A Reliable and Resilient Framework for Multi-UAV Mutual Localization

Zexin Fang*, Bin Han* and Hans D. Schotten*†
*Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau (RPTU), Kaiserslautern, Germany
†German Research Center of Artificial Intelligence (DFKI), Kaiserslautern, Germany

***Abstract*—This paper presents a robust and secure framework for achieving accurate and reliable mutual localization in multiple unmanned aerial vehicle (UAV) systems. Challenges of accurate localization and security threats are addressed and corresponding solutions are brought forth and accessed in our paper with numerical simulations. The proposed solution incorporates two key components: the Mobility Adaptive Gradient Descent (MAGD) and Time-evolving Anomaly Detectio (TAD). The MAGD adapts the gradient descent algorithm to handle the configuration changes in the mutual localization system, ensuring accurate localization in dynamic scenarios. The TAD cooperates with reputation propagation (RP) scheme to detect and mitigate potential attacks by identifying UAVs with malicious data, enhancing the security and resilience of the mutual localization.**

***Index Terms*—Coordinated attack, UAV, Gradient descend, Mutual localization.**

I. Introduction

Multi-UAV systems hold significant promise for revolutionizing various domains, particularly the future Sixth Generation (6G). For instance, multi-UAV systems have the potential to provide reliable communication links in challenging environments, support connectivity in remote or disaster-stricken areas, and overcome limitations of ground infrastructure [**?**].

In UAV applications, Global Positioning System (GPS) modules may face challenges in providing precise position information in urban areas, tunnels, or environments with obstacles. Alternative options like radio trilateration can be used but have limited coverage and require calibration and installation cost [**?**][**?**]. A mutual position system utilizing anchor UAVs with accurate GPS positions can provide precise estimates for target UAVs with poor GPS reception. Distance estimation methods such as Time of Flight (ToF) or Received Signal Strength Indicator (RSSI) ranging can be used in this system.

Existing localization research primarily addresses terrestrial scenarios in static networked sensors, often lacking altitude considerations. However, the uneven distribution of anchor UAVs in three dimensions adds complexity to localization algorithms. Additionally, in multi-UAV mutual localization, the mobility of UAVs introduces variations in reliable position and distance information. Therefore, comprehensive research and novel methodologies are necessary to tackle these challenges [**?**]. On top of that, security is also a critical concern in multi-UAV mutual localization. While extensive research has been done on security in static sensor networks [**?**][**?**][**?**], its validation in dynamic scenarios is lacking. The changing topology of target UAVs and malicious UAVs can significantly impact the performance of attack and defense schemes. Further investigation is needed to validate the performance and robustness of these schemes for dynamic multi-UAV mutual localization scenarios.

This work demonstrates a robust and secure framework that ensures accurate and reliable mutual localization while addressing potential security threats. The subsequent sections of the paper are structured as follows. In Sec.II we investigate the error model of our scenario. In Sec.III we introduce our proposed methodologies, meanwhile, evaluate the overall efficiency and accuracy of the mutual localization system in the specific scenario under consideration. Then in SecIV we outline the potential attack scheme and proposed defend scheme (TAD), and validate our proposed scheme with numerical simulations presented in Sec.V. In Sec.VI, we conclude our paper by summarizing the key findings.

II. Error model setup

A. Distance estimation error

Considering the limited range and sensitivity to environmental conditions of ToF ranging, a better approach that suits our scenario is RSSI ranging. This method relies on a path loss model to establish a relationship between the RSSI value and the distance of a radio link from an anchor UAV. Such a model can be described as:

$$P_{\mathrm{r}}(d) = P_{\mathrm{r}}(d_0) - 10n_{\mathrm{p}} * \log(\frac{d}{d_0}), \tag{1}$$

where $P_{\mathrm{r}}(d)$ indicates the RSSI value at the distance d from the anchor UAV; d_0 is the predefined reference distance, meanwhile $P_{\mathrm{r}}(d)$ is the RSSI measurement value at d_0; n_p denotes the path loss factor of the radio link.

Regarding the fact that a radio channel suffers from different forms of fading, therefore RSSI measurement error $P_{\mathrm{r}}^{\Delta}(d)$ is inevitable and will result in a distance estimation error $\mathcal{E}$. We investigated RSSI measurement results between two Zigbee nodes [**?**] [**?**] and Sigfox nodes [**?**]. $P_{\mathrm{r}}^{\Delta}(d)$ is zero-mean Gaussian distributed with a standard deviation $\sigma_{\mathrm{r}}(d)$. However, in the case of small distances, $\sigma_{\mathrm{r}}(d)$ shows a weak relation to the distance, which indicates fading dominates over path loss in this range. We consider an outdoor urban environment with NLOS (Non-Line of sight) radio links, which is quite common in our use case, thus $P_{\mathrm{r}}^{\Delta}(d)$ is likely to be fluctuating in a same manner. To simplify our analysis, the standard deviation $\sigma_{\mathrm{r}}(d, \mathrm{t})$ is considered to be randomly and uniformly

distributed, meanwhile subjected to the square of the distance to approximate measurement results, as described follows:

$$P_{\mathrm{r}}^{\Delta}(d,\mathrm{t}) \sim \mathcal{N}\left(0, \sigma_{\mathrm{r}}(d,\mathrm{t})^2\right) \tag{2}$$

$$\sigma_{\mathrm{r}}(d,\mathrm{t}) \sim \gamma_d * \mathcal{U}\left(\sigma_{\min}^{r}, \sigma_{\max}^{r}\right) \tag{3}$$

$$\gamma_d = S * d^2 + 1 \tag{4}$$

where γ_d is the modification factor, which modifies the relation between distance and $\sigma_{\mathrm{r}}(d,\mathrm{t})$; S is the scaling factor, which is to scale how strong is γ_d subjected to d.

Assume a pass loss model with pass loss factor $n_{\mathrm{p}} = 3$, reference distance $d_0 = 1$ and RSSI measurement value $P_{\mathrm{r}}(d_0) = -30\mathrm{dBm}$, while $\sigma_{\min}^{r} = 0.5$, $\sigma_{\max}^{r} = 2$ and $S = 0.0001$. The simulation of such a model is shown in Fig. 1.

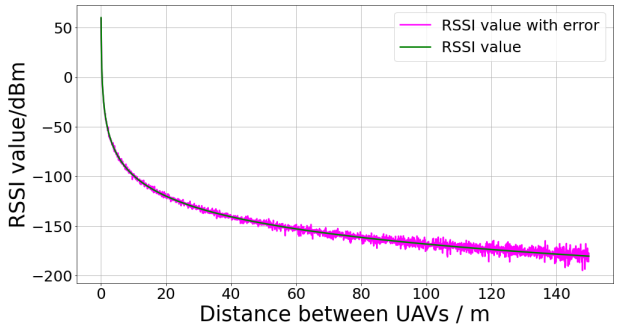


Fig. 1. Simulated RSSI value over distance

By applying error to $P_{\mathrm{r}}(d)$ and find the corresponding distance of errored RSSI value, we are able to estimate the distance error $\mathcal{E}(d)$ over the distance, simulation results are presented in Fig. 2

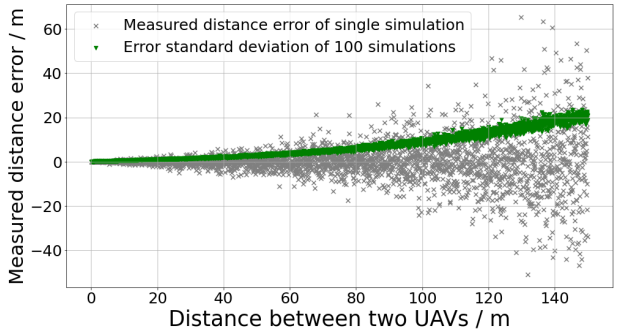


Fig. 2. Estimation error and standard deviation over distance between 2 UAVs

The simulation results shows that distance estimation error $\mathcal{E}(d)$ is zero mean Gaussian distributed with $\mathcal{E}(d) \sim (0, \sigma_d^2(d))$, while $\sigma_d(d)$ fluctuates but increases over the distance. However, based on the simulation results, distance estimation over 150 can be extremely unreliable. Additionally, the communication cost can be drastically increased as more anchor UAVs are exposed to the target UAV.

B. Position measurement error

For a set of anchor UAVs $\mathcal{U} = \{u_0, u_1, \dots u_{\mathrm{n}}\}$, each UAV has an error of its position, typically caused by various factors. With the assumption that the GPS module of UAV mitigated many of these error factors, we limited the GPS error to the Gussian error caused by the measurement. The actual position $\mathrm{p}_n(t)$ and its pseudo position $\mathrm{p^{\circ}}_n(t)$ at time step t of the n_{th} UAV can be described :

$$\mathrm{p}_n(t) = [x_n(t), y_n(t), z_n(t)] \tag{5}$$

$$\mathrm{p^{\circ}}_n(t) = \mathrm{p}_n(t) + [x_n^{\Delta}(t), y_n^{\Delta}(t), z_n^{\Delta}(t)] \tag{6}$$

$$[x_n^{\Delta}(t), y_n^{\Delta}(t), z_n^{\Delta}(t)] \sim \mathcal{N}^2\left(0, \sigma_{\mathrm{p},n}^2/3\right) \tag{7}$$

$$\sigma_{\mathrm{p},n} \sim \mathcal{U}\left(\sigma_{\min}^{p}, \sigma_{\max}^{p}\right) \tag{8}$$

where $[x_n^{\Delta}(t), y_n^{\Delta}(t), z_n^{\Delta}(t)]$ is position measurement error, which can be described by a zero mean Gaussian distribution with standard deviation $\sigma_{\mathrm{p},n}$. $\sigma_{\mathrm{p},n}$ is considered to be random uniform distributed. Within a valid coverage of mutual localization, a target UAV $u_k \in \mathcal{U}$ measures the distance from anchor UAVs. The real distance $d_{k,n}$ and measured distance $d_{k,n}^{\circ}$ can be described as follows :

$$d_{k,n} = \|\mathrm{p}_k(t) - \mathrm{p}_n(t)\| \tag{9}$$

$$d_{k,n}^{\circ} = d_{k,n} + \mathcal{E}(d_{k,n}, t) \tag{10}$$

III. Adaptive and Robust Mutual Localization

A. Introduction to different localization techniques

Thorough studies have been conducted focusing on distance-based localization techniques. We focus on 3 different localization techniques: least square (LS) based localization, $l1$ norm (LN-1) based localization, and gradient descend (GD) based localization, to investigate their localization performance in the presence of uneven spatial distribution of anchor UAVs. These techniques have been widely recognized for their robustness and efficiency in sensor network scenarios [**?**][**?**].

Given the measured distance $d_{k,n}^{\circ}$ of anchor UAVs and their positions $\mathrm{p^{\circ}}_n$, the position of u_k can be estimated by minimizing the error between measured distance and calculated distance, as described follows:

$$\mathrm{p}_k = \arg\min_{[x,y,z]} \sum_{n=0}^{N} \left| \|\mathrm{p^{\circ}}_n - \mathrm{p}_k\| - d_{k,n}^{\circ} \right|. \tag{11}$$

This optimization problem can be directly solved by LS technique with,

$$[x_k, y_k, z_k, \|\mathrm{p}_k\|^2]^{\mathrm{T}} = (\mathrm{A}^{\mathrm{T}}\mathrm{A})^{-1}\mathrm{Ab} \tag{12}$$

where A and b are matrices containing anchor position and measured distances information,

$$A = \begin{Bmatrix} -2x_0 & -2y_0 & -2z_0 & 1 \\ \vdots & \vdots & \vdots & 1 \\ -2x_n & -2y_n & -2z_n & 1 \end{Bmatrix} \mathrm{b} = \begin{Bmatrix} d^{\circ 2}_{k,0} - \|\mathrm{p}_0^{\circ}\|^2 \\ \vdots \\ d^{\circ 2}_{k,n} - \|\mathrm{p}_n^{\circ}\|^2 \end{Bmatrix}$$

Moreover, such a localization problem can be formulated as a plane fitting problem, where the objective is to find

a 4D plane $W = f(x, y, z)$ that fits the measurements A and b. The coefficients of the plane can be represented as $u = [x_k, y_k, z_k, \|\mathrm{p}_k\|^2]^{\mathrm{T}}$. The optimization can be performed by minimizing the $l1$ norm-based distance metric [**?**].

$$\begin{aligned} &\min_{u,w} \|w\|_1 \\ &\text{subject to } \mathrm{A}u - w = \mathrm{b} \end{aligned} \tag{13}$$

And u can be solved iteratively by using Alternating Direction Method of Multiplier (ADMM) steps,

$$\begin{aligned} u^i &= \mathrm{G}\mathrm{A}^{\mathrm{T}}(b + u^{i-1} - \frac{\lambda^{i-1}}{\rho}) \\ w_k &= S_{\frac{1}{\rho}}(\mathrm{A}u^{i-1} - b + \frac{\lambda^{i-1}}{\rho}) \\ \lambda^i &= \lambda^{i-1} + \rho(\mathrm{A}u^i - w^i - b) \end{aligned} \tag{14}$$

where $\mathrm{G} = (\mathrm{A}^{\mathrm{T}}\mathrm{A})^{-1}$, λ is the Lagrange multiplier and ρ is the penalty parameter for violating the linear constraint. Meanwhile, $S_{\frac{1}{\rho}}$ is the soft threshold function in $l1$ norm, defined as $S_{\frac{1}{\rho}} = \mathrm{sign}(x) * \max(|x| - \frac{1}{\rho}, 0)$.

Eq. 11 can be also reformulated as $\mathrm{p}_k = \arg\min_{[x,y,z]} f(x, y, z)$. By applying gradient descent to cost function $f(x, y, z)$, we are able to estimate the position $\hat{\mathrm{p}}_k$ of u_k iteratively. At the i_{th} iteration, the negative gradient g^i and position $\hat{\mathrm{p}}_k$ can be calculated,

$$g^i = -\nabla_{(x,y,z)}(f(x, y, z))|_{(x=\hat{x}_k^{i-1}, y=\hat{y}_k^{i-1}, z=\hat{z}_k^{i-1})} \tag{15}$$

$$\hat{\mathrm{p}}_k^i = \hat{\mathrm{p}}_k^{i-1} + \alpha^i \times \frac{g^i}{||g^i||} \tag{16}$$

where $\hat{\mathrm{p}}_k^{i-1}$ is the estimated position at the $(i-1)_{th}$ iteration. α^i is the step size at the i_{th} iteration. α^i can be adjusted by discount factor β to prevent over-descending.

The computational complexity of the three above-introduced techniques is summarized in Tab. III-A [**?**].

TABLE I
COMPUTATIONAL COMPLEXITY

LS	LN-1	GD
$\mathcal{O}(N^2)$	$\mathcal{O}(\max(K_{\mathrm{ADMM}}N, N^2))$	$\mathcal{O}(K_{\mathrm{GD}}N)$

B. Performance evaluation under uneven spatial distribution

For UAV applications, energy consumption is a critical concern. To compare the LS, LN-1, and GD localization techniques under energy-limited conditions, we set $K_{\mathrm{ADMM}} = N$ and $K_{\mathrm{GD}} = N$ to ensure equal computational complexity for all three approaches. In the simulation, the target UAV u_k is surrounded by anchor UAVs distributed within a cubic area. The shape of this cubic area varies, ranging from $[x_k \pm 35.35, y_k \pm 35.35, z_k \pm 1]$ to $[x_k \pm 29.29, y_k \pm 29.29, z_k \pm 28]$ to keep a maximum $d_{k,n} = 50$. The RSSI error model configured as shown in Fig. 1, and simulation is set up as follows: $N = 30$, $[\sigma^p_{\min}, \sigma^p_{\max}] = [0.1, 3]$ and $\rho = 0.1$, $[\alpha^0, \beta] = [1, 0.5]$. Each

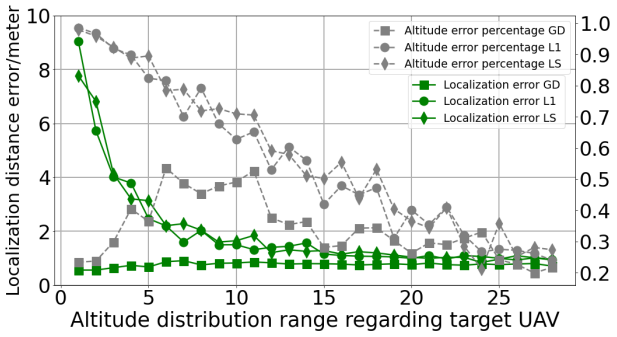


Fig. 3. Localization error over spatial distribution

estimation was repeated 50 times to exclude randomness. The results are presented in Fig. 3.

The simulation results show that the error of LS based and LN-1 based localization decreases as the distribution of anchor UAVs becomes more even in terms of latitude, longitude, and altitude. However, the error in GD based localization is not significantly affected by the distribution of anchor UAVs. Specifically, when anchor UAVs are densely distributed in one dimension compared to the other two dimensions, LS and LN-1 localization techniques can become highly unreliable in the densely distributed dimension. In contrast, GD based localization doesn't show a strong correlation with the distribution of anchor UAVs in this regard. In summary, GD based localization is better suited for scenarios involving multiple UAVs, where the distribution of UAVs may be uneven in all three dimensions.

C. Weighted localization and error conversion

To speed up the convergence of gradient descent and ensure the stability of localization, a weighted localization approach can be proposed, as described below:

$$\hat{\mathrm{p}}_k = \arg\min_{[x,y]} \sum_{n=0}^{N} \left| \|\mathrm{p}_n^\circ - \mathrm{p}\| - d_{k,n}^\circ \right| * w_n^e \tag{17}$$

where w_n^e is the error weight of anchor UAVs, which can be determined by the distance estimate error $\mathcal{E}$ and position measurement error power $\sigma_{\mathrm{p},n}$. To calculate the error weight, we can convert the position measurement error to the distance estimate error, as illustrated in Fig. 4.

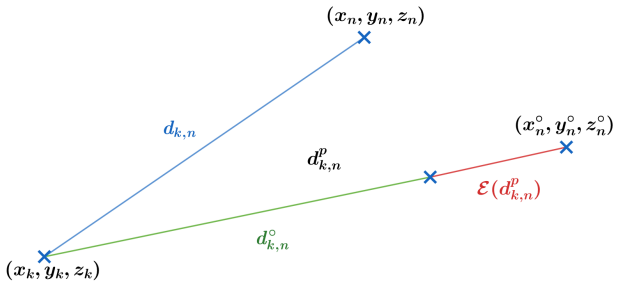


Fig. 4. Position and distance estimation error conversion

For an anchor UAV u_n with actual position $[x_n, y_n, z_n]$ and measured position $[x_n^\circ, y_n^\circ, z_n^\circ]$, $d_{k,n}$ is the actual distance and

$d^{\circ}_{k,n}$ is the measured distance. $d^{p}_{k,n}$ is the erred distance solely caused by position error. $\mathcal{E}(d^{p}_{k,n})$ is the converted distance estimation error jointly caused by position measurement and distance estimate. $\mathcal{E}(d^{p}_{k,n})$ can be approximated by a non-zero mean Gaussian distribution, as introduced in [**?**]. Such converted distance estimate error can described as $\mathcal{E}_{cd} \sim \mathcal{N}(\mu_{\mathrm{cd}}, \sigma_{\mathrm{cd}})$. Nevertheless, $\sigma_{\mathrm{d}}(d_{k,n})$ can't be directly retrieved with a single measurement of $d^{\circ}_{k,n}$. With the approximation $\sigma_{\mathrm{d}}(d_{k,n}) \leftarrow \sigma_{\mathrm{d}}(d^{\circ}_{k,n})$, $d^{\circ}_{k,n} \leftarrow d_{k,n} + \mu_{cd}$ and known $\sigma_{\mathrm{p},n}$, $[\mu_{\mathrm{cd}}, \sigma_{\mathrm{cd}}]$ can be obtained through least squares estimation. Error weight can be calculated as $w^{e}_{n} = \frac{\sum_{u_n \in \mathcal{U}} \sigma_{\mathrm{c},n}}{n * \sigma_{\mathrm{c},n}}$.

D. Mobility adaptive gradient descent Algorithm

An appropriate initial step size α^0 is crucial for gradient descent-based estimation. Conventional approaches with fixed initial step sizes may not perform optimally in our scenario. To tackle this issue, we can use adaptive step sizes that dynamically adjust at each stage based on the changing speed of the target UAV u_k and the availability of anchor UAVs.

A mobility adaptive gradient descent algorithm can be designed, as shown in Alg III.1. Step size is initialized in lines 5-6 with the given thresholds ($\epsilon^{\max}_{\mathrm{t}_0}$ and $\epsilon^{\min}_{\mathrm{t}_0}$) at the beginning. As the localization error is initially large, a larger $\hat{\alpha}$ is used for stability. Lines 7-18 perform a gradient descent-based estimation using the previous position estimate (to guarantee a good convergence within K) and information from anchor UAVs. Momentum m stabilizes gradient descent, while discount factor β_1 reduces step size within each estimation. $\bar{D}_i$ represents the average distance difference between $\hat{d}_n$ and d°_n, serving as an indicator of over-descending. Convergence threshold θ_t and max iteration threshold K are used to terminate iterations. Lines 21-23 estimate current speed $V(t)$, average speed $\bar{V}$, and average distance difference $\bar{\bar{D}}$. The current distance difference $\bar{D}(t)$ can deviate due to occasional mis-localization, but a consistently enlarging $\bar{D}(t)$ suggests a small $\hat{\alpha}$, which results in a gradual loss of position accuracy. When $\hat{\alpha}$ is small, $\mathrm{p}(t)$ remains close to the previous estimate, resulting in a small estimated $V(t)$. In lines 27-29, a smoothing window of length ϕ is applied to the estimates to mitigate fluctuations, and a modification factor ρ is determined conjunctively by $V(t)$ and $D(t)$ to modify $\bar{\alpha}$. Lines 24-28 adapt the learning rate based on stability and speed. When the position estimation is stable (indicated by $\bar{D}(t)$ shows no significant deviation), $\hat{\alpha}$ is reduced by β_2 and $\bar{V}$ to ensure good accuracy. The minimum threshold of $\hat{\alpha}$ is determined by $\epsilon^{\min}_{\mathrm{t}_0}$ and $\bar{V}$. If the estimation is not stable, $\hat{\alpha}$ is increased by ρ.

E. Accuracy estimation of mutual localization system

We access the robustness and accuracy of MAGD through simulations with varying numbers of anchor UAVs and fixed step sizes, and then compare the simulation results based on MAGD. The movement speed of u_k is periodically changed to simulate real mobility. Anchor UAVs u_n are randomly initialized within a cubic area around target UAV u_k. The system configuration is summarized in Tab II.

Algorithm III.1: Mobility adaptive gradient descend algorithm

1 Input: $\hat{\mathrm{p}}(0) = \hat{\mathrm{p}}_{init}$; discount factor β_1 and β_2; step size threshold $\epsilon^{\max}_{\mathrm{t}_0}$, $\epsilon^{\min}_{\mathrm{t}_0}$; maximum iteration, convergence threshold and momentum: K, θ, m; Simulation time T
2 Output: $\hat{\mathrm{p}}(t)$
3 **Function** MAGD($t = 1 : T$) **is**
4 **if** $t = 1$ **then**
5 $\hat{\alpha} \leftarrow \max(\frac{\epsilon^{\max}_{\mathrm{t}_0}}{n}, \epsilon^{\min}_{\mathrm{t}_0})$
6 update: $\hat{\mathrm{p}} \leftarrow \hat{\mathrm{p}}(t-1)$; $\bar{D}_0 \leftarrow +\infty$
7 **for** $i = 1 : I$ **do**
8 **for** $n = 1 : N$ **do**
9 get $\mathrm{p}^{\circ}_n, \sigma_{\mathrm{p},n}, d^{\circ}_n$ from u_n
10 get $\mu_{\mathrm{c},n}, \sigma_{\mathrm{c},n}$ `// Error conversion`
11 $w^{e}_{n} \leftarrow \frac{\sum_{u_n \in \mathcal{U}} \sigma_{\mathrm{c},n}}{n * \sigma_{\mathrm{c},n}}$ `// Calculate error weight`
12 $\hat{d}_n = \|\hat{\mathrm{p}} - \mathrm{p}^{\circ}_n\|$
13 $G^i \leftarrow \sum_{u_n \in \mathcal{U}} \frac{(\hat{\mathrm{p}} - \mathrm{p}^{\circ}_n) * w^{e}_{n}}{\hat{d}_n} * (\hat{d}_n - d^{\circ}_n + \mu_{c,n})$ `// Gradient`
14 update: $\hat{\mathrm{p}} \leftarrow \hat{\mathrm{p}} + m * \hat{\mathrm{p}} + \frac{\hat{\alpha}}{n} * \frac{G^i}{\|G^i\|}$; $\hat{d}_n$ $\bar{D}_i \leftarrow \frac{1}{n} * \sum_{u_n \in \mathcal{U}} (\hat{d}_n - d^{\circ}_n + \mu_{c,n}) * w^{e}_{n}$
15 **if** $\bar{D}_i > \bar{D}_{i-1}$ **then**
16 $\hat{\alpha} \leftarrow \hat{\alpha} * \beta_1$ `// reduce step size`
17 **else if** $\frac{\bar{D}_{i-1} - \bar{D}_i}{\bar{D}_i} <= \theta$ **then**
18 break
19 update: $\hat{\mathrm{p}}(t) \leftarrow \hat{\mathrm{p}}$; $\bar{D}(t) \leftarrow \bar{D}_i$;
20 $V(t) \leftarrow \|\hat{\mathrm{p}}(t) - \hat{\mathrm{p}}(t-1)\|$ `// Estimate speed`
21 $\bar{V} \leftarrow \frac{1}{t} \sum_{t=1}^{t} V(t)$ `// Estimated average speed`
22 $\bar{\bar{D}} \leftarrow \frac{1}{t} \sum_{t=1}^{t} D(t)$ `// Average distance difference`
23 **if** $t < \Phi$ **then**
24 $\phi = t$
25 **else if** $t >= \Phi$ **then**
26 $\phi = \Phi$
27 $\rho_D \leftarrow \frac{\sum_{t=t-\phi}^{t} \bar{D}(t)}{(t=t-\phi) * \bar{D}}$ `// Apply smooth window`
28 $\rho_V \leftarrow \frac{\sum_{t=t-\phi}^{t} V(t)}{(t=t-\phi) * \bar{V}}$
29 $\rho \leftarrow \sqrt{\frac{\rho_D}{\rho_V}}$ `// Modification factor`
30 **if** $t \neq 1$ & $\frac{|\bar{D}(t) - \bar{\bar{D}}|}{\bar{\bar{D}}} <= 0.5$ **then**
31 $\hat{\alpha} \leftarrow \hat{\alpha} - \beta_2 * \bar{V}$ `// Reduce step size`
32 $\hat{\alpha} \leftarrow \max(\hat{\alpha}, \max(\frac{\epsilon^{\min}_{\mathrm{t}}}{n}, \frac{\bar{V}}{2}))$
33 **if** $t \neq 1$ & $\rho > 1.5$ **then**
34 $\hat{\alpha} \leftarrow \hat{\alpha} * \rho$ `// Enlarge step size`

TABLE II
SIMULATION SETUP 1

	Parameter	Value	Remark
System	n_a	$5 \sim 40$	Anchor UAVs
	$\sigma^2_{\mathrm{p},n}$	$\sim \mathcal{U}(0.1, 3.0)$	Position error power / m^2
	$\bar{V}$	$\sim \mathcal{U}(0.6, 3.4)$	Travel speed $\mathrm{m/s}$
	T	50 s	Simulation time
MGAD	$[\epsilon^{\max}_{\mathrm{t}_0}, \epsilon^{\min}_{\mathrm{t}_0}]$	[50,5]	Step size thresholds
	$[\beta_1, \beta_2]$	$[0.5, 0.05]$	Discount factors
	m	1×10^{-5}	Momentum
	θ	1×10^{-8}	Convergence threshold
	K	30	Maximum iteration

The simulation results in Fig 5 depict the average error of 50 estimates. Among the three best fixed step sizes, $\alpha = (1.5, 2.3, 2.7)$ yield average localization errors across all n_a of $(1.63, 1.67, 1.66)$ respectively. In comparison, the average localization error archived by MAGD in this regard is 1.47, indicating that MAGD outperforms conventional approaches with fixed α^0. In this specific setup, step sizes ranging from 1.4 to 3.0 show robust performance, although such a range may be challenging to find in practice. By adjusting α^0 to different scenarios, our proposed method efficiently provides robust position estimation with good accuracy.

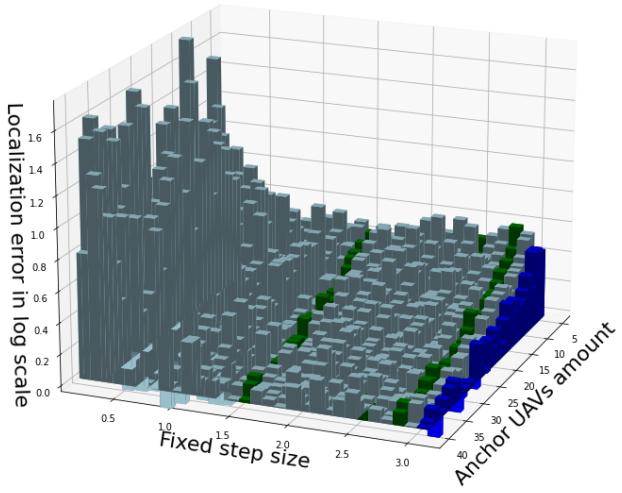


Fig. 5. Localization error of fixed step sizes and MAGD (3 best step sizes are marked in green and MAGD in darkblue)

IV. Attack Paradigm and Mutual Attack Detection System

A. Attack Paradigm

Potential attacks on localization techniques can be categorized into several aspects.

Jamming mode: the attacker jams the beacon signal of u_n to introduce large distance estimation error and induce a wrongly received $\mathrm{p}(n)$ and $\sigma_{\mathrm{p},n}$. The received signal can be represented as $[\mathrm{p}_n^\circ + \tilde{\mathrm{p}}_n, (d_{k,n}^\circ + \tilde{d}_{k,n})^+, \sigma_{\mathrm{p},n} + \tilde{\sigma}_{\mathrm{J}}]$. Take the simplification, $\tilde{\mathrm{p}}_n \sim \mathcal{N}^3\left(0, \tilde{\sigma}_{\mathrm{J}}^2/3\right)$, $\tilde{d}_{k,n} \sim \mathcal{U}\left(0, \tilde{\sigma}_{\mathrm{J}}^2\right)$, where $\tilde{\sigma}_{\mathrm{J}}^2$ is the jamming index. **Bias mode**: the attacker hijacks some of the UAVs to erroneously report its position with a certain position bias to mislead others. In this scenario, the received signal can be modeled as $[\mathrm{p}_n^\circ + \tilde{\mathrm{B}}, d_{k,n}^\circ, \sigma_{\mathrm{p},n}]$, where $\tilde{\mathrm{B}}$ denotes position bias. **Manipulation mode**: the attacker hijacks some of the UAVs to report its position with an extra error, simultaneously modify its $\sigma_{\mathrm{p},n}$ to be extremely small for the intention of manipulating w_n^e. The received signal can be concluded as $[\mathrm{p}_n^\circ + \tilde{\mathrm{p}}_n, d_{k,n}^\circ, 1/\tilde{\sigma}_{\mathrm{M}}]$, where $\tilde{\mathrm{p}}_n \sim \mathcal{U}\left(0, \tilde{\sigma}_{\mathrm{M}}^2/3\right)$, $\tilde{\sigma}_{\mathrm{M}}^2$ is the manipulation index.

In a constantly moving scenario, attack strategies can be categorized as follows. **Global random attack**: All malicious UAVs are uniformly distributed and randomly attack all nearby UAVs. This strategy aims to degrade position estimation globally and penetrate existing attack detection systems, as suggested in [**?**]. **Global coordinated attack**: Similar to the global random attack, the malicious UAVs coordinate their attacks within a certain time frame. **Stalking strategy**: All malicious UAVs follow a victim UAV and constantly attack it. This strategy does not impact estimation accuracy globally but targets the victim specifically.

B. Anomaly detection and trust propagation mechanism

Considering the above-mentioned attack schemes, a robust attack detection algorithm should be degrading the trustworthiness of suspicious UAVs. To achieve this, a reputation weight r_n can be applied in MAGD, more specifically in Alg III.1 line 13 and 15,

$$G^i \leftarrow \sum_{u_n \in \mathcal{U}} \frac{(\hat{\mathrm{p}} - \mathrm{p}_n) * w_n^e * r_n}{d_n} * (d_n - d_n^\circ) \tag{18}$$

$$\bar{D}_i \leftarrow \frac{1}{n} * \sum_{u_n \in \mathcal{U}} (\hat{d}_n - d_n^\circ + \mu_{c,n}) * w_n^e * r_n \tag{19}$$

Our proposed method, illustrated in Alg IV.1, estimates reputation weight using the cumulative distribution function of $\mathcal{N}(\mu_{\mathrm{cd},n}, \sigma_{\mathrm{cd},n})$. In lines 7-8, u_k calculates the estimated distance error $\hat{\mathcal{E}}_n$ based on information from u_n and the converted error distribution. Lines 12-16 address potential manipulation attacks by limiting $\sigma_{\mathrm{c},n}$ to a predefined minimum position error power $\sigma_{\mathrm{p,min}}$. Then compare the cumulative density ξ_n with a preset probability threshold ϵ^t to detect the attack behavior of u_n. Depending on the detection results, the reputation weight update is performed with a punishment or reward $[\lambda_r, \lambda_p]$. The updated $r_n(t)$ considers its previous value $r_n(t-1)$, a forget factor γ, and the corresponding reward or penalty. Then $r_n(t)$ is thresholded within the range of [0,1]. This approach aims at countering coordinated attacks, allowing $r_n(t)$ to recover gradually when attacks from u_n become less frequent, without compromising mutual localization accuracy.

Algorithm IV.1: Time-evolving anomaly detection

1 Input: Reward λ_r and penalty λ_p, forget factor γ and confidence threshold ϵ^t
2 Output: $r_n(t)$
3 Initialize: $r_n(t=1) \leftarrow 1$
4 **Function** TAD($t = 1 : T$) **is**
5 get $\hat{\mathrm{p}}(t)$ from MAGD(t) meanwhile apply $r_n(t-1)$
6 **for** $n = 1 : N$ **do**
7 get $\sigma_{\mathrm{p},n}, d_n^\circ, \mathrm{p}_n^\circ$ from u_n
8 get $\mu_{\mathrm{c},n}, \sigma_{\mathrm{c},n}$
9 $\hat{d}_n \leftarrow \|\hat{\mathrm{p}} - \mathrm{p}_n\|$
10 $\hat{\mathcal{E}}_n \leftarrow |\hat{d}_n - d^\circ n + \mu_{\mathrm{cd}}|$ // Distance error of u_n
11 calculate CDF ξ_n,
12 $\sigma_{\mathrm{c},n} \leftarrow \max(\sigma_{\mathrm{c},n}, \sigma_{\mathrm{p},min})$
13 $\xi_n \leftarrow P_{\hat{\mathcal{E}}_n}\left[\hat{\mathcal{E}}_n \mid \mu_{\mathrm{c},n}, (\sigma_{\mathrm{c},n})^2\right]$
14 **if** $\xi_n > \epsilon^t$ **then**
15 $\hat{r}_n \leftarrow \lambda_r$ // Assign reward
16 **else**
17 $\hat{r}_n \leftarrow \lambda_p$ // Assign penalty
18 update $r_n(t)$
19 $r_n(t) \leftarrow \gamma * [r_n(t-1) + 1] - 1 + \hat{r}_n$
20 $r_n(t) \leftarrow \min(1, \max(0, r_n(t)))$

To address the vulnerability of target UAVs to spatial "ambushing" or stalking attacks, we incorporate a global reputation system. This system allows UAVs to share their local reputations with each other. Nevertheless, malicious reputation information can be shared as well, therefore a reputation propagation scheme is implemented. This ensures that reputation weights are carefully propagated, maintaining the reliability and accuracy of reputation information within the system. The propagated reputation weights can be described as follows:

$$\tilde{r}_{k,n} = \frac{\sum\limits_{m \notin k,n} r_{k,m} * r_{m,n}}{\sum\limits_{m \notin k,n} r_{k,m}}, \tilde{\tilde{r}}_{k,n} = \frac{\mathrm{F_p}(\tilde{r}_{k,n}) + r_{k,n}}{2}. \quad (20)$$

While u_k is utilizing the mutual localization system, $u_1 ... u_n$ are the accessible anchor UAVs, and $r_{k,n}$ is the local reputation. u_m has uploaded its local reputation to the cloud, enabling reputation $r_{m,n}$ from u_m to u_n to be accessed. Meanwhile, u_k has a local reputation $r_{k,m}$ to u_m. Based on the local reputation $r_{k,m}$, the uploaded reputation will be discriminated against accordingly. A propagated reputation $\tilde{r}_{k,n}$ is strongly leaning to UAV which has a good reputation to u_k. $\mathrm{F_p}$ is the propagation function designed to discriminate the already notorious u_n(a convex function is applied). Subsequently, proceed with the mean of local reputation and propagated reputation to MAGD.

V. Simulation Results

A. Evaluation under different attack mode and strategy

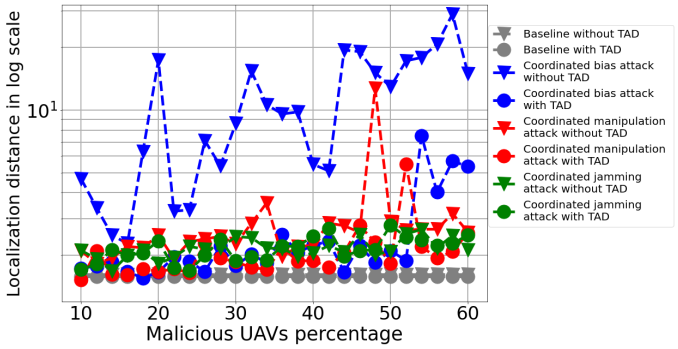
TABLE III
Simulation Setup 2

	Parameter	Value	Remark
MGAD	Map Size	$[300, 300, 10]$	Define map size
	n	100	number of anchor UAVs
	$\sigma^2_{\mathrm{p},n}$	$\sim \mathcal{U}(0.1, 3.0)$	Position error power / m^2
	V	$\sim \mathcal{U}(0.3, 1.7)$	Travel speed $\mathrm{m/s}$
	T	100 s	Simulation time
	m	1×10^{-5}	Momentum
	θ	1×10^{-8}	Convergence threshold
	K	30	Maximum iteration
TAD	$[\lambda_r, \lambda_p]$	$[0.3, -0.7]$	Reward and penalty
	γ	0.5	Forget factor
	ϵ^t	0.95	Confidence threshold
Attacker	n_m	30	Malicious UAVs
	r_a	0.5	Attack rate if random attack
	T_a	50	Attack time frame if coordinated attack
	$\tilde{\mathrm{B}}_n$	$[200, 200, 5]$	Position bias if bias attack
	$\tilde{\sigma}^2_{\mathrm{M},n}$	200	Manipulation index if manipulation attack attack
	$\tilde{\sigma}^2_{\mathrm{J},n}$	5	Jamming index if jamming attack attack

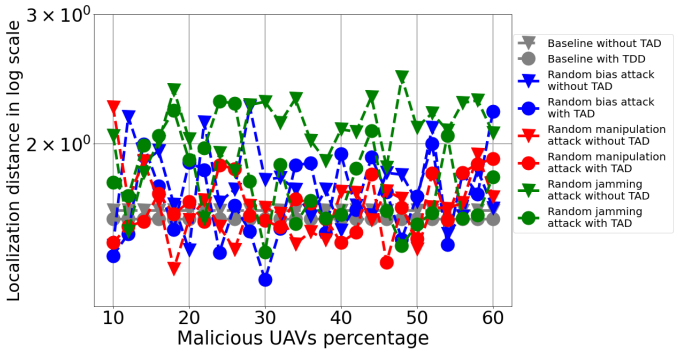
To validate the robustness and effectiveness of TAD, we carried out simulations of our mutual localization system under different attack modes and strategies, while 10 targets u_k navigates through attackers. We assume the attacker has limited resources and can only jam/hijack some part of the UAVs. The attacks can be organized as random or coordinated. The MAGD configuration follows Tab.II, while system, TAD and attacker parameters are listed in Tab.III. The attack rate and attack time frame are set to 0.5 and 50 to keep an unvarying attack power. All anchor UAVs are distributed within the map and navigate to random destinations, which leads to an average of 15 anchor UAVs within a mutual localization range of 50. Target UAVs can be anchor UAVs to each other, $\sigma^2_{\mathrm{p},k}$ is set to be $\max(\sigma^2_{\mathrm{p},n})$. The simulation results are shown in Fig. 6 and Tab. IV.

TABLE IV
Estimate error () under different attack scheme and malicious UAVs percentage

Attack schemes \ Percentage	10-20%	20-30%	30-40%	40-50%	50-60%
No attack	1.62	–	–	–	–
No attack with TAD	1.58	–	–	–	–
Coord. Bias	3.89	7.29	10.80	12.84	19.54
Coord. Bias with TAD	1.72	1.88	2.05	2.06	4.25
Random Bias	1.82	1.84	1.73	1.68	1.74
Random Bias with TAD	1.64	1.66	1.62	1.74	1.74
Coord. Mani.	2.05	2.32	2.58	4.63	2.82
Coord. Mani. with TAD	1.72	1.86	1.88	2.16	2.71
Random Mani.	1.77	1.57	1.54	1.68	1.66
Random Mani. with TAD	1.58	1.71	1.61	1.56	1.71
Coord. Jam.	1.97	2.06	2.24	2.18	2.39
Coord. Jam. with TAD	1.94	2.03	2.03	2.28	2.43
Random Jam.	1.95	1.93	2.12	2.16	2.19
Random Jam. with TAD	1.95	2.04	1.62	1.72	1.68



(a) Coordinated attack scheme



(b) Random attack scheme

Fig. 6. Localization error of different over malicious UAVs percentage

Contrary to findings in static sensor networks, our results indicate that coordinated attacks are more effective than uncoordinated ones, contradicting the suggestion that both schemes are equally effective [**?**][**?**]. The inconsistency in error injection

during each MAGD's gradient descent process leads to this difference. MAGD can still provide accurate estimations under less dense attacks due to varying attack density, preventing a cascading effect of mislocalization caused by injected errors. Random attacks lead to temporary large localization errors, which can be quickly resolved within a few timesteps. In contrast, coordinated attacks cause sustained mis-localization (detailed trace error analysis emitted in this paper due to the length limit). Moreover, the results demonstrate that attack mode bias exhibits higher effectiveness in causing large localization errors. This is attributed to the fact that the injected errors in this mode do not offset each other, leading to a cumulative impact on the localization accuracy. Additionally, the coordinated jamming mode poses a formidable challenge to TAD as it enlarges $\sigma_{c,n}$ of malicious UAVs, which makes it challenging for TAD to identify attacks. Nonetheless, our proposed weighted localization approach effectively mitigates such attacks by favoring anchor UAVs with smaller $\sigma_{c,n}$, thereby bolstering the overall resilience and robustness of the localization system.

To further assess TAD and RP, we conducted simulations with malicious UAVs employing a coordinated stalking strategy to attack the victim target u_k. The parameters for MAGD and TAD follow those listed in Table III, while the attack mode is set to bias mode. The percentage of malicious UAVs is set at 30%, which includes 3 target UAVs capable of attacking other target UAVs while sharing malicious reputation. We assume the attacker knows the actual position of the victim target with ambiguity (the estimated position $\hat{\mathrm{p}}_k$, shared by u_k, should not be used as it can be misleading when attacks become effective). The results in Fig. 7 show average errors of 20 simulations at different time steps.

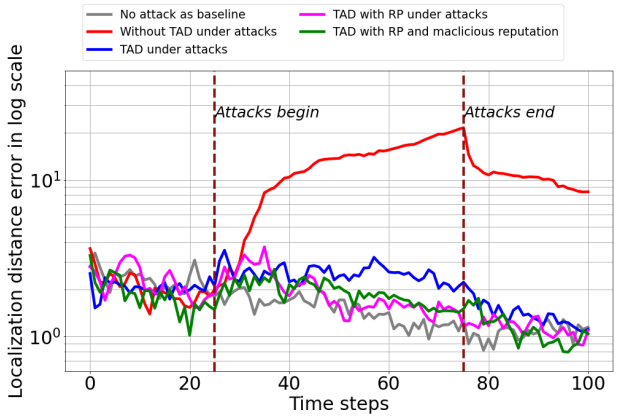


Fig. 7. Localization error at different time step (for the baseline, UAVs are set to follow the target as well)

Our simulation results demonstrate the effectiveness of TAD against stalking attack strategies with the given attack density, significantly reducing localization errors compared to the absence of TAD. Moreover, the introduction of RP further enhances localization performance, leading to a faster convergence of localization errors compared to TAD alone. Notably, RP also exhibits resilience to malicious reputation information.

VI. Conclusion

In this paper, we evaluated localization techniques and presented a novel localization scheme (MAGD) that adapts to the mobility and changing availability of anchor UAVs. Additionally, we introduced defense schemes (TAD and RP) to counter potential attacks. Our numerical simulations demonstrated the effectiveness of these methodologies in dynamic scenarios.

However, it is essential to acknowledge that this study did not extensively address potential attacks against RP. A sophisticated attacker might manipulate a subset of compromised UAVs to launch attacks on target UAVs while others share a malicious reputation. This poses a challenge for our TAD and RP to effectively detect and mitigate such attacks. The potential threat calls for a novel approach to identifying attack patterns.

Acknowledgment

This work is supported in part by the German Federal Ministry of Education and Research within the project Open6GHub (16KISK003K/16KISK004), in part by the European Commission within the Horizon Europe project Hexa-X-II (101095759).
B. Han (bin.han@rptu.de) is the corresponding author.