2025 International Conference on Intelligent Computing
July 26-29, Ningbo, China
https://www.ic-icc.cn/2025/index.php

A Heading Correction Method for UAV Swarms Against Yaw Deception Based on the Consensus Potential Field

Huan Zhao[1][0009-0004-0308-6214], Yuxin Xue[2][0009-0007-1599-0245], and Zhaojun Gu[3](✉)

[1] Computer Science and Technology Academy, Civil Aviation University of China, Tianjin, 300300, China
[2] Safety Science and Engineering Academy, Civil Aviation University of China, Tianjin, 300300, China
[3] Institute of Science, Technology and Innovation, Civil Aviation University of China, Tianjin, 300300, China
zhaohuan_cauc@163.com

Abstract. A yaw spoofing heading correction method utilizing a consensus force field is introduced to address the issue of drone swarm heading deviation during Global Navigation Satellite System (GNSS) spoofing attacks. Firstly, a noisy environment based on asymmetric information environment is established to simulate the attack and defense scenario of unmanned aerial vehicle clusters against yaw deception attacks under environmental noise interference. Then, based on the attack principle, the yaw correction problem is transformed into an artificial potential field problem where the repulsive field is invisible, and the repulsive source is predicted based on spatial relationships to achieve preliminary correction of the yaw direction; Finally, by designing a lightweight gamma Consensus mechanism and further correcting the yaw direction through credibility calculation and consensus mechanism, collaborative defense against yaw deception attacks is achieved. The experimental results indicate that, Under the CPF method, the cluster achieved a destination error of 10.32 meters, a trajectory deviation of 13.35 meters, and a task completion rate of 90.45%. Compared with game models, random decision, and other methods, there is a significant improvement, which verifies the effectiveness and robustness of the method in the face of yaw deception attacks in long-distance flight missions.

Keywords: UAV swarm, artificial potential field, consensus mechanism, GNSS spoofing defense

1 Introduction

Unmanned aerial vehicle (UAV) swarms are a groundbreaking technology used in various fields such as intelligent transportation and disaster response [1–3]. These swarms heavily depend on global navigation satellite systems (GNSS) for accurate positioning and synchronized navigation. However, the vulnerability to GNSS spoofing attacks, where false signals are broadcasted to disrupt trajectories, poses a significant risk to swarm autonomy [4, 5]. The Black Sea swarm incident in 2023 exempli-

fies the susceptibility of even sophisticated systems to yaw spoofing, resulting in mission failures. Conventional defense mechanisms like redundant antenna arrays and inertial navigation systems (INS) come with drawbacks such as increased payload and error accumulation, constraining their applicability in large-scale swarms [6–8].

Designing a lightweight distributed defense mechanism is crucial for addressing heading bias while preserving group agility. Current data-driven techniques, like game theory deception games [9] and particle swarm optimization (PSO) [10], lack real-time spatial awareness and do not adequately capture the dynamic interactions between deception sources and population dynamics. Machine learning methods [11] necessitate substantial training data and encounter difficulties in adapting to new attack patterns. Additionally, potential field models [12] often overlook the consensus-driven efforts essential for ensuring group consistency.

To fill these gaps, we have introduced a Consensus Force Field (CPF) model. This model is a distributed, model-free framework that integrates spatial relational reasoning and consensus-based work to counter GNSS spoofing. In contrast to previous approaches, CPF views spoofing attacks as unknown repulsive sources within artificial potential fields. This allows group members to collectively forecast disturbance trajectories and compute corrective forces in real-time. The novelty of this model lies in three key components: (1) a spatiotemporal potential field model that represents attack-defense interactions as dynamic repulsive forces; (2) a spatial relationship-aware prediction algorithm that utilizes relative position updates to predict the movement of spoofing sources; and (3) a consensus-driven collaborative defense strategy that harmonizes individual heading corrections by aggregating forces in a distributed manner to maintain trajectory consistency without centralized control.

This study enhances drone swarm navigation by proposing a lightweight and scalable defense framework that overcomes key limitations of existing approaches, such as payload constraints, error buildup, and centralized control bottlenecks. By conceptualizing deception as a dynamic force field and promoting consensus-driven processes, the CPF enables autonomous clustering operations in challenging adversarial settings, thereby facilitating the development of advanced intelligent systems.

2 Related Work

The defense measures against yaw angle attacks are mainly divided into detection stage and defense stage. [13] Wei et al. developed PerDet, a perceptual data-driven framework using accelerometers, gyroscopes, and GPS data. By fusing heterogeneous sensor input, PerDet achieves a detection rate of 99.69% through an optimized ML classifier. Recent progress includes [14] Khoei et al., who applied capsule networks to fraud classifications, increasing accuracy to 99.1%, while reducing computational over-head. These efforts highlight the effectiveness of machine learning in leveraging rich sensor data for spoof detection. Collaborative strategies leverage swarm intelligence and external networks. [15] proposed a deep ensemble learning framework for cellular connected drones that uses path loss analysis between base stations to detect trajectory deviations. Even in the case of limited infrastructure, the method achieves

97% accuracy in a dual-base-station configuration. But this method is only applicable to the anomaly detection problem of a single aircraft

For drone swarms, Meng et al. [16] developed ASD, which is a two-stage algorithm: (1) SSD for single-source attacks through cooperative positioning, and (2) RSOM for multi-source scenarios. ASD ensures lightweight real-time detection in dynamic crowd environments. Signal level analysis is the basis for attack modeling and countermeasures. [17] Ma et al. analyzed the spoofing effect on the receiver loop and demonstrated that amplitude-gain manipulation can lure UAVs to a specified location while evading detection. On this basis,[18] Wang et al. introduced the Doppler and Clock Drift Double Difference method for stationary spoofing source location, which was verified by field experiments. These efforts have revealed physical layer vulnerabilities in GPS receivers.

The action decision against deception attacks is a key factor that directly determines the continuity and integrity of cluster tasksGame theory simulates the interaction of attackers and defenders to achieve the best defense. [19] Eldosouky et al. formulated a Stackelberg game in which drones use cooperative positioning to counter spoofers, analyzing to derive an equilibrium strategy to minimize capture risk. In our previous work [20], we designed a vector adversarial method for asymmetric information environments, implemented cluster based col-elaborative defense based on flight vectors, and verified the effectiveness of the environment and method. [21] Guo et al. designed a SINS/GPS anti-spoofing method that uses Kalman filter to dynamically adjust false satellite signals to achieve accurate directional departure under integrated navigation. Early layered systems, such as [22] Sedjelmaci et al., combined signal analysis and net-work monitoring for multi-layered drone security to jointly address spoofing and jamming.

3 Heading Correction Method Based on the CPF

3.1 Kinematics and scenario model

Since most drones are equipped with barometric altimeters when deployed, these physically-driven altitude measurement sensors are nearly immune to effective attacks. Therefore, during the mission, the reliability of altitude signals does not need to be considered, and only the 2D motion changes need to be taken into account. For aircraft *i*, its kinematic model can be expressed as equation (1).

$$\begin{cases} \mathbf{P}_i(t) = \left[x_i(t), y_i(t)\right] & \text{Position} \\ \mathbf{v}_i(t) = \dfrac{\mathrm{d}\mathbf{P}_i(t)}{\mathrm{d}t} = \left[v_i^x(t), v_i^y(t)\right] & \text{Velocity} \\ \mathbf{a}_i(t) = \dfrac{\mathrm{d}\mathbf{v}_i(t)}{\mathrm{d}t} = \left[a_i^x(t), a_i^y(t)\right] & \text{Acceleration} \end{cases} \tag{1}$$

According to Newton's dynamics, the acceleration of the aircraft $\mathbf{a}_i(t)$ satisfies the mechanical relationship:

$$\begin{cases} \mathbf{a}_i(t) = \left(\mathbf{F}_i^{th}(t) + \mathbf{F}_i^{dr}(t)\right) \cdot m^{-1} \\ \mathbf{F}_i^{th}(t) = F_i(t)\left[\cos\psi(t) \quad \sin\psi(t)\right] \\ \mathbf{F}_i^{dr}(t) = Gauss\left(\mathbf{v}_i(t), \sigma\right) \end{cases} \tag{2}$$

Where $\mathbf{F}_i^{th}$ is the two-dimensional component of the rotor thrust in the horizontal direction of the aircraft, F_i is the maximum power scalar of the aircraft, $\psi(t)$ is the yaw angle of the aircraft at the current moment, $\mathbf{F}_i^{dr}$ is the two-dimensional nonlinear resistance, and $Gauss\left(\mathbf{v}_i(t), \sigma, \|\cdot\|\right)$ is the environmental noise generator, which applies Gaussian noise with a noise coefficient σ to the velocity $\mathbf{v}_i(t)$ of the aircraft at time *t*. The effect of σ is represented by the range of random fluctuations of $\mathbf{v}_i(t)$ in the two-dimensional direction. The update process of the aircraft's motion state can be expressed as:

$$\begin{cases} \mathbf{v}_i(t+\Delta t) = \mathbf{v}_i(t) + \Delta t \cdot \mathbf{a}_i(t) \\ \mathbf{P}_i(t+\Delta t) = \mathbf{P}_i(t) + \Delta t \cdot \mathbf{v}_i(t) + 2^{-1}\mathbf{a}_i(t)\Delta t^2 \end{cases} \tag{3}$$

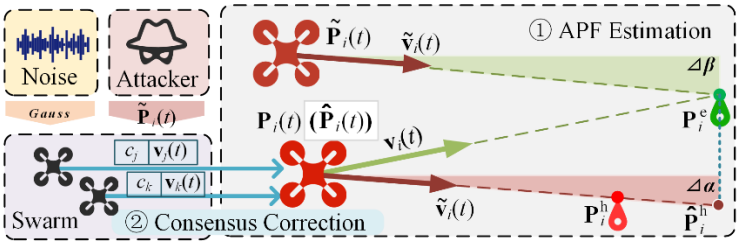

Fig. 1. CPF verification environment and principles

Figure 1 shows the CPF model operating environment and defense principles. At time t, aircraft *i* is located at position $\mathbf{P}_i(t)$. According to the planned flight trajectory, the aircraft should fly to the destination $\mathbf{P}_i^{e}$ at speed $\mathbf{v}_i(t)$. However, at this moment, an attacker launches a position spoofing attack on the aircraft, intending to make the aircraft receive an incorrect position, mistakenly believing it is at $\mathbf{P}_i(t)$, and changing its flight direction to $\mathbf{v}_t(t)$, heading towards the hijacking location $\mathbf{P}_i^{h}$. Throughout the entire flight process, all aircraft in the swarm are unable to detect the true position of $\mathbf{P}_i^{h}$, while the attacker is able to obtain all the aircraft's information,

thus creating an asymmetrical attack-defense scenario [20]. Based on current research on UAV GNSS spoofing signal detection methods [13-19], we assume that all swarm members are equipped with advanced detection algorithms, capable of detecting abnormal signals within a unit of time.

3.2 Heading correction based on the CPF

After the aircraft detects a malicious signal, it will no longer trust its own position information $\mathbf{P}_i(t)$. Based on equation (3), it will use the position from the previous moment $\mathbf{P}_i(t-\Delta t)$ and velocity information $\mathbf{v}_i(t-\Delta t)$ to calculate the estimated position $\mathbf{P}_i(t)$ at time t.

Based on the principle of yaw attack, in space, $\measuredangle\alpha$ and $\measuredangle\beta$ have a similar relationship. With the coordinates of $\mathbf{P}_i(t)$ and $\mathbf{P}_i(t)$ known, and combining $\mathbf{P}_i(t)$ with the similarity theory based on equation (4), the estimation of $\mathbf{P}_i^{\mathrm{h}}$ is performed to obtain the estimated hijacking point $\mathbf{P}_i^{\mathrm{h}}$. In the equation, $\|\mathbf{a},\mathbf{b}\|_2^x$ represents the Euclidean distance in the x-direction between two vectors a and b in 2D space, and $\|\mathbf{a},\mathbf{b}\|_2^y$ represents the Euclidean distance in the y-direction.

$$\left\|\mathbf{P}_i(t)-\mathbf{P}_i^{\mathrm{e}}\right\|_2^x\cdot\left\|\mathbf{P}_i(t)-\mathbf{P}_i^{\mathrm{h}}\right\|_2^y=\left\|\mathbf{P}_i(t)-\mathbf{P}_i^{\mathrm{e}}\right\|_2^y\cdot\left\|\mathbf{P}_i(t)-\mathbf{P}_i^{\mathrm{h}}\right\|_2^x \tag{4}$$

Based on the estimated coordinates of the hijacking point, the artificial potential field theory is used to formulate a hijacking course correction problem based on an unknown repulsive field. Specifically, the target coordinates are treated as an attractive source, while the estimated coordinates are treated as a repulsive source. The resultant force is calculated based on equation (5), where k_{att} and k_{rep} represent the attraction and repulsion factors, respectively. After $\mathbf{F}_i^{\mathrm{total}}$ is calculated, it will be incorporated into the acceleration calculation process in equation (2) and used to compute the potential field velocity $\mathbf{v}_t^{\mathrm{APF}}(t)$ based on equation (3).

$$\begin{cases}\mathbf{F}_i^{\mathrm{total}}=\mathbf{F}_i^{\mathrm{att}}+\mathbf{F}_i^{\mathrm{rep}}\\ \mathbf{F}_i^{\mathrm{att}}=k_{\mathrm{att}}\left\|\mathbf{P}_i(t),\ \mathbf{P}_i^{\mathrm{e}}\right\|_2,\mathbf{F}_i^{\mathrm{rep}}=k_{\mathrm{rep}}\left(\left\|\mathbf{P}_i(t),\mathbf{P}_i^{\mathrm{h}}\right\|_2\right)^{-1}\end{cases} \tag{5}$$

After the initial heading calibration of a single aircraft, it requests healthy heading information from partners within its communication range. Each member has a built-in trustworthiness calculator as shown in equation (6), where $\zeta(j)$ represents the number of times the aircraft has detected spoofing attacks from the start of the mis-

sion to time t. A higher c_j value indicates that the member's vector information is more reliable. Upon receiving the request, the member sends its flight vector information along with its trustworthiness value to the requester.

$$c_j = 1 - \frac{\zeta(j)}{t} \tag{6}$$

To reduce the computational burden on the aircraft, a heading correction algorithm based on a sparse consensus mechanism— γ -Consensus—is designed. Upon receiving messages from members, the requester retains only the top $\gamma \times 100\%$ vector information based on trustworthiness ranking. Let h be the number of healthy nodes within the communication range, $\eta = \lfloor h \cdot \gamma \rfloor$ be the number of retained members. $\mathbf{c}_\eta = \left[c_1 \; c_2 \; \ldots c_\eta \right]^T$ denotes the trustworthiness vector, and the velocity vector matrix is denoted as $\mathbf{V}(t) = \left[\mathbf{v}_1(t) \, \mathbf{v}_2(t) \ldots \mathbf{v}_h(t) \right]^T$. The final calibrated velocity obtained by the affected aircraft is expressed as:

$$\mathbf{v}_i^{\text{con}} = \frac{1}{2}\left(\mathbf{v}^{\text{APF}} + \left(\mathbf{V}(t) \right)^T \text{diag}\left(\mathbf{c}_\eta \right) \mathbf{1}_\eta \right) \tag{7}$$

Based on CPF, the swarm can achieve a model-free collaborative defense method against spoofing attacks. Compared to model-based and other complex methods, the complexity of CPF is primarily determined by the sorting algorithm, which saves more onboard resources and enhances the scalability of the computational power.

4 Experimental results and analysis

4.1 Experiment setup

The simulation software is coded in Python and operates on an experimental setup utilizing a Garine system powered by an Intel (R) Core (TM) Ultra 5 125H processor clocked at 1.20 GHz. The system comprises a workstation with 32.0 GB DDR4 RAM (31.6 GB usable) and runs on the 64-bit Windows 11 operating system (x64 architecture). The simulation platform is constructed in Python, utilizing NumPy (version 1.26.0) and SciPy (version 1.11.1) for dynamic modeling, in conjunction with Matplotlib (version 3.8.0) for visualizing trajectories.

After repeated experiments and previous work, the environmental noise is set to $\sigma = 0.5$, $k_{\text{att}} = 0.4$, $k_{\text{rep}} = 0.6$, and the flight physical parameters are referenced from the Parrot Anafi drone, with a mass of 0.5 kg, a maximum horizontal flight speed of 15 m/s, and a line-of-sight communication radius of 50 m. The maximum flight time is set to 30 minutes with 1800 time slots. In each time slot, at least zero and at most all group members will be subjected to malicious attacks, and affected aircraft will receive incorrect location information.

Table 1. Evaluation metrics.

Metrics	Description	Metrics	Description
T(s)	The time consumed to reach termination state.	E_e(m)	The deviation from the expected destination.
S(m)	The total flight distance of aircraft.	H(True/False)	Whether the aircraft has been hijacked.
E_r(m)	The deviation from the expected trajectory.	P(%)	The proportion of healthy members in the swarm.

4.2 Performance evaluation experiment

After taking off from the initial position, the swarm executes flight missions under the interference of environmental noise and malicious attacks. Fig. 2 shows the flight trajectory of the swarm's defense method based on an unknown repulsive field environment. The blue dots in the figure represent the starting flight position of the aircraft, the green dots indicate the expected destination, and the red diamonds mark the location of the malicious hijacking. The green dashed line represents the expected trajectory of the aircraft under ideal conditions, the red dashed line shows the flight trajectory the aircraft will execute without defensive measures if deceived, and the blue solid line indicates the actual flight trajectory. As shown in the figure, all six members in the swarm successfully reached a safe area under malicious attacks and environmental noise disturbances, proving the effectiveness of the proposed method.

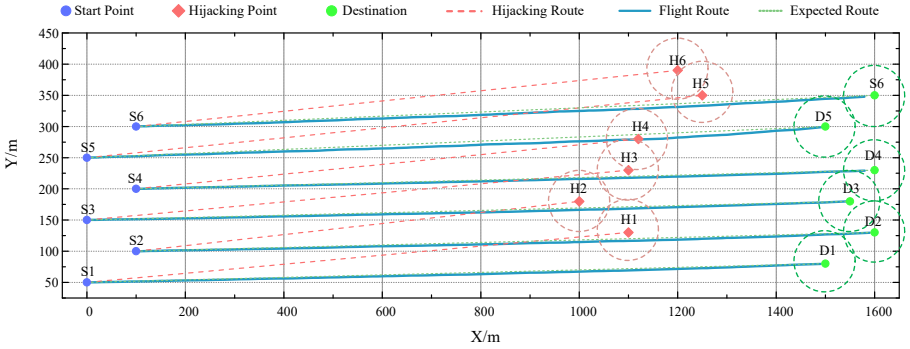

Fig. 2. Swarm Flight Trajectory Diagram in CPF.

Table 2 summarizes the various flight information of the swarm upon task completion. The experimental results show that swarm members can reach the safe area within approximately 120s, and the deviation from the expected route during short-distance flight is less than 10m. Regarding environmental disturbances and malicious attacks throughout the mission, the error from the endpoint after completion is within the range of 5–21m.

Table 2. Record of Swarm Job Results.

No.	*S*/m	*T*/s	E_r/m	E_e/m	*H*
1	1490.29	121	2.79	10.04	False
2	1490.32	120	3.50	10.02	False
3	1550.41	111	3.37	5.24	False
4	1480.29	120	2.37	20.03	False
5	1500.32	119	8.47	5.95	False
6	1480.30	120	5.57	20.68	False

Fig. 3 presents the impact of flight distance and swarm size on the performance of the proposed algorithm. Specifically, Fig. 3 (a) demonstrates how the average destination error and drift error of the swarm vary as the horizontal coordinates of the target and hijacking location are enlarged by multiple factors, increasing flight distance. The blue curve with semitransparent bands shows the average and standard deviation (SD) of the swarm members' deviation from the expected flight trajectory, while the red curve with bands indicates the average and SD of their distance from the target end-point after completion. Fig. 3 (b) illustrates how these errors change with the number of swarm members. Here, the blue curve and bands represent the average and SD of the error distance between the swarm and the target location post-task, while the red curve and bands correspond to the offset error and SD from the expected trajectory during flight. The results indicate that increasing the number of nodes improves the destination accuracy and reduces error fluctuations among members, but the drift error remains stable with slightly increased fluctuations among members.

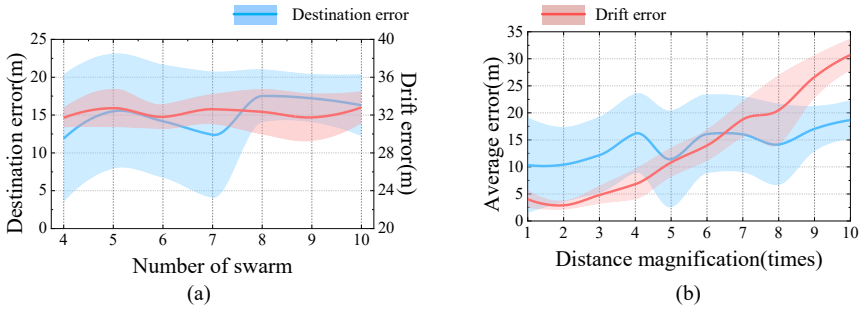

Fig. 3. Variation of Flight Error with Distance.

In all ten cases shown in the Fig. 2 (a), the swarm can successfully reach the destination without being hijacked, and the error distance between the aircraft and the destination position remains within 10–20m. However, the error tends to increase as the distance expansion factor increases. The color bands on both sides of the curve also reflect substantial fluctuations in the error distance among members and the destination position. However, as flight distance increases, member interactions become more frequent, and fluctuations tend to decrease. The average offset distance between the swarm and the expected trajectory shows a clear upward trend, with offset fluctua-

tions gradually amplifying, mainly owing to the accumulation of errors from the lengthening of the flight distance.

Table 3 shows the time and other performance parameters required by the swarm to complete tasks over a greater distance (with the horizontal axis magnified 11–13 times). When the distance expansion factor reached 12 times, owing to the influence of the maximum flight time, some members, although not hijacked, were unable to reach the safe area and were considered mission failures. Therefore, only the average drift error is recorded. The experimental results show that as the flight distance increases, some aircraft cannot reach the safe area because of the continuous impact of environmental disturbances and malicious attacks, resulting in a decrease in the overall flight distance of the swarm and the completion of swarm tasks.

Table 3. Record of swarm job results.

Magnification	S/m	T/s	Er/m	P/%
11	17280.33	1645	35.23	100%
12	16879.67	Full	40.5	66.67%
13	14686.5	Full	43.95	16.67%

4.3 Performance comparison experiment

Table 4. Method number and description.

Method	Description
CPF	Swarm counteracts attacks through joint force and consensus mechanism
Game	Swarms and attackers make offensive and defensive decisions through games.
PID	Using velocity as input of PID controller to resist malicious attacks.
PSO	Members adjust flight direction based on their best position and the global best position.
Random	The attacker and defender randomly select targets for attack and defense.

Table 4 lists the five defense methods and compares the defense performance of the five defense methods, including the proposed method. Fig. 4 shows the flight trajectories of swarms under four comparative algorithms. As Fig. 4 (a) and Fig. 4 (b) show, both the game and PID models can help the swarm reach a safe area, and the flight trajectory of the PID model has a satisfactory fit with the expected trajectory. In the PSO model in Fig. 4 (c), the aircraft can bypass the hijacking location, but the flight trajectory deviates considerably. During the simulation, cluster members could not reach the safe area, resulting in substantial endpoint errors and trajectory deviations. In the random decision model, the flight direction of the swarm changes frequently, especially when approaching the target area. After reaching the simulation time, member 5 did not reach the safe area, indicating that the defense performance was random.

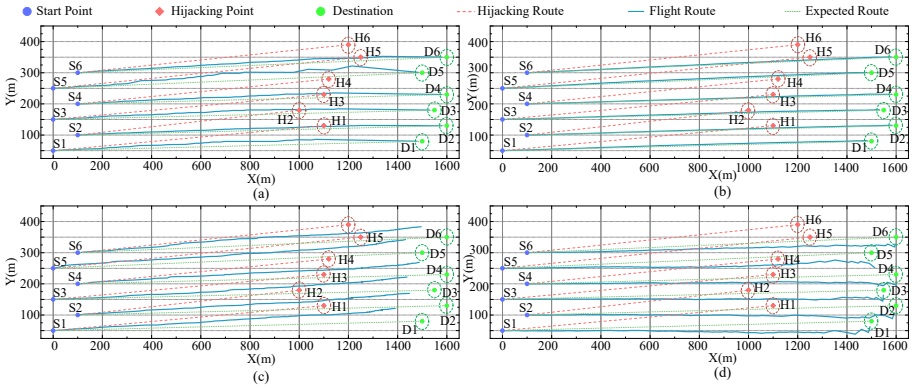

Fig. 4. Swarm flight trajectory in different methods:
(a) Game model, (b) PID model, (c) PSO model, (d) Random model.

The experimental results indicate that, in comparison to the proposed method, the algorithm based on the game model exhibits a higher distance error and greater fluctuations in trajectory deviation, although it shows smaller fluctuations in endpoint deviation and requires more time for flight missions. The defense method utilizing the vector PID model demonstrates strong performance in terms of endpoint error and trajectory deviation, with minimal performance fluctuations within the swarm. However, this method demands more time than the proposed approach. Conversely, the defense algorithm based on the PSO model offers satisfactory time efficiency, yet it suffers from substantial endpoint and trajectory deviations. The endpoint deviation among swarm members shows significant fluctuations, and the trajectory deviation approaches the maximum drift distance, rendering it susceptible to hijacking. Under the random decision model, the trajectory deviation of swarm content exhibits considerable fluctuations, and the time cost is elevated.

The experimental results indicate that the Consensus Potential Field (CPF) method exhibits superior performance, achieving a E_e of 10.32 meters and a E_r of 4.35 meters. This performance significantly surpasses that of baseline methods such as Game (E_e = 20.19 m, E_r = 16.28 m), PID (E_e = 18.04 m, E_r = 3.68 m), PSO (E_e = 116.91 m, E_r = 42.09 m), and Random (E_e = 21.21 m, E_r = 29.83 m). Notably, CPF maintains a 100% survival rate compared to Random's 66.67% and achieves a balanced total path length of 1498.65 meters, demonstrating its capability to mitigate spoofing-induced deviations while preserving swarm coherence. The CPF method's key advantages include minimal trajectory drift (4.35 m, 73% lower than Game), precise destination targeting (10.32 m, 44% better than PID), and robust reliability (100% survival rate). These findings substantiate CPF's superiority in terms of accuracy, stability compared to baseline methods.

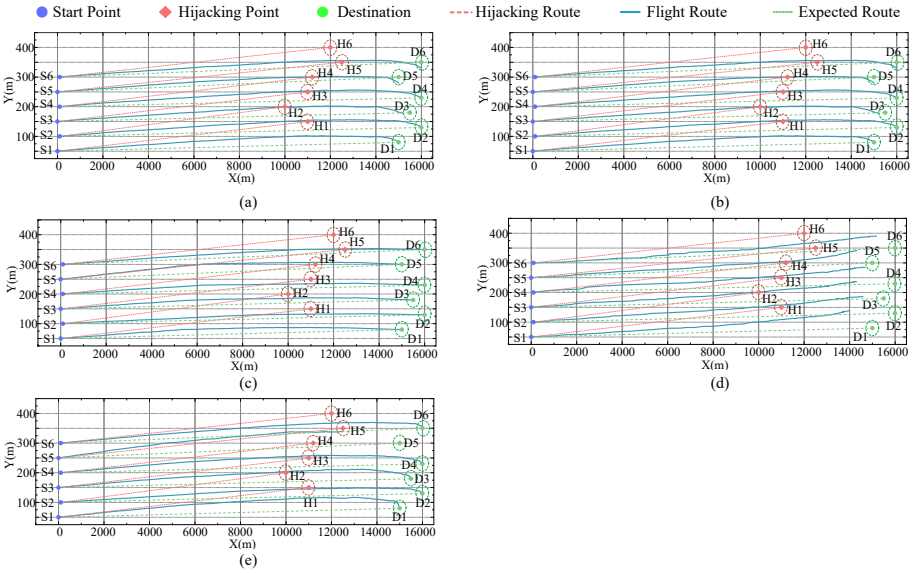

Fig. 5. Swarm Flight Trajectory in different methods:
(a) Trajectory in CPF model, (b) Trajectory in Game model, (c) Trajectory in PID model, (d) Trajectory in PSO model, (e) Trajectory in Random model.

Fig. 5 illustrates the flight trajectory of the swarm under five defense strategies, including the proposed method. In Fig. 5 (a), the group effectively defends against a malicious attack using the CPF model, reaching the safe zone within the specified time. Conversely, Figure 4(b) displays a notable deviation in the flight path of node 5, caused by intersecting with the hijacking path shortly after takeoff. Fig. 5 (c) exhibits a distinct deviation in trajectory compared to Fig. 5 (b), resulting in two members falling victim to hijacking. In the scenario of a spoofing attack as depicted in Fig. 5 (d), the swarm's flight path, controlled by the particle swarm optimization model, experiences a significant deviation, impeding task completion. Lastly, Fig. 5 (e) portrays a population safeguarded by a random decision model, leading to substantial trajectory bias and member hijacking.

5 Conclusion and Outlook

This paper addresses the navigation security issue of UAV swarms under yaw spoofing attacks. An asymmetric attack-defense simulation scenario based on environmental noise is constructed. By integrating spatial relationship modeling, it predicts the location of hijacking points, solves the problem of potential field estimation under an unknown repulsive force field, and realizes heading calibration through a model-free lightweight collaborative defense method based on the Consensus Potential Field (CPF).The experimental results show that that CPF has achieved the collaborative optimization of high-precision navigation, low trajectory drift, and high swarm coop-

eration reliability under spoofing attacks, providing an efficient solution for UAV swarms to resist yaw spoofing.

Acknowledgements. This work was supported in part by the National Natural Science Foundation of China under Grant U2333201 and in part by the fundamental research funds for the central universities of Civil Aviation University of China under No. 3122025054.

References

1. Zhao, X., Wang, L., Qi, F., Wang, J.: Research on propagation mechanism for gyro installation error of dual-axis rotational inertial navigation system in UAV coordinated U-turn. Measurement. 234, 114808 (2024).
2. Liu, Y., Noguchi, N., Liang, L.: Development of a positioning system using UAV-based computer vision for an airboat navigation in paddy field. Computers and Electronics in Agriculture. 162, 126–133 (2019).
3. Wu, S., Chen, Z., Bangura, K., Jiang, J., Ma, X., Li, J., Peng, B., Meng, X., Qi, L.: A navigation method for paddy field management based on seedlings coordinate information. Computers and Electronics in Agriculture. 215, 108436 (2023).
4. Guo, Y., Wu, M., Tang, K., Tie, J., Li, X.: Covert Spoofing Algorithm of UAV Based on GPS/INS-Integrated Navigation. IEEE Transactions on Vehicular Technology. 68, 6557–6564 (2019).
5. Dang, Y., Benzaïd, C., Yang, B., Taleb, T., Shen, Y.: Deep-Ensemble-Learning-Based GPS Spoofing Detection for Cellular-Connected UAVs. IEEE Internet of Things Journal. 9, 25068–25085 (2022).
6. Fan, Y., Zhang, Z., Trinkle, M., Dimitrovski, A.D., Song, J.B., Li, H.: A Cross-Layer Defense Mechanism Against GPS Spoofing Attacks on PMUs in Smart Grids. IEEE Transactions on Smart Grid. 6, 2659–2668 (2015).
7. Bada, M., Boubiche, D.E., Lagraa, N., Kerrache, C.A., Imran, M., Shoaib, M.: A policy-based solution for the detection of colluding GPS-Spoofing attacks in FANETs. Transportation Research Part A: Policy and Practice. 149, 300–318 (2021).
8. Liang, W., Li, K., Li, Q.: Anti-spoofing Kalman filter for GPS/rotational INS integration. Measurement. 193, 110962 (2022).
9. He, J., Gong, X.: Resilient Path Planning of Unmanned Aerial Vehicles Against Covert Attacks on Ultrawideband Sensors. IEEE Transactions on Industrial Informatics. 19, 10892–10900 (2023)
10. Zhang, Z.-C., Hou, F., Wang, D.-W., Liu, J., Zhao, W.-S.: PSO-Algorithm-Assisted Design of Compact SSPP Transmission Line. IEEE Microwave and Wireless Technology Letters. 33, 247–250 (2023).
11. Nayfeh, M., Li, Y., Shamaileh, K.A., Devabhaktuni, V., Kaabouch, N.: Machine Learning Modeling of GPS Features with Applications to UAV Location Spoofing Detection and Classification. Computers & Security. 126, 103085 (2023).
12. Fan, J., Chen, X., Liang, X.: UAV trajectory planning based on bi-directional APF-RRT* algorithm with goal-biased. Expert Systems with Applications. 213, 119137 (2023).

13. Wei, X., Wang, Y., Sun, C.: PerDet: Machine-Learning-Based UAV GPS Spoofing Detection Using Perception Data. Remote Sensing. 14, 4925 (2022).
14. Talaei Khoei, T., Al Shamaileh, K., Devabhaktuni, V.K., Kaabouch, N.: Performance analysis of capsule networks for detecting GPS spoofing attacks on unmanned aerial vehicles. Int. J. Inf. Secur. 24, 62 (2025).
15. Dang, Y., Benzaid, C., Yang, B., Taleb, T., Shen, Y.: Deep-Ensemble-Learning-Based GPS Spoofing Detection for Cellular-Connected UAVs. IEEE Internet Things J. 9, 25068–25085 (2022).
16. Meng, L., Zhang, L., Yang, L., Yang, W.: A GPS-Adaptive Spoofing Detection Method for the Small UAV Cluster. Drones. 7, 461 (2023).
17. Zajdel, R., Sośnica, K., Bury, G.: Geocenter coordinates derived from multi-GNSS: a look into the role of solar radiation pressure modeling. GPS Solut. 25, 1 (2020).
18. He, D., Yang, G., Li, H., Chan, S., Cheng, Y., Guizani, N.: An Effective Countermeasure Against UAV Swarm Attack. IEEE Network. 35, 380–385 (2021).
19. Eldosouky, A., Ferdowsi, A., Saad, W.: Drones in Distress: A Game-Theoretic Countermeasure for Protecting UAVs Against GPS Spoofing. IEEE Internet of Things Journal. 7, 2840–2854 (2020).
20. Gu, Z., Zhao, H., Wang, J., Tan, R., Nie, L.: A Defense Strategy for UAV Swarm Against GNSS Spoofing Attacks Based on Game Model. In: Huang, D.-S., Zhang, X., and Chen, W. (eds.) Advanced Intelligent Computing Technology and Applications. pp. 383–395. Springer Nature Singapore, Singapore (2024).
21. Guo, Y., Cao, J., Tang, K., Luo, K., Geng, X.: Anti-Unmanned Directional Drive-Off Method Under Integrated Navigation Mode. IEEE Transactions on Automation Science and Engineering. 22, 2607–2616 (2025).
22. Sedjelmaci, H., Senouci, S.M., Ansari, N.: A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks. IEEE Transactions on Systems, Man, and Cybernetics: Systems. 48, 1594–1606 (2018).