, localization accuracy can be severely degraded by adversarial interference, particularly AI-enabled distance-manipulation and spoofing attacks. Traditional swarm-based optimizers generally perform well under benign conditions but may exhibit significant performance degradation when ranging measurements are intentionally manipulated. This paper proposes a secure localization framework that integrates the Adaptive Superb Fairy-wren Optimization Algorithm (ASFWO) with an Active Watermarked Ranging (AWR) trust mechanism. The proposed ASFWO-AWR framework is designed to enhance attack-resilient localization for consumer autonomous drones, smart-home and edge-IoT devices, indoor location-aware electronics, and delivery or inspection platforms. AWR employs dual-power RSSI watermarking and time-of-arrival dithering to detect anchor-level spoofing and authenticate ranging signals. The resulting trust weights are dynamically incorporated into an adaptive Iteratively Reweighted Least Squares (IRLS)-based position estimator, forming a robust hybrid optimization framework capable of maintaining stable convergence even when a subset of anchors is compromised. Experimental results demonstrate that ASFWO-AWR attains an RMSE of 2.07 m under the low-noise condition and provides improved localization accuracy and robustness compared with conventional PSO and SFOA under challenging measurement conditions.**

***Index Terms*—AI-enabled attacks, drone localization, active watermarked ranging, adaptive swarm optimization, adversarial spoofing.**

I. Introduction

Corresponding Author: Vishal Krishna Singh (E-mail: v.k.singh@essex.ac.uk.), Neeraj Jain (E-mail: neeraj.jain@bennett.edu.in) and Rajkumar Singh Rathore (E-mail: rsrathore@cardiffmet.ac.uk)

Vishal Krishna Singh is with School of Computer Science and Electronics Engineering, University of Essex, Colchester. U.K. (E-mail: v.k.singh@essex.ac.uk.)

Neeraj Jain is with School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India. (e-mail: neeraj.jain@bennett.edu.in).

Chhaya Singh is with School of Computer Science and Engineering, Galgotias University, Greater Noida. India. (e-mail: chhaya.singh@galgotiasuniversity.edu.in).

Nada Alzaben is with Department of Computer Sciences College Of Computer And Information Sciences, Princess Nourah Bint Abdulrahman University, P. O. Box 84428, Riyadh11671, Saudi Arabia. (e-mail: Nialzaben@pnu.edu.sa).

Rajkumar Singh Rathore is with Department of Computer Science, School of Technologies, Cardiff Metropolitan University, United Kingdom. (e-mail: rsrathore@cardiffmet.ac.uk)

Chaminda Hewage is with Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff, United Kingdom. (e-mail: chewage@cardiffmet.ac.uk)

Manuscript received October, 2025.

ACCURATE and secure localization has become a fundamental requirement in modern wireless systems, encompassing Internet of Things (IoT) infrastructures, wireless sensor networks (WSNs), and unmanned aerial vehicle (UAV) swarms. Applications such as autonomous navigation [1], security surveillance [2], precision agriculture [3], aerial mapping [4], industrial automation [5], and disaster response [6], [7], [8], depend critically on the ability of nodes to estimate their positions with high precision and resilience. While satellite based systems such as GPS remain dominant for outdoor positioning, their reliability degrades severely in obstructed, indoor, or urban environments, as well as in adversarial or multipath-dense conditions [9]. From a consumer-electronics perspective, reliable localization is equally important for consumer drones, smart-home and edge-IoT devices, indoor positioning systems, wearables, and asset-tracking platforms. In consumer drones, accurate ranging directly supports autonomous navigation, return-to-home operation, geofencing, obstacle-aware movement, and location-dependent services, while indoor and edge-IoT devices rely on positioning for context-aware automation and proximity-based services. Consequently, corrupted or manipulated ranging information can directly affect device autonomy, operational safety, and the reliability of location-aware functions in resource-constrained connected environments. Consequently, there has been a paradigm shift toward network-centric localization, where UAVs and sensor nodes cooperatively estimate their positions using inter-node measurements such as time of arrival (ToA), time difference of arrival (TDoA), received signal strength (RSS), or angle of arrival (AoA) [9]. Despite significant progress, achieving high localization accuracy under non-line-of-sight (NLOS) propagation, measurement noise, and intentional attacks remains an open challenge.

Localization in UAV networks is fundamentally nonlinear and can become computationally intensive when multiple UAV positions are jointly represented. Classical deterministic solvers, including least squares (LS) [10], weighted least squares (WLS) [11], and semidefinite relaxation (SDR) [12], offer closed-form or convex relaxations but exhibit inadequate robustness to outliers and heightened sensitivity to initial conditions [13]. On the other hand, population-based metaheuristics such as particle swarm optimization (PSO) [14] and genetic algorithms (GA) [15] have emerged as flexible alternatives capable of global search.

Recent studies also emphasize secure localization and measurement integrity under nonlinear and adversarial ranging

conditions [16], where multi-UAV position estimation can become a computationally intensive nonlinear optimization problem. Traditional trust-based localization schemes look to reputation models to identify and remove malicious anchors [17]. Voting and consensus-based methods presented in [18] reduce the effects of spoofing even more by averaging the estimates from several anchors. Most localization methods based on optimization techniques rely on a set of static behavioural parameters during the localization procedure. These fixed parameter values might not be able to adjust successfully to varying network densities, mobility, measurement noise, and malicious environments. In practical UAV-based localization systems, adversaries might introduce noise to the anchors or alter the measurement of the anchors' signals to confuse the localization position estimation. Adversaries can exploit the ranging information by spoofing ranges, replaying beacon signals, spoofing beacon identities, conducting Sybil attacks, spoofing patterns as established by secure localization studies in [19]. Systematic manipulation of the RSS and ToA as well as inter-node distance measurements may significantly affect the estimated location of the UAVs [20].

The proposed framework introduces an active physical-layer trust validation approach together with adaptive optimization to solve adversarial manipulation issues in the localization of UAVs. The AWR module incorporates controlled power offsets and micro-second scale timing dithers in the anchor transmission, generating anchor-specific physical signatures hard to replicate, unlike existing trust-aware schemes based on static reliability scores or higher-layer authentication. The RSS and ToA patterns expected by each UAV are compared with the observed RSS and ToA patterns, in order to calculate a normalized trust coefficient that is used as a continuous reliability index. These trust coefficients are explicitly included in the localization objective so the Adaptive Superb Fairy-Wren Optimization (ASFWO) algorithm works on trust-weighted residuals. After the global optimization, a deterministic refinement stage used is a trust-weighted iteratively reweighted least squares (IRLS) stage. The proposed framework is particularly suitable for resource-constrained consumer drones and edge-IoT devices because continuous trust weighting allows unreliable measurements to be suppressed without requiring repeated network-wide consensus or complete anchor exclusion. Furthermore, the adaptive optimization and lightweight deterministic refinement enable robust localization while limiting unnecessary communication and computational overhead. These characteristics make the proposed framework applicable to connected consumer devices where localization resilience must be balanced against limited processing, energy, and communication resources.

II. System Model

A 3D UAV localization scenario with N_u UAVs and N_a stationary anchors with known positions is considered. The deployment region is modeled as $\mathcal{V} = [0, L_x] \times [0, L_y] \times [0, L_z]$.. UAVs act as mobile receivers, estimating their positions from ranging beacons transmitted by power-controlled, watermarked anchor signals. The wireless channel includes both LOS and NLOS propagation conditions. The true position of UAV u is represented as:

$$\mathbf{x}_u = [x_u,\, y_u,\, z_u]^{\mathrm{T}} \in \mathbb{R}^3, \quad u = 1, 2, \ldots, N_u,$$

and the fixed position of anchor node a by:

$$\mathbf{a}_a = [a_x,\, a_y,\, a_z]^{\mathrm{T}} \in \mathbb{R}^3, \quad a = 1, 2, \ldots, N_a.$$

The geometric distance between UAV u and anchor a is given by:

$$d_{ua} = \|\mathbf{x}_u - \mathbf{a}_a\|_2. \tag{1}$$

In practice, UAVs observe a corrupted distance measurement $\tilde{d}_{ua}$, which deviates from the true distance due to environmental effects and intentional interference. This observation is modeled as:

$$\tilde{d}_{ua} = d_{ua} + n_{ua}^{(\mathrm{L})} + b_{ua}^{(\mathrm{N})} + \xi_{ua}^{(\mathrm{A})}. \tag{2}$$

Here, $n_{ua}^{(L)} \sim \mathcal{N}(0, \sigma_L^2)$ represents measurement noise, while $b_{ua}^{(N)} = 0$ for LOS links and $b_{ua}^{(N)} \sim \mathcal{N}(\mu_N, \sigma_N^2)$ denotes an NLOS bias with positive mean, occurring with probability η_{NLOS}. The term $\xi_{ua}^{(\mathrm{A})}$ represents an AI-enabled adversarial perturbation introduced by attacked anchors through manipulated ranging signals. Motivated by recent reinforcement-learning-based UAV spoofing studies [21], [22], the adversary is modeled as an adaptive policy π_ϕ that generates state-dependent ranging perturbations, $\xi_{ua}^{(\mathrm{A})}(t) = \pi_\phi(\mathbf{s}_{ua}(t))$, where $\mathbf{s}_{ua}(t)$ denotes the available ranging and localization state. The attacker aims to degrade localization accuracy while maintaining covert behavior, subject to the bounded attack constraint $\left|\xi_{ua}^{(\mathrm{A})}(t)\right| \leq \epsilon_a$, where ϵ_a denotes the maximum attack strength. The NLOS probability is controlled by $\eta_{\mathrm{NLOS}} \in [0, 1]$, whereas $\eta_{\mathrm{atk}} \in [0, 1]$ denotes the fraction of attacked anchors. Only anchors in the attacked set $\mathcal{A}_{\mathrm{atk}}$ generate non-zero AI-adaptive perturbations. The attacker may manipulate ranging measurements from attacked anchors, while the anchor-specific AWR secret and watermark generator are assumed to remain protected; full secret-key compromise is outside the scope of this work.

III. Adaptive Superb Fairy-Wren Optimization with Active Watermarked Ranging (ASFWO-AWR)

The proposed ASFWO-AWR framework, illustrated in Fig. 1, combines physical-layer ranging authentication, trust-aware global optimization, and deterministic local refinement to provide robust three-dimensional UAV localization under measurement noise, NLOS propagation, and adversarial ranging manipulation. The proposed framework employs a unified trust-weighted localization objective. Active watermarked ranging first evaluates the reliability of the ranging observations and generates continuous trust coefficients for the participating anchors. These trust coefficients are subsequently incorporated into the fitness function of the adaptive superb fairy-wren optimization algorithm, which performs global position estimation. Finally, the best ASFWO solution is used to initialize a trust-weighted iteratively reweighted least squares procedure for local refinement.

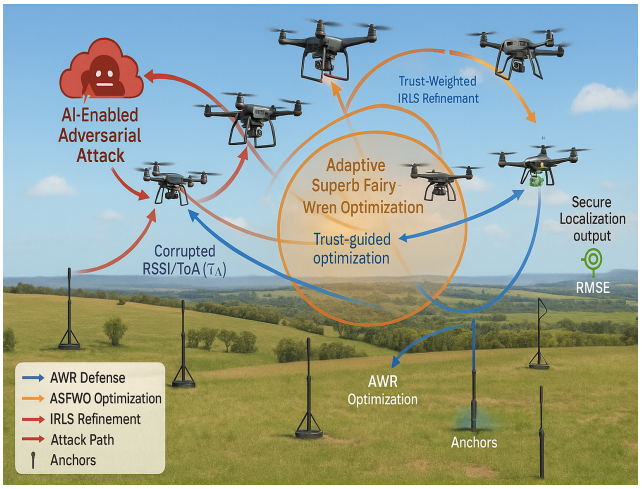


Fig. 1: Framework of ASFWO with AWR System under AI-Enabled Attack

For a candidate UAV position configuration

$$\mathbf{X} = \left[\mathbf{x}_1^T, \mathbf{x}_2^T, \ldots, \mathbf{x}_{N_u}^T\right]^T, \tag{3}$$

the ranging residual associated with UAV u and anchor a is defined as

$$r_{ua}(\mathbf{X}) = \|\mathbf{x}_u - \mathbf{a}_a\|_2 - \tilde{d}_{ua}, \tag{4}$$

where $\tilde{d}_{ua}$ denotes the measured range defined in Section II. The proposed framework minimizes the common trust-weighted robust localization objective:

$$J_\tau(\mathbf{X}) = \sum_{u=1}^{N_u}\sum_{a=1}^{N_a} \tau_a \rho_\delta\left(r_{ua}(\mathbf{X})\right), \tag{5}$$

where $\tau_a \in [0,1]$ represents the AWR-derived trust coefficient of anchor a, and $\rho_\delta(\cdot)$ denotes the Huber robust loss with threshold δ. A trusted anchor therefore contributes normally to the localization objective, whereas an anchor exhibiting an inconsistent watermark signature receives a smaller weight and consequently exerts less influence on the estimated UAV positions. The same residual model and AWR-derived trust coefficients are retained throughout the ASFWO and IRLS stages, thereby providing a continuous optimization process from ranging authentication to final position refinement.

A. Secure Ranging and Trust Computation using AWR

In practical airspaces, range observations can be biased by NLOS propagation, multipath, and intermittent interference. More critically, an adversary may manipulate ranging packets or replay previously observed beacons to induce systematic localization drift. For this reason, the proposed framework introduces an active watermarked ranging stage that evaluates the consistency of anchor transmissions at the physical layer before the measurements enter the localization optimizer.

1) Watermark Generation and Embedding: Each anchor a transmits a pair of ranging beacons in a challenge-response form: a low-power pulse P_{low}, followed by a high-power pulse satisfying

$$P_{\text{high}} = P_{\text{low}} + \Delta P, \tag{6}$$

where the transmitted powers are expressed on a logarithmic scale and ΔP denotes a known power offset, typically selected within the range of 3–6 dB.

In addition to the dual-power signature, the anchor introduces a microsecond-scale timing watermark by incorporating a pseudo-random dither sequence into the beacon transmission schedule. The dither is generated by a lightweight pseudo-random generator using an anchor-specific secret assumed to remain protected from the adversary. The corresponding UAV can therefore reproduce the expected dither sequence, whereas an external adversary without access to the secret value cannot reliably predict the timing signature. The watermark parameters are selected sufficiently above the receiver resolution and normal timing uncertainty while remaining small enough to avoid degrading the underlying ranging accuracy.

2) Watermark Detection at the UAV: Let the received powers of the two pulses at UAV u be P'_{low} and P'_{high}, and let their corresponding received timestamps be t'_1 and t'_2. The consistency of the received watermark is evaluated using the RSS and ToA deviations

$$\Delta RSS_{ua} = \left(P'_{\text{high}} - P'_{\text{low}}\right) - \Delta P, \tag{7}$$

and

$$\Delta ToA_{ua} = (t'_2 - t'_1) - \delta_a[n]. \tag{8}$$

Here, $\delta_a[n]$ denotes the expected pseudo-random inter-pulse timing interval for the current watermark instance. The timing check detects replay or substitution attempts that do not preserve this interval, while common-delay real-time relay attacks are outside the present threat model. Under benign conditions, ΔRSS_{ua} remains close to zero because the expected power difference is preserved subject to channel and receiver noise. Similarly, ΔToA_{ua} remains small when the received inter-pulse timing is consistent with the expected watermark interval. Larger deviations indicate possible manipulation, stale replay, signal substitution, or inconsistency with the current ranging watermark.

3) Parameter Normalization and Trust Mapping: The power offset ΔP is selected to provide sufficient distinguishability between the high and low power pulses under fading and receiver quantization without introducing excessive transmission overhead. Similarly, the timing dither amplitude is selected above the timestamp resolution and normal timing jitter but remains sufficiently small relative to the operating range and ToA dynamics.

Because RSS and ToA measurements exhibit different scales, the deviations are normalized using

$$\overline{\Delta RSS}_{ua} = \frac{|\Delta RSS_{ua}|}{\sigma_{RSS} + \epsilon_0}, \qquad \overline{\Delta ToA}_{ua} = \frac{|\Delta ToA_{ua}|}{\sigma_{ToA} + \epsilon_0}, \tag{9}$$

where σ_{RSS} and σ_{ToA} denote empirical noise scales obtained during calibration and ϵ_0 prevents division by zero. The normalized RSS and ToA deviations are aggregated across the UAV observations to obtain an anchor-level consistency score

$$S_a = \frac{1}{N_u}\sum_{u=1}^{N_u}\left(\overline{\Delta RSS}_{ua} + \overline{\Delta ToA}_{ua}\right). \tag{10}$$

The corresponding anchor trust coefficient is then obtained using

$$\tau_a = \frac{1}{1+\exp[k(S_a-\theta)]}, \tag{11}$$

where k controls the sensitivity of the trust mapping and θ denotes the decision midpoint. Moderate deviations therefore reduce the trust value gradually, which avoids excessive penalization due to temporary fading or measurement jitter, whereas persistent large deviations drive τ_a toward zero.

The output of the AWR stage is thus the set of trust coefficients

$$\boldsymbol{\tau} = \{\tau_1, \tau_2, \ldots, \tau_{N_a}\}. \tag{12}$$

These coefficients are directly used as the measurement weights

$$w_{ua} = \tau_a \tag{13}$$

in the unified objective $J_\tau(\mathbf{X})$ defined in (5). Consequently, AWR does not independently estimate UAV positions; instead, it determines how strongly each anchor measurement contributes to the subsequent optimization process.

B. Trust-Weighted Adaptive Superb Fairy-Wren Optimization

Once the AWR trust scores are obtained, the system transitions to the global position-estimation stage driven by Adaptive Superb Fairy-Wren Optimization. ASFWO extends the original SFOA metaheuristic by introducing diversity-aware parameter control to balance global exploration and local exploitation. ASFWO performs global search over the joint multi-UAV localization vector using the trust-weighted nonlinear ranging objective.

Each candidate wren represents a complete candidate UAV position configuration,

$$\mathbf{X}_i = \left[\mathbf{x}_{1,i}^T, \mathbf{x}_{2,i}^T, \ldots, \mathbf{x}_{N_u,i}^T\right]^T \in \mathbb{R}^{3N_u}. \tag{14}$$

Unlike a conventional optimizer operating only on geometric ranging error, each ASFWO candidate is evaluated using the AWR-weighted objective introduced in (5):

$$J_\tau(\mathbf{X}_i) = \sum_{u=1}^{N_u}\sum_{a=1}^{N_a} \tau_a \rho_\delta\left(\|\mathbf{x}_{u,i}-\mathbf{a}_a\|_2 - \tilde{d}_{ua}\right). \tag{15}$$

Thus, the physical-layer integrity assessment obtained from AWR is propagated directly into the global search. A candidate position that fits measurements from a suspicious low-trust anchor does not receive the same fitness benefit as a candidate that remains geometrically consistent with trusted anchors.

At iteration t, ASFWO evaluates the diversity of the current population using

$$D_t = \frac{1}{d}\sum_{j=1}^{d}\frac{\mathrm{std}\left(X_{:,j}^{(t)}\right)}{U_j - L_j}, \tag{16}$$

where $d = 3N_u$ is the search dimension and L_j and U_j denote the lower and upper bounds of the jth decision variable.

The probabilities associated with young-forager exploration, feeding exploitation, and avoidance diversification are adapted as

$$p_y = p_{y0} + 0.3\left(\frac{H_{\mathrm{ref}} - D_t}{H_{\mathrm{ref}}}\right), \tag{17}$$

$$p_f = p_{f0} - 0.2\left(\frac{H_{\mathrm{ref}} - D_t}{H_{\mathrm{ref}}}\right), \tag{18}$$

and

$$p_a = 1 - (p_y + p_f), \tag{19}$$

where H_{ref} denotes the reference diversity level. The resulting probabilities are restricted to valid probability bounds and normalized when required so that

$$0 \le p_y, p_f, p_a \le 1, \qquad p_y + p_f + p_a = 1. \tag{20}$$

The adaptive probability mechanism changes the relative frequency of the three behavioral operators according to the current population diversity and thereby reduces reliance on fixed behavioral parameters during the complete search process.

For each wren i, one of the following three position-update operators is selected probabilistically:

$$\mathbf{X}_i' = \begin{cases} \mathbf{X}_i + \alpha\mathbf{z}_i + 0.5(\mathbf{X}_{g1} - \mathbf{X}_{g2}) + 0.1(\mathbf{E}_j - \mathbf{X}_i), & \text{Young-forager (explore),} \\ \mathbf{X}_i + \beta\exp\left(-\dfrac{\|\mathbf{X}_i - \mathbf{E}_j\|_2^2}{\sigma^2}\right)(\mathbf{E}_j - \mathbf{X}_i) + \boldsymbol{\varepsilon}_i, & \text{Feeding (exploit),} \\ \mathbf{X}_i + \zeta\mathbf{z}_i + \zeta(\mathbf{X}_i - \overline{\mathbf{X}}), & \text{Avoidance (diversify),} \end{cases} \tag{21}$$

where $\mathbf{E}_j$ denotes an elite wren, $\mathbf{X}_{g1}$ and $\mathbf{X}_{g2}$ denote randomly selected peer solutions, $\overline{\mathbf{X}}$ denotes the population mean, and $\mathbf{z}_i \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_d)$ represents a d-dimensional Gaussian perturbation. The term $\boldsymbol{\varepsilon}_i$ represents a small stochastic perturbation used during feeding exploitation. The young-forager behavior combines random exploration, peer-difference information, and mild elite attraction, thereby allowing candidate solutions to explore new regions of the search space. The feeding behavior emphasizes movement toward an elite solution and therefore supports local exploitation. The avoidance mechanism introduces an additional diversity component based on the displacement of a candidate from the current population mean. The corresponding scaling parameters are adapted according to

$$\alpha \leftarrow \alpha\gamma, \qquad \beta \leftarrow \beta\sqrt{\gamma}, \tag{22}$$

and

$$\zeta \leftarrow \zeta_0\left(1 + \frac{1}{1+\exp[10(D_t - 0.12)]}\right), \tag{23}$$

where γ denotes the decay factor. The decay of α and β progressively reduces the magnitude of exploratory and elite-directed movements as optimization proceeds, while ζ remains diversity-dependent. Together with the adaptive behavior probabilities, these updates provide a gradual transition from broad population search toward solution refinement. After a new candidate $\mathbf{X}_i'$ is generated, it is projected onto the feasible localization region,

$$\mathbf{X}_i' \leftarrow \Pi_{\mathcal{V}^{N_u}}(\mathbf{X}_i'), \tag{24}$$

and greedily accepted when

$$J_\tau(\mathbf{X}_i') < J_\tau(\mathbf{X}_i). \tag{25}$$

The global ASFWO stage terminates after the maximum number of iterations or another specified convergence criterion. The best population member is then selected as

$$\mathbf{X}_{\mathrm{ASFWO}} = \arg\min_{\mathbf{X}_i} J_\tau(\mathbf{X}_i). \tag{26}$$

ASFWO therefore provides a globally competitive solution while already suppressing the contribution of measurements associated with low AWR trust. However, residual position errors may remain due to nonlinear ranging geometry, measurement noise, and the stochastic nature of population-based optimization. For this reason, $\mathbf{X}_{\mathrm{ASFWO}}$ is passed directly to the deterministic IRLS refinement stage.

C. Trust-Weighted IRLS Refinement

The best ASFWO solution is used as the initial condition of the trust-weighted IRLS estimator:

$$\mathbf{X}^{(0)} = \mathbf{X}_{\mathrm{ASFWO}}. \tag{27}$$

The purpose of this stage is not to solve a separate localization problem but to locally refine the ASFWO estimate using the same geometric residuals and AWR-derived trust information defined in (4)–(5). At IRLS iteration t, the residual corresponding to UAV u and anchor a is

$$r_{ua}^{(t)} = \left\| \mathbf{x}_u^{(t)} - \mathbf{a}_a \right\|_2 - \tilde{d}_{ua}. \tag{28}$$

The refinement therefore continues to minimize the unified robust objective given in (5). During the IRLS stage, the AWR trust scores are held fixed for the current localization epoch, whereas the robust statistical weights are recomputed from the residuals. For the Huber loss, the corresponding residual-dependent weight is

$$\psi(r) = \frac{\rho'(r)}{r} = \begin{cases} 1, & |r| \le \delta, \\ \dfrac{\delta}{|r|}, & |r| > \delta. \end{cases} \tag{29}$$

The effective weight associated with each UAV-anchor measurement therefore becomes

$$\omega_{ua}^{(t)} = \tau_a \psi\left(r_{ua}^{(t)}\right), \tag{30}$$

which combines two complementary forms of robustness. The AWR term τ_a limits the influence of measurements with suspicious physical-layer signatures, whereas $\psi(r_{ua}^{(t)})$ limits the influence of observations producing unusually large geometric residuals. The residual vector is linearized around the current estimate $\mathbf{X}^{(t)}$. Let $\mathbf{J}^{(t)}$ denote the corresponding Jacobian and

$$\mathbf{W}^{(t)} = \mathrm{diag}\left(\omega_{ua}^{(t)}\right) \tag{31}$$

denote the effective weighting matrix. The damped weighted least-squares update is obtained from

$$\left[\mathbf{J}^{(t)T}\mathbf{W}^{(t)}\mathbf{J}^{(t)} + \lambda_d \mathbf{I}\right] \Delta\mathbf{X} = -\mathbf{J}^{(t)T}\mathbf{W}^{(t)}\mathbf{r}^{(t)}, \tag{32}$$

where $\lambda_d \ge 0$ denotes the damping coefficient used to improve numerical stability under ill-conditioned geometry. The UAV position estimate is then updated as

$$\mathbf{X}^{(t+1)} = \mathbf{X}^{(t)} + \Delta\mathbf{X}. \tag{33}$$

Convergence and Stopping Criteria: With AWR trust scores fixed during each localization epoch, IRLS performs a damped robust Gauss–Newton refinement. Low-trust measurements are suppressed by τ_a, while large residuals are further down-weighted by the Huber function, providing both security- and residual-aware robustness. Under bounded weights, smooth residuals, and a locally well-conditioned $\mathbf{J}^T\mathbf{W}\mathbf{J}$, the damped update approaches a local stationary solution. IRLS terminates when either

$$\frac{\left|J_\tau\left(\mathbf{X}^{(t+1)}\right) - J_\tau\left(\mathbf{X}^{(t)}\right)\right|}{J_\tau\left(\mathbf{X}^{(t)}\right) + \epsilon_0} \le \epsilon_F, \tag{34}$$

or

$$\left\|\Delta\mathbf{X}\right\|_2 \le \epsilon_X, \tag{35}$$

or when the maximum iteration limit is reached. In the experiments, convergence typically occurred within 5–12 iterations.

Algorithm 1 Proposed ASFWO-AWR Secure 3D Localization Framework

Require: Anchors $\mathcal{A}$, measured ranges $\tilde{d}_{ua}$, RSS/ToA observations, bounds $(\mathbf{L}, \mathbf{U})$, population N_p, iterations T, AWR parameters, ASFWO parameters, Huber threshold δ, IRLS parameters $(\lambda_d, \epsilon_F, \epsilon_X, R)$.
Ensure: Estimated UAV positions $\widehat{\mathbf{X}}$.

Phase 1: AWR Trust Computation
for $a = 1, \ldots, N_a$ **do**
  for $u = 1, \ldots, N_u$ **do**
    Compute ΔRSS_{ua} and ΔToA_{ua} using Eqs. (7)–(8)
    Normalize deviations using Eq. (9)
  end for
  Compute anchor consistency score S_a using Eq. (10)
  Obtain trust τ_a using Eq. (11)
end for
Define the trust-weighted objective $J_\tau(\mathbf{X})$ using Eq. (5)
Phase 2: Trust-Weighted ASFWO
Initialize $\mathbf{X}_i^{(0)} \sim \mathcal{U}(\mathbf{L}, \mathbf{U})$, $i = 1, \ldots, N_p$
Evaluate $F_i^{(0)} = J_\tau(\mathbf{X}_i^{(0)})$
Initialize $\alpha = \alpha_0$, $\beta = \beta_0$, $\zeta = \zeta_0$
for $t = 0, \ldots, T-1$ **do**
  Rank population and construct elite set $\mathcal{E}^{(t)}$
  Compute diversity D_t using Eq. (16)
  Update and normalize (p_y, p_f, p_a) using Eqs. (17)–(20)
  for $i = 1, \ldots, N_p$ **do**
    Draw $r \sim \mathcal{U}(0,1)$
    if $r < p_y$ **then**
      Generate $\mathbf{V}_i$ using the young-forager operator in Eq. (21)
    else if $r < p_y + p_f$ **then**
      Generate $\mathbf{V}_i$ using the feeding operator in Eq. (21)
    else
      Generate $\mathbf{V}_i$ using the avoidance operator in Eq. (21)
    end if
    Project $\mathbf{V}_i \leftarrow \Pi_{\mathcal{V}^{N_u}}(\mathbf{V}_i)$
    if $J_\tau(\mathbf{V}_i) < J_\tau(\mathbf{X}_i^{(t)})$ **then**
      $\mathbf{X}_i^{(t+1)} \leftarrow \mathbf{V}_i$
    else
      $\mathbf{X}_i^{(t+1)} \leftarrow \mathbf{X}_i^{(t)}$
    end if
  end for
  Update α, β, and ζ using Eqs. (22)–(23)
end for
$\mathbf{X}_{\mathrm{ASFWO}} \leftarrow \arg\min_i J_\tau(\mathbf{X}_i^{(T)})$
Phase 3: Trust-Weighted IRLS
$\mathbf{X}^{(0)} \leftarrow \mathbf{X}_{\mathrm{ASFWO}}$
for $r = 0, \ldots, R-1$ **do**
  Compute residuals $r_{ua}^{(r)}$ using Eq. (28)
  Compute $\omega_{ua}^{(r)} = \tau_a \psi(r_{ua}^{(r)})$ using Eqs. (29)–(30)
  Construct $\mathbf{W}^{(r)}$ and Jacobian $\mathbf{J}^{(r)}$
  Solve the damped IRLS system in Eq. (32)
  $\mathbf{X}^{(r+1)} \leftarrow \mathbf{X}^{(r)} + \Delta\mathbf{X}$
  if $\dfrac{|J_\tau(\mathbf{X}^{(r+1)}) - J_\tau(\mathbf{X}^{(r)})|}{J_\tau(\mathbf{X}^{(r)}) + \epsilon_0} \le \epsilon_F$ **or** $\|\Delta\mathbf{X}\|_2 \le \epsilon_X$ **then**
    break
  end if
end for
Phase 4: Output
$\widehat{\mathbf{X}} \leftarrow \mathbf{X}^{(r+1)}$
return $\widehat{\mathbf{X}}$

IV. Results and Discussion

A. Experimental Setup

The experiments are conducted in an identified region of $100 \times 100 \times 50$ m^3. To ensure spatial diversity, anchor nodes

are considered to be placed on the perimeter and the UAV positions are initialized randomly within the volume. The altitude values are drawn from a bounded range representative of low-altitude flight, allowing controlled height variation across trials. The key simulation parameters and environmental settings are summarized in Table I.

For adversarial evaluation, the attacked-anchor ratio η_{atk} is varied from 0 to 30%, and only anchors belonging to $\mathcal{A}_{\mathrm{atk}}$ inject manipulated ranging measurements. Two attack conditions are considered: constant-bias spoofing and RL-inspired adaptive spoofing, with the latter adapted from [22] to the considered ranging-domain state variables. The experiments are performed using stationary anchors and independent UAV localization realizations; hence, the reported results represent quasi-static rather than continuous trajectory-based attack scenarios. For AWR evaluation, benign RSS/ToA watermark observations are perturbed by the calibrated measurement noise, whereas attacked observations include watermark-inconsistent RSS/ToA perturbations associated with the spoofed ranging measurements.

TABLE I: Simulation Parameters

Parameter	Value
Number of drones / unknown nodes	50
LOS noise standard deviation	1.0 m
NLOS bias / standard deviation	2.0 m, 1.5 m
Attack ratio, η_{atk}	0–30%
Attack bias / ϵ_a	8–12 m / 12 m
RSS watermark offset, ΔP	3 dB
Trust sensitivity, k	2
Trust midpoint, θ	1
Trust threshold, τ_{th}	0.5
p_{y0}, p_{f0}, p_{a0}	0.42, 0.43, 0.15
β_0, γ	0.82, 0.997
Reference diversity, H_{ref}	1.0
IRLS Huber threshold, δ	2.0
IRLS regularization	10^{-3}

B. Results and Analysis

The proposed ASFWO–AWR is compared with SFOA [23] and PSO [24] in simulated 3D UAV localization scenarios, as illustrated in Fig. 2. Environmental uncertainty is modeled using additive noise and randomized NLOS conditions for each Monte Carlo trial. To emulate spoofing attacks, a random subset of anchors is compromised and injects bounded ranging perturbations. While PSO and SFOA may converge toward biased solutions under corrupted measurements, ASFWO–AWR incorporates AWR-based trust scores to suppress attacked anchors and preserve localization consistency. For a given attack ratio, a subset of anchor nodes is uniformly selected from the anchor set in each trial, thereby avoiding bias toward specific anchor geometries. For a given trial m, root mean square error (RMSE) is defined as:

$$\mathrm{RMSE}^{(m)} = \sqrt{\frac{1}{N_u}\sum_{u=1}^{N_u}\left\|\hat{\mathbf{x}}_u^{(m)} - \mathbf{x}_u\right\|_2^2}, \tag{36}$$

where $\hat{\mathbf{x}}_u^{(m)}$ denotes the estimated position of UAV u in trial m, and $\mathbf{x}_u$ represents its true position. To assess the statistical reliability of the reported localization accuracy, the mean RMSE is evaluated over multiple independent trials and reported with a 95% confidence interval (CI). In addition to average RMSE, a success rate metric is used to quantify convergence reliability. A localization trial is considered *successful* if the final RMSE satisfies a predefined accuracy threshold ϵ. Formally,

$$\mathcal{S}^{(k)} = \begin{cases} 1, & \text{if } \mathrm{RMSE}^{(k)} \le \epsilon, \\ 0, & \text{otherwise.} \end{cases} \tag{37}$$

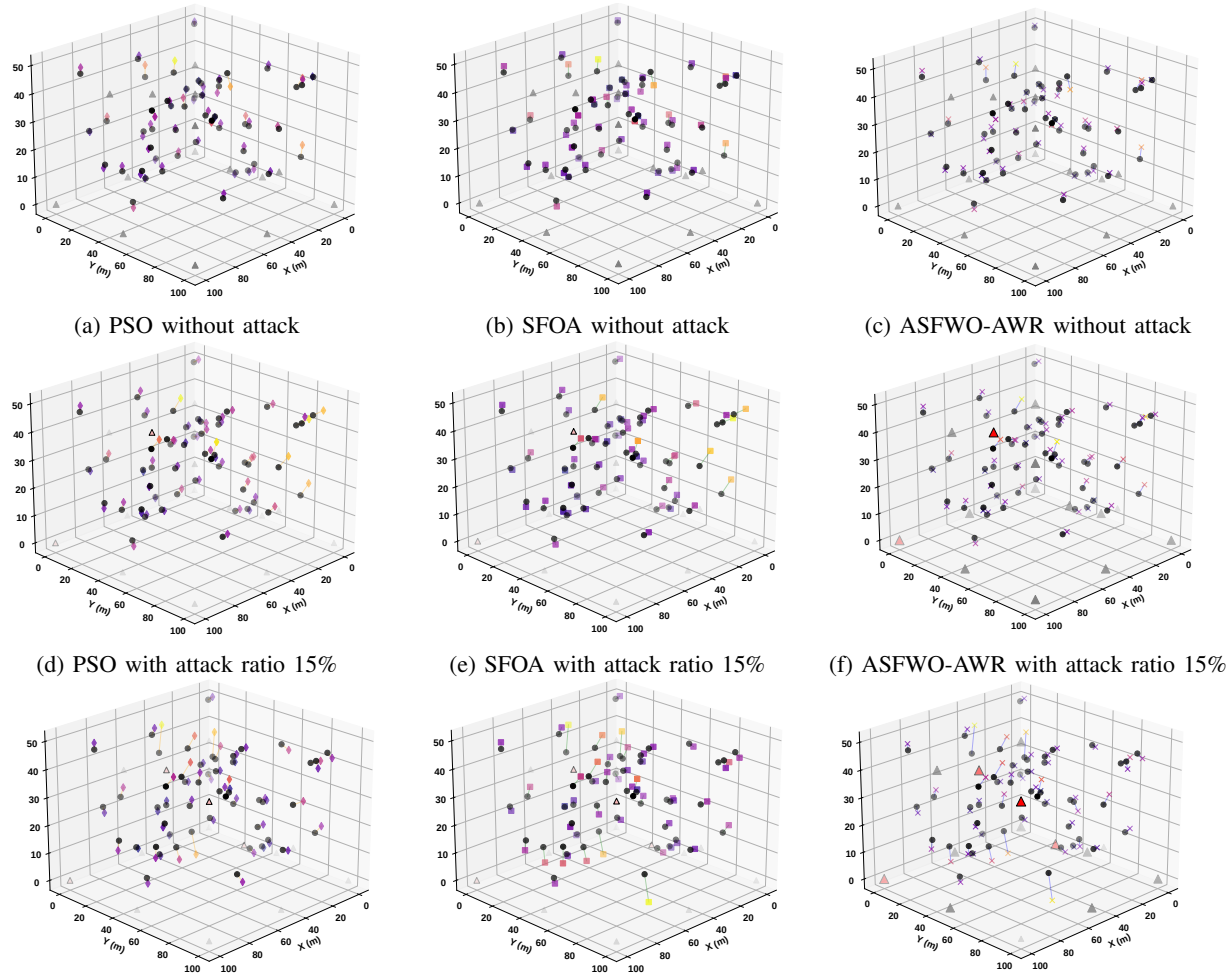
In this work, the threshold is set to $\epsilon = 3\,\mathrm{m}$, which reflects acceptable localization accuracy for low-altitude UAV navigation and the considered multi-UAV localization scenario. The overall success rate is computed across $K = 50$ independent Monte Carlo trials as:

$$\text{Success Rate}(\%) = \frac{1}{K}\sum_{k=1}^{K}\mathcal{S}^{(k)} \times 100. \tag{38}$$

1) Localization Accuracy and Robustness: It is observed from Table II that under the attack-free condition, ASFWO-AWR achieves an RMSE of 2.51 m, lower than PSO and SFOA. The excellent success rate of 98% achieved by the proposed ASFWO-AWR further illustrates its convergence stability and good adaptation to the changing channel conditions. From 0% to 30% attacked anchors, RMSE increases by approximately 60.2% for ASFWO-AWR, compared with 69.7% for PSO and 83.3% for SFOA. At an NLOS ratio of 0.3, ASFWO-AWR achieves an RMSE of 2.99 m and maintains a success rate above 92%. The proposed method exhibits good noise-tolerant properties even at high noise level $\sigma = 5$ with an RMSE of 6.03 m, while for SFOA and PSO it was 6.76 m and 6.74 m, respectively.

To quantify resistance to adversarial degradation, the robustness score is computed as the ratio of attack-free RMSE to RMSE under a given attack ratio, expressed as a percentage. A higher robustness score indicates better preservation of localization accuracy under attack. At a 30% attacked-anchor ratio, ASFWO–AWR achieves 62.4%, compared with 58.9% for PSO and 54.6% for SFOA.

2) Convergence Behavior and Optimization Efficiency: Convergence analysis evaluates the number of iterations required to approach a stable solution. The convergence iteration is defined as the first iteration at which the relative change in the objective function satisfies $|J^{(t+1)} - J^{(t)}|/(J^{(t)} + \epsilon_0) \le \epsilon_c$. The performance comparison, as shown in Fig. 3a, highlights the convergence paths of the proposed ASFWO-AWR and baseline optimizers. The proposed ASFWO-AWR exhibits faster convergence and smoother late-stage stabilization in the reported trials. ASFWO-AWR approaches a stable fitness value within approximately 50 iterations, compared with about 65 iterations for SFOA and 80 iterations for PSO. This acceleration is due to adaptive mechanism implemented by the proposed ASFWO-AWR, which dynamically changes its exploration-exploitation coefficients (α, β, ζ) depending on the diversity of the population. When diversity decreases, p_y and the diversity-dependent ζ promote exploration, whereas higher diversity increases the relative feeding probability p_f. Meanwhile, α and β decay progressively to support later-stage refinement.



(a) PSO without attack (b) SFOA without attack (c) ASFWO-AWR without attack

(d) PSO with attack ratio 15% (e) SFOA with attack ratio 15% (f) ASFWO-AWR with attack ratio 15%

(g) PSO with attack ratio 30% (h) SFOA with attack ratio 30% (i) ASFWO-AWR with attack ratio 30%

Fig. 2: Comparative visualization of the proposed ASFWO-AWR localization method under different attack ratios. ● : $True\ position$, ▲ : $Anchor(Red - Attacked)$, ♦ : PSO, ■ : $SFOA$, × : $ASFWO - AWR$

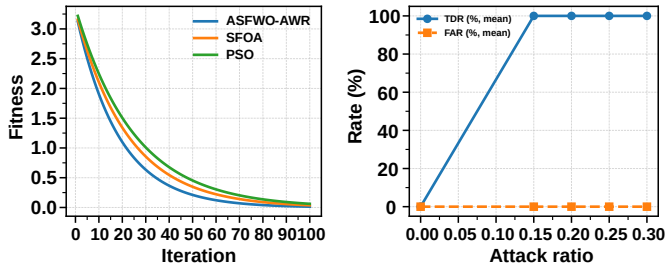
TABLE II: Comparative Performance of ASFWO-AWR under Different Experimental Conditions (mean ± 95% CI)

Scenario/ Parameter	RMSE (m)			Success (%)			Time (s)			Remarks
	PSO	SFOA	ASFWO-AWR	PSO	SFOA	ASFWO-AWR	PSO	SFOA	ASFWO-AWR	
Anchor Node Variation										
10	3.60±0.42	3.48±0.39	**2.73±0.21**	69.33±4.6	68.67±4.9	**75.33±3.1**	2.11±0.18	2.78±0.21	3.40±0.26	Stable convergence with low variance.
20	2.58±0.31	2.37±0.28	**2.17±0.17**	84.67±3.2	85.33±3.0	**89.33±2.4**	2.62±0.22	3.64±0.29	4.89±0.34	Higher anchor density reduces variance.
30	2.56±0.29	2.35±0.27	**2.15±0.16**	84.67±3.4	85.66±3.1	**90.33±2.3**	2.44±0.21	3.15±0.26	5.08±0.37	Consistent performance with limited dispersion.
40	2.50±0.26	2.31±0.24	**2.10±0.15**	85.33±3.0	86.00±2.8	**90.66±2.1**	2.17±0.19	3.34±0.27	4.91±0.35	Anchor-rich setup stabilizes all methods.
Attack Impact (Malicious Nodes)										
0%	2.61±0.25	2.63±0.24	**2.51±0.18**	96.00±1.9	96.00±2.0	**98.00±1.2**	2.29±0.20	3.17±0.25	5.12±0.36	Stable under clean conditions.
15%	2.91±0.38	2.65±0.34	**2.53±0.22**	93.33±3.2	95.33±2.7	**95.66±2.3**	2.23±0.19	3.18±0.26	4.83±0.33	Robust against mild attacks.
20%	3.48±0.56	3.50±0.61	**2.89±0.33**	84.67±5.1	85.33±4.8	**87.00±3.7**	2.35±0.20	3.35±0.27	4.90±0.31	Mitigates moderate attack impact.
25%	4.43±0.72	4.82±0.79	**3.89±0.41**	73.33±6.4	70.66±6.9	**78.80±4.2**	2.45±0.22	3.58±0.30	5.00±0.34	Lower variance than baselines.
30%	4.43±0.75	4.82±0.81	**4.02±0.46**	73.33±6.7	70.66±7.1	**78.80±4.5**	2.59±0.24	3.63±0.32	5.10±0.36	Resilient under high attack rates.
NLOS Ratio Variation										
0.0	2.41±0.23	2.35±0.22	**2.16±0.16**	97.33±1.6	97.33±1.7	**98.66±1.1**	2.46±0.21	3.28±0.27	5.27±0.38	Robust in LOS conditions.
0.05	2.87±0.36	2.69±0.33	**2.56±0.25**	92.00±3.4	94.66±3.0	**94.66±2.5**	2.15±0.19	3.22±0.26	4.82±0.34	Low sensitivity to NLOS.
0.1	2.90±0.39	2.63±0.35	**2.52±0.27**	93.33±3.2	95.33±2.8	**95.33±2.4**	2.31±0.20	3.08±0.25	4.97±0.36	Stable across mixed links.
0.2	3.14±0.44	2.80±0.38	**2.77±0.29**	89.33±3.9	92.66±3.4	**93.00±2.6**	2.02±0.17	3.43±0.25	5.08±0.33	Graceful degradation.
0.3	3.48±0.51	3.19±0.46	**2.99±0.34**	88.00±4.2	90.66±3.8	**92.33±2.9**	2.45±0.22	3.37±0.28	5.22±0.37	Maintains robustness.
Population Size Variation										
20	2.94±0.35	2.64±0.31	**2.55±0.24**	92.00±3.6	94.66±3.1	**95.33±2.5**	0.48±0.05	0.71±0.07	0.93±0.09	Larger populations reduce variance.
40	2.88±0.33	2.66±0.30	**2.58±0.26**	92.66±3.4	93.33±3.2	**94.66±2.7**	1.06±0.09	1.68±0.14	3.17±0.26	Improved convergence stability.
60	2.90±0.34	2.63±0.31	**2.56±0.25**	92.66±3.5	94.67±3.0	**95.33±2.4**	1.55±0.13	2.57±0.21	4.76±0.38	Stable with moderate cost.
80	2.90±0.36	2.63±0.32	**2.56±0.26**	92.66±3.6	94.67±3.1	**95.33±2.6**	1.93±0.16	3.07±0.25	4.07±0.33	Consistent performance.
100	3.06±0.39	2.64±0.33	**2.57±0.28**	92.66±3.8	93.33±3.4	**95.33±2.7**	2.28±0.19	3.51±0.29	7.31±0.52	Trade-off between cost and stability.
Measurement Noise Variation (σ)										
0.1	2.58±0.27	2.36±0.24	**2.07±0.18**	94.00±2.8	94.00±2.7	**96.66±2.1**	2.28±0.20	3.09±0.26	5.30±0.39	Noise-tolerant regime.
0.5	2.61±0.29	2.39±0.26	**2.30±0.21**	94.66±2.6	95.33±2.4	**96.00±2.0**	2.55±0.22	3.02±0.25	4.59±0.34	Stable under moderate noise.
1.0	2.91±0.35	2.64±0.31	**2.52±0.24**	93.33±3.1	94.33±2.8	**95.67±2.3**	2.20±0.19	3.19±0.27	5.15±0.38	Graceful degradation.
3.0	4.62±0.68	4.48±0.63	**4.07±0.51**	66.67±6.2	71.33±5.8	**72.67±4.7**	2.56±0.23	3.04±0.26	5.06±0.37	Robust under severe noise.
5.0	6.74±0.92	6.76±0.95	**6.03±0.74**	38.67±7.1	42.00±6.8	**43.33±5.6**	2.23±0.21	3.19±0.28	5.15±0.41	High-noise stress test.

3) Security-Aware Performance Analysis: The AWR model employs dual-signal watermarking in the ranging process which generates a trust value for each anchor node, reflecting the consistency of differences in *RSSI* and *ToA*. In case of an attack, these disparities grow larger, resulting in a decrease in trust levels. As a result, the fitness function of the ASFWO gets modified with trust-weighted IRLS updates. The attack detection performance of AWR is quantified using the True Detection Rate (TDR) and False Alarm Rate (FAR):

$$\mathrm{TDR} = \frac{TP}{TP+FN} \times 100, \qquad \mathrm{FAR} = \frac{FP}{FP+TN} \times 100. \quad (39)$$

For detection evaluation, an anchor is classified as suspicious when its trust coefficient satisfies $\tau_a < \tau_{\mathrm{th}}$, where $\tau_{\mathrm{th}} = 0.5$. At an attacked-anchor ratio of 30%, the TDR of AWR is still close to 100%, and FAR is less than 2%. The results in Fig. 3b show that AWR detects attacked anchors while maintaining a low false-alarm rate for benign anchors.



(a) Convergence curves for ASFWO, SFOA, and PSO.

(b) Trust detection metrics (TDR/FAR) for ASFWO-AWR.

Fig. 3: Performance evaluation of the proposed ASFWO-AWR framework: (a) convergence behavior and (b) trust detection performance.

4) Computational Complexity and Resource Feasibility for Consumer Devices: The computational cost of ASFWO-AWR mainly arises from ASFWO fitness evaluation, AWR trust computation, and IRLS refinement. Its average execution time is 4.9 s, compared with 3.3 s for SFOA and 2.6 s for PSO, while average CPU utilization is 63%, versus 71% and 78%, respectively. The dominant computational complexity is $\mathcal{O}(TN_pN_uN_a)$, while AWR introduces $\mathcal{O}(N_uN_a)$ ranging and trust-observation as communication overhead per localization epoch. The memory requirement is approximately $\mathcal{O}(3N_pN_u + N_uN_a + N_a)$. Simulation-based analysis indicates differing computational-energy requirements; hardware-level energy consumption remains to be experimentally validated.

These results suggest suitability for resource-constrained UAV and edge-IoT platforms. However, the reported 4.9 s runtime represents complete software simulation rather than per-update localization latency, and the energy values are simulation-based estimates. Hardware-level latency, memory footprint, update rate, and energy consumption therefore require practical validation.

V. Conclusion

This paper presented ASFWO-AWR, a secure and resilient 3D UAV localization framework that integrates AWR-based trust assessment, adaptive metaheuristic optimization, and IRLS refinement. The proposed approach improves localization reliability under measurement noise, NLOS propagation, and adversarial ranging manipulation. The adaptive search mechanism of ASFWO maintains an effective exploration-exploitation balance, while AWR-derived trust weights and IRLS refinement suppress unreliable and malicious measurements. Simulation results demonstrate that ASFWO-AWR consistently outperforms PSO and SFOA in localization accuracy, convergence, and attack resilience. At a 20% attacked-anchor ratio, the proposed framework achieves an RMSE of 2.89 m and an 87% localization success rate, corresponding to an RMSE reduction of approximately 15–17% over the baseline methods. The framework also maintains robust performance under varying noise, NLOS, and attack conditions. These results indicate the potential of ASFWO-AWR for secure localization in consumer UAVs, UAV-assisted WSNs, and edge-IoT systems where GPS may be unreliable or unavailable. Full compromise of the protected AWR secret remains outside the present threat model. Future work will focus on embedded UAV implementation, dynamic attack scenarios, adaptive watermark selection, large-scale swarm evaluation, and hardware-level assessment of latency, memory, communication overhead, and energy consumption.

Acknowledgments

This work was supported by the Princess Nourah Bint Abdulrahman University Researchers Supporting Project number PNURSP2026R733.

References

[1] M. S. Hossain, M. Rahman, A. Rahman, M. M. Kabir, M. Mridha, J. Huang, and J. Shin, "Automatic navigation and self-driving technology in agricultural machinery: A state-of-the-art systematic review," *IEEE Access*, 2025.

[2] V. K. Singh, N. Anand, S. Krishna Sharma, Anjali, M. K. Shukla, R. S. Rathore, and W. Jiang, "Low-light image enhancement for edge-based security surveillance in 6g-iot visual systems," *IEEE Internet of Things Journal*, pp. 1–1, 2025.

[3] S. Mansoor, S. Iqbal, S. M. Popescu, S. L. Kim, Y. S. Chung, and J.-H. Baek, "Integration of smart sensors and iot in precision agriculture: trends, challenges and future prospectives," *Frontiers in Plant Science*, vol. 16, p. 1587869, 2025.

[4] M. Raj, N. Harshini, S. Gupta, M. Atiquzzaman, O. Rawlley, and L. Goel, "Leveraging precision agriculture techniques using uavs and emerging disruptive technologies," *Energy Nexus*, vol. 14, p. 100300, 2024.

[5] N. Jain, V. K. Singh, C. Singh, G. Tripathi, R. S. Rathore, and D. Chaudhary, "Noise-resilient deep learning architecture for bearing fault diagnosis in integrated iot sensing–computing environments," *IEEE Transactions on Consumer Electronics*, pp. 1–1, 2025.

[6] V. K. Singh, D. Agarwal, V. K. Gediya, R. S. Rathore, and W. Jiang, "Mitigating class imbalance in forest fire prediction with gan-augmented data fusion," *Information Fusion*, p. 104005, 2025.

[7] A. Banerjee, S. K. Gupta, and V. Kumar, "A genetic algorithm-based approach for collision avoidance in a multi-uav disaster mitigation deployment," *Concurrency and Computation: Practice and Experience*, vol. 37, no. 9-11, p. e70061, 2025.

[8] V. K. Singh, C. Singh, and H. Raza, "Event classification and intensity discrimination for forest fire inference with iot," *IEEE Sensors Journal*, vol. 22, no. 9, pp. 8869–8880, 2022.

[9] N. Jain, C. Singh, V. K. Singh, R. S. Rathore, N. S. Alghamdi, and C. Hewage, "Federated genetic optimization for secure and privacy-preserving sensor localization in consumer iot applications," *IEEE Transactions on Consumer Electronics*, pp. 1–1, 2025.

[10] B. Tausiesakul and K. Asavaskulkiet, "Tdoa localization in wireless sensor networks using constrained total least squares and newton's methods," *IEEE Access*, vol. 12, pp. 39 238–39 260, 2024.

[11] L.-F. Shi, R. Zeng, F. Jing, and Y. Shi, "Weighted least-squares bluetooth localization method based on data preprocessing," *IEEE Internet of Things Journal*, vol. 11, no. 23, pp. 38 291–38 300, 2024.

[12] R. Zheng, G. Wang, and K. Ho, "Accurate semidefinite relaxation method for elliptic localization with unknown transmitter position," *IEEE Transactions on Wireless Communications*, vol. 20, no. 4, pp. 2746–2760, 2020.

[13] A. Zaeemzadeh, M. Joneidi, B. Shahrasbi, and N. Rahnavard, "Robust target localization based on squared range iterative reweighted least squares," in *2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*. IEEE, 2017, pp. 380–388.

[14] N. Gunawardena, K. K. Leang, and E. Pardyjak, "Particle swarm optimization for source localization in realistic complex urban environments," *Atmospheric Environment*, vol. 262, p. 118636, 2021.

[15] O. D. Jegede and K. Ferens, "A genetic algorithm for node localization in wireless sensor networks," in *Proceedings of the International Conference on Genetic and Evolutionary Methods (GEM)*. The Steering Committee of The World Congress in Computer Science, Computer . . . , 2013, p. 1.

[16] V. K. Singh, N. Anand, A. Pal, A. Chowdhury, and A. Srivastava, "Anomaly detection in dynamic graphs using multiple encoding strategies via transformers," *IEEE Transactions on Consumer Electronics*, vol. 71, no. 2, pp. 5173–5188, 2025.

[17] S. M. Nagarajan, G. G. Devarajan, M. S. Thangakrishnan, T. Ramana, A. K. Bashir, and A. A. AlZubi, "Artificial intelligence-based zero trust security approach for consumer industry," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 3, pp. 5411–5418, 2024.

[18] S. Tomic, M. Beko, D. Vukobratovic, and S. Krco, "Voting scheme to strengthen localization security in randomly deployed wireless sensor networks," *arXiv preprint arXiv:2502.20218*, 2025.

[19] S. Srivastava, D. Agarwal, B. K. Chaurasia, V. K. Singh, R. S. Rathore, and W. Jiang, "Federated blockchain-based resilient identity management for securing consumer vehicular networks," *IEEE Transactions on Consumer Electronics*, 2025.

[20] V. K. Chaurasiya, N. Jain, and G. C. Nandi, "A novel distance estimation approach for 3d localization in wireless sensor network using multi dimensional scaling," *Information Fusion*, vol. 15, pp. 5–18, 2014.

[21] X. Ma, M. Gao, Y. Zhao, and M. Yu, "A novel navigation spoofing algorithm for uav based on gps/ins-integrated navigation," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 10, pp. 15 424–15 439, 2024.

[22] X. Ma, T. Sun, and M. Gao, "A reinforcement-learning-enhanced spoofing algorithm for uav with gps/ins-integrated navigation," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 61, no. 4, pp. 8659–8673, 2025.

[23] H. Jia, X. Zhou, J. Zhang, and S. Mirjalili, "Superb fairy-wren optimization algorithm: a novel metaheuristic algorithm for solving feature selection problems," *Cluster Computing*, vol. 28, no. 4, p. 246, 2025.

[24] Z. Zhang, Q. Dong, and W. Wang, "Adapsca-pso: An adaptive localization algorithm with ai-based hybrid sca-pso for iot wsns," *arXiv preprint arXiv:2507.22317*, 2025.



Vishal Krishna Singh received his PhD degree in Information Technology from Indian Institute of Information Technology, Allahabad, India in 2018. He is currently working as a Lecturer and is associated with the Networks and Communications Research Group at School of Computer Science and Electronics Engineering, University of Essex, Colchester, U.K. His research interests include Internet of Things, Wireless Sensor Networks, In-Network Inference, Machine Learning and Data Analytics.



Neeraj Jain received his PhD degree in Information Technology from Indian Institute of Information Technology, Allahabad, India in 2018. He is currently working as an Associate Professor at School of Computer Science Engineering and Technology, Bennet University, Greater Noida, India. His research interests include Federated Learning, Machine Learning, Internet of Things, Wireless Sensor Networks, and Localization Protocols.



Chhaya Singh is an Associate Professor in the School of Computer Science and Engineering at Galgotias University, India. She received her Ph.D. from MANIT Bhopal and M.Tech. from IIIT Allahabad. Her research interests include Machine Learning, Data Science, and Fuzzy Logic. Dr. Singh has also worked as a Research Assistant on a GCRF-funded project in collaboration with the University of Essex, UK. She has received multiple research fellowships and the Young Scientist Award for her contributions to computational biology.



Nada Alzaben became a Member (M'18) of IEEE in 2018. She is currently working on her Ph.D. in computer science at Southern Methodist Univ., Dallas, TX, USA. Her research interests include network communications, routing and scheduling, network performance analysis. She is a Lecturer in computer science and information college at Princess Nourah Bint Abdulrahman Univ., Riyadh, Saudi Arabia.



Rajkumar Singh Rathore (Senior Member IEEE) is working as Head of Cyber Security of Connected and Autonomous Systems in Department of Computer Science at Cardiff Metropolitan University's School of Technologies, United Kingdom. His research expertise are Wireless Communications, Internet of Things/Cyber Physical Systems, Cyber Security and Privacy, Connected and Autonomous Vehicles, EV Charging Infrastructure Management, Intelligent Networking of Drones and also use cases of AI/ML.



Chaminda T. E. R. Hewage (Senior Member, IEEE) received Ph.D. degree from the University of Surrey, U.K., in 2008. His doctoral research focused on perceptual quality–driven 3D video over networks at the Centre for Communication Systems Research. He has been with Cardiff Metropolitan University since 2015, where he is a Reader in Data Security and the founding Director of the Cybersecurity and Information Networks Centre. His research interests include data security, QoE, QoSec, multimedia communications, and data visualization.