

Remote ID Spoofing-Aware Trajectory Planning for Small Unmanned Aerial Systems

Jeremiah Webb¹, Bryce Bjorkman¹, Abel Diaz Gonzalez¹, Austin Coursey¹

Noah Dahle¹, Kailani Lemieux Mack¹, Filippos Fotiadis², Gautam Biswas¹, Bryan C. Ward¹, Abenezer Taye¹

¹Vanderbilt University, Nashville, TN, USA

²The University of Texas at Austin, Austin, TX, USA

Abstract—This work presents a decentralized, spoofing-aware trajectory planning framework for small unmanned aerial systems operating under Remote Identification (RID) location spoofing attacks. Existing planners typically assume RID broadcasts are trustworthy, which can increase the risk of loss of separation and mid-air collisions when spoofing occurs. In contrast, the proposed approach explicitly treats RID information as unverified and incorporates physical-layer observations to assess broadcast credibility. Received signal-strength measurements from neighboring aircraft are used to detect spoofing and probabilistically localize a spoofing agent. The resulting uncertainty is converted into a risk-bounded unsafe region using a chance-constrained formulation and integrated into a per-agent Markov decision process-based planner. This enables real-time, decentralized collision avoidance while preserving mission objectives and scalability. Simulation results in a multi-aircraft package delivery scenario demonstrate reduced near mid-air collision events compared to planners that assume truthful RID data, while maintaining computational efficiency suitable for real-time execution. [Code]¹

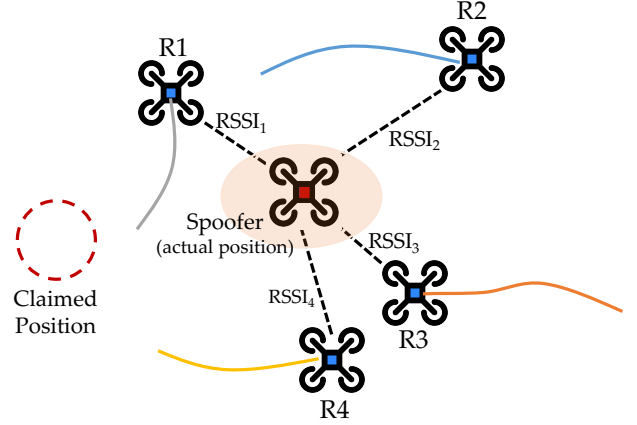


Fig. 1: Spoofing-aware trajectory planning framework.

I. INTRODUCTION

Small Unmanned Aerial Systems (sUAS) are increasingly deployed in a wide range of civilian and commercial applications, including surveillance, precision agriculture, and package delivery. The safe and scalable integration of these aircraft into shared low-altitude airspace relies on the use of Remote Identification (RID), a Federal Aviation Administration-mandated broadcast-based communication protocol that transmits aircraft state information, such as position, velocity, and identification, using unencrypted and unauthenticated wireless messages. While RID improves situational awareness, accountability, and scalability of sUAS operations, its lack of built-in security mechanisms exposes these operations to significant cyber vulnerabilities [1].

Because RID is a relatively recent regulatory requirement, research specifically addressing RID spoofing is limited. However, a broader body of literature has investigated the problem of verifying the true location of an aircraft from signal observations to detect inconsistencies between claimed and physical positions. Among these, [1] and [2] provide a comprehensive overview of RID spoofing attacks and defense strategies. However, the proposed countermeasures are mostly authentication-based, which violates the plain text broadcast assumption of RID. [3] uses multilateration with synchronized

receivers to estimate transmitter location and compare it with broadcast claims. However, the approach requires dense, time-synchronized ground receivers. [4] analyzes temporal consistency of broadcast messages to detect anomalous trajectories with a goal of validating reported trajectories over time, but their method assumes that broadcast data is mostly trustworthy. [5] studies RID spoofing detection using Received Signal Strength Indicator (RSSI) inconsistencies and geometric constraints. Similarly, [6] leveraged receiver motion-induced Doppler shifts to detect GNSS spoofing attacks, while [7] proposed data-driven methods for spoofing detection. However, these studies focus only on detection and do not address the problem of dynamically estimating the true location of the spoofer. In this work, we adopted a state estimator-based approach, combined with range-based multilateration, to estimate the true location of the spoofer aircraft, as illustrated in Fig. 1.

On the other hand, there is a rich body of literature for multi-agent trajectory planning methods. Decentralized methods, where each aircraft resolves conflicts locally, are generally preferred over centralized planners due to their robustness and scalability. Among these, [8] formulates a chance-constrained trajectory planning problem that converts uncertainty into risk-bounded unsafe regions and enforces probabilistic safety guarantees. [9] proposes an MDP-based trajectory planning framework that enables scalable real-time decision-making

¹<https://github.com/brycethebjorkman/uli-net-sim/tree/spoofing-aware-trajectory-planning>

by balancing safety and goal progress. [10] introduces the velocity obstacle framework for collision avoidance in dynamic environments by predicting future conflicts based on relative motion. [11] extends this idea to reciprocal collision avoidance, where agents cooperatively adjust their velocities to avoid collisions. [12] proposes conflict-based search for multi-agent trajectory planning, which resolves collisions through hierarchical constraint refinement. However, it is primarily designed for discrete environments and assumes full knowledge of agent states. Similarly, [13] presented a reinforcement learning approach combined with robust optimization to achieve probabilistic safety guarantees under uncertainty. Further, [14] has shown that a distributed model predictive control approach can achieve high scalability in handling multi-agent collision avoidance. All of these trajectory planners rely on accurate knowledge of neighboring agent states and do not consider adversarially falsified RID broadcasts.

The key contribution of this work is enabling safe trajectory planning in the context where RID broadcasts are not inherently trustworthy due to location spoofing attacks. We proposed a framework that estimates the true location of an aircraft using physical-layer observations and generates safe trajectories for all aircraft in the environment. The proposed framework consists of three tightly coupled components: (i) spoofing detection, (ii) spoofer localization and unsafe area determination under uncertainty, and (iii) risk-aware trajectory planning. The aircraft are only expected to coordinate in spoofing detection and localization with a ground control station, which computes spoofer state estimates and broadcasts the unsafe regions to avoid, while agents maintain independent trajectory planning and execution, eliminating the need for a centralized planner.

The remainder of this paper is organized as follows. Section II provides a brief discussion of the necessary background material related to RID broadcasts. Section III presents the problem formulation and provides an overview of our approach. In Section IV, we describe how the spoofing detection and localization scheme works. We then discuss how the risk-domain region is constructed and how the safe trajectories are computed in Section V. Section VI explains the simulation architecture. Finally, Section VII presents the implemented drone package delivery scenario and evaluates safety and computational runtime performance. The paper concludes with Section VIII.

II. BACKGROUND

In this section, we outline the background material related to RID broadcasts, which are the central focus of this study.

A. Remote ID

The Federal Aviation Administration (FAA) requires unmanned aircraft operating in U.S. airspace to periodically broadcast Remote Identification (RID) messages. These broadcasts provide situational awareness information to nearby observers and airspace management systems. A standard Re-

mote ID-enabled aircraft must transmit the following message elements [15]:

- 1) Aircraft identity, consisting of either:
 - a) A manufacturer-assigned serial number, or
 - b) A session ID.
- 2) Latitude and longitude of the control station.
- 3) Geometric altitude of the control station.
- 4) Latitude and longitude of the unmanned aircraft.
- 5) Geometric altitude of the unmanned aircraft.
- 6) Velocity of the unmanned aircraft.
- 7) A time mark corresponding to the Coordinated Universal Time (UTC) of the position measurement.
- 8) Emergency status of the unmanned aircraft.

Many small unmanned aircraft systems (sUAS) lack on-board sensing capable of reliably detecting nearby aircraft. Consequently, RID information can be used to support collision avoidance and situational awareness. However, RID is susceptible to spoofing attacks in which a malicious transmitter broadcasts false state information. Such attacks can lead to loss of separation and reduced operational safety, potentially compromising mission integrity.

III. PROBLEM FORMULATION

A. Problem Description

We consider an unstructured urban airspace in which a decentralized, homogeneous fleet of multirotor aircraft operates in a free-flight manner across a city-scale environment. Each aircraft is tasked with delivering a package from an initial warehouse location to a designated delivery site. In addition, we model a spoofing aircraft with a trajectory that is not known a priori and that broadcasts a falsified RID position. The objective of this study is to estimate the true location of this aircraft and generate safe trajectories for the benign aircraft in the environment. These trajectories enable the benign aircraft to avoid collision with the spoofer aircraft and reach their destinations safely.

B. Aircraft Model

Each aircraft evolves in discrete time according to

$$\zeta_{t+1} = f(\zeta_t, \mathbf{u}_t), \quad (1)$$

where $\zeta_t \in \mathcal{X} \subset \mathbb{R}^n$ denotes the aircraft state at time step $t \in \mathbb{Z}^+$, and $\mathbf{u}_t \in \mathcal{U} \subset \mathbb{R}^m$ is the control input at time step t , with $\mathcal{U}$ being the action set containing all the control action combinations for an aircraft. The state ζ_t consists of position, velocity, attitude, and angular rates. The control input is given by the total thrust and body torques, $\mathbf{u}_t = (T_t, \tau_{\phi_t}, \tau_{\theta_t}, \tau_{\psi_t})$. The function f is obtained by discretizing a continuous-time six-degrees-of-freedom (6-DoF) dynamic model of an octorotor [16]. The underlying continuous-time dynamics is given by

$$\dot{\zeta} = \begin{cases} \ddot{x} = (s\theta c\psi c\phi + s\phi s\psi) \frac{T}{m_t}, \\ \ddot{y} = (s\theta s\psi c\phi - s\phi c\psi) \frac{T}{m_t}, \\ \ddot{z} = -g + c\phi c\theta \frac{T}{m_t}, \\ \dot{\phi} = p + q s\phi t\theta + r c\phi t\theta, \\ \dot{\theta} = q c\phi - r s\phi, \\ \dot{\psi} = q \frac{s\phi}{c\theta} + r \frac{c\phi}{c\theta}, \\ \dot{p} = \frac{I_{yy} - I_{zz}}{I_{xx}} qr + \frac{l}{I_{xx}} \tau_\phi, \\ \dot{q} = \frac{I_{zz} - I_{xx}}{I_{yy}} pr + \frac{l}{I_{yy}} \tau_\theta, \\ \dot{r} = \frac{I_{xx} - I_{yy}}{I_{zz}} pq + \frac{l}{I_{zz}} \tau_\psi, \end{cases} \quad (2)$$

where s , c , and t represent $\sin$, $\cos$, and $\tan$ functions, respectively. The thrust T is selected from nine logarithmically spaced values between 50 and 500 N, and each torque component is selected from seven uniformly spaced values between -150 and 150 Nm.

Assumption 1 (Communication and sensing model). All agents are RID-enabled and periodically broadcast state information at a fixed transmit power. The aircraft ID information in the RID messages are assumed to be authentic.

Assumption 2 (Aircraft behavior and system model). All agents are cooperative and share identical multirotor dynamics, except for a single adversarial aircraft performing a spoofing attack, whose dynamics remain unknown to the cooperative agents. Unless spoofing is detected, RID-reported states are treated as reliable by neighboring agents.

IV. SPOOFING DETECTION AND LOCALIZATION

A. Spoofing Detection

Because RID messages are not inherently trustworthy, additional observations are often used to assess their consistency. In this paper, we use physical-layer measurements, such as the received signal strength indicator (RSSI), to provide an independent source of information about the transmitter's location. These measurements can be used to infer an estimate of the transmitter position, which is then compared with the position reported in the RID message. The discrepancy between the inferred and reported states serves as a way to verify the truthfulness of the broadcast message. We refer to this process as RID spoofing detection.

In this work, we adopt a spoofing detection scheme from [5]. Here, we provide a brief summary of how the approach works. The method uses a Kalman filter to monitor the consistency between predicted and observed measurements through the innovation sequence. If a significant deviation, quantified by the Normalized Innovation Squared (NIS), is observed, then there is a mismatch between the physical-layer observation and the expected location of the transmitter. Thus, spoofing is detected.

B. Spoofing Localization

Once spoofing is detected, a key step in the safe trajectory planning process is dynamically estimating the true location of the malicious aircraft. We refer to this process as spoofing localization. We formulate the spoofing localization problem as a state estimation problem, where an interacting multiple model uses different motion hypotheses for the spoofer in the prediction step, and the position of the spoofer computed from a range-based multilateration approach is used in the correction step. In this subsection, we discuss how each component is formulated and implemented.

1) *Interacting Multiple Model:* A key challenge in estimating the true location of the spoofer is the lack of knowledge of the spoofer aircraft dynamics and its intended maneuver. To address this challenge, we adopt a Bayesian filtering method known as the IMM filter [17]. The intuition behind the IMM filter is to use multiple filters in parallel to track the target, each with a different motion hypothesis. The final estimate is computed by assigning different weights to each estimate.

In this study, we adopt constant velocity (CV) and constant acceleration (CA) motion hypotheses for the spoofer. The system and measurement models of these hypotheses have a general structure of the form

$$\begin{cases} \mathbf{x}_{t+1}^{(m)} = \mathbf{F}^{(m)} \mathbf{x}_t^{(m)} + \mathbf{w}_t^{(m)}, & \mathbf{w}_t^{(m)} \sim \mathcal{N}(\mathbf{0}, \mathbf{Q}^{(m)}), \\ \mathbf{z}_t = \mathbf{H}^{(m)} \mathbf{x}_t^{(m)} + \mathbf{v}_t, & \mathbf{v}_t \sim \mathcal{N}(\mathbf{0}, \mathbf{R}). \end{cases} \quad (3)$$

where $m \in \{\text{CV}, \text{CA}\}$, $\mathbf{F}$ and $\mathbf{H}$ are the system and measurement models, and $\mathbf{w}$ and $\mathbf{v}$ denote the process and measurement noises, with $\mathbf{Q}$ and $\mathbf{R}$ being the corresponding process and measurement noise covariances.

We now describe how the system and measurement models for the general structure described in (3) are defined for both CV and CA motion hypotheses.

a) *Constant Velocity (CV) Model:* The equation of motion for the CV model is defined as a linear prediction of the spoofer's state from a previous time step to the time of the measurements, where the state vector is composed of the linear position and velocity components. The system and measurement models for the CV model are given as:

$$\mathbf{F}^{\text{CV}} = \begin{bmatrix} \mathbf{I}_3 & \Delta t \mathbf{I}_3 \\ \mathbf{0} & \mathbf{I}_3 \end{bmatrix}, \quad \mathbf{H}^{\text{CV}} = [\mathbf{I}_3 \quad \mathbf{0}_{3 \times 3}]. \quad (4)$$

b) *Constant Acceleration (CA) Model:* The equation of motion for the CA model is defined as a linear prediction of the spoofer's state from a previous time step to the time of the measurements, where the state vector is composed of the linear position, velocity, and acceleration components. The system and measurement models for the CA model are given as:

$$\mathbf{F}^{\text{CA}} = \begin{bmatrix} \mathbf{I}_3 & \Delta t \mathbf{I}_3 & \frac{1}{2} \Delta t^2 \mathbf{I}_3 \\ \mathbf{0} & \mathbf{I}_3 & \Delta t \mathbf{I}_3 \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_3 \end{bmatrix}, \quad \mathbf{H}^{\text{CA}} = [\mathbf{I}_3 \quad \mathbf{0}_{3 \times 6}]. \quad (5)$$

At each time step, the two filters (i.e., those based on CV and CA motion hypotheses) execute the standard Kalman

filter predict–update cycle and provide the state estimate $\hat{\mathbf{x}}_t^{(m)}$, covariance $\mathbf{P}_t^{(m)}$, and model probability $\mu_t^{(m)}$ (computed from the innovation likelihood). The fused estimate is then obtained by combining the outputs of these two filters as

$$\hat{\mathbf{x}}_t = \sum_m \mu_t^{(m)} \hat{\mathbf{x}}_t^{(m)}, \quad (6)$$

$$\mathbf{P}_t = \sum_m \mu_t^{(m)} \left(\mathbf{P}_t^{(m)} + (\hat{\mathbf{x}}_t^{(m)} - \hat{\mathbf{x}}_t)(\hat{\mathbf{x}}_t^{(m)} - \hat{\mathbf{x}}_t)^\top \right). \quad (7)$$

These fused position estimate and covariance values are used as the spoofer position estimate for downstream planning.

A key parameter in the IMM filter that defines the probability that the spoofer switches from one motion hypothesis to another is the state transition matrix. The specific state transition matrix and all other IMM filter related parameters used in this paper are presented in Table IV.

2) *Multilateration*: The measurement used for the update stage of the IMM filter ($\mathbf{z}_t$) is obtained via a process known as federated multilateration. In this approach, the position of the spoofer is determined when at least four receivers are available (three positional unknowns and transmission power). The multilateration procedure depends on computing the range estimates inferred from a free-space path loss model of wireless signal propagation [18]:

$$P_r(d) = P_t - 20 \log_{10}(d) - 20 \log_{10}(\hat{f}) - 32.44 \quad (8)$$

where d denotes the transmitter–receiver distance and $\hat{f}$ denotes transmission frequency. In addition, P_r and P_t denote received and transmission powers, respectively. In this study, we assume the RID messages are transmitted at 2.4 GHz. When at least four receivers observe a transmission, the GCS performs multilateration by jointly estimating transmitter position in 3D space ($\mathbf{x} \in \mathbb{R}^3$) and transmit power P_t via nonlinear least squares,

$$\min_{\mathbf{x}, P_t} \sum_i (P_{r_i} - (P_t - 20 \log_{10} \|\mathbf{x} - \mathbf{r}_i\| - 40.04))^2, \quad (9)$$

where $\mathbf{r}_i$ are the known positions of the receiving agents. The above optimization problem is solved using a non-linear least-squares solver based on the Trust Region Reflective (TRF) algorithm, as implemented in SciPy [19]. Because the cost function is non-convex due to the nonlinear dependence of the received power on the logarithm of the Euclidean distance $\|\mathbf{x} - \mathbf{r}_i\|$, the optimization may admit multiple local minima, and solution quality depends on initialization. Consequently, we initialized the solver from the current estimate or the centroid of receiver positions.

V. RISK-AWARE TRAJECTORY PLANNING

In this section, we discuss the last component of the proposed framework that generates the safe trajectories.

A. Chance-Constrained Unsafe Region

After obtaining a probabilistic estimate of the spoofer location, we convert it into a deterministic unsafe region using a chance-constrained formulation. The following definition adopts the formulation in [8].

Definition 1 (Chance-constrained unsafe region). Let $\hat{\mathbf{x}}_t \in \mathbb{R}^3$ and $\mathbf{P}_t \in \mathbb{R}^{3 \times 3}$ denote the mean and covariance of the spoofer location estimate obtained from the IMM filter at time step t . Let $\mathbf{x}_t \in \mathbb{R}^3$ denote the position of the aircraft.

For a given risk level $\alpha \in (0, 1)$, the chance-constrained safe set is defined as

$$(\mathbf{x}_t - \hat{\mathbf{x}}_t)^\top \mathbf{P}_t^{-1} (\mathbf{x}_t - \hat{\mathbf{x}}_t) > F_{\chi_3^2}^{-1}(1 - \alpha), \quad (10)$$

and the corresponding unsafe region is given by the complement of this set.

The threshold $F_{\chi_3^2}^{-1}(1 - \alpha)$ denotes the inverse cumulative distribution function of a chi-squared random variable with three degrees of freedom, corresponding to the three-dimensional uncertainty in the spoofer location estimate. Satisfaction of (10) ensures that the probability of the aircraft entering the unsafe region does not exceed α , i.e.,

$$\Pr\left((\mathbf{x}_t - \hat{\mathbf{x}}_t)^\top \mathbf{P}_t^{-1} (\mathbf{x}_t - \hat{\mathbf{x}}_t) \leq F_{\chi_3^2}^{-1}(1 - \alpha)\right) \leq \alpha, \quad (11)$$

which implies that $\mathbf{x}_t$ lies outside the risk domain with confidence $1 - \alpha$.

Geometrically, the inequality defines an ellipsoidal unsafe region centered at $\hat{\mathbf{x}}_t$, whose size is determined by the spoofer location uncertainty $\mathbf{P}_t$ and the risk parameter α . A well-conditioned covariance matrix, corresponding to favorable observer geometry, results in a compact and nearly isotropic ellipsoid. In contrast, poor geometries (e.g., near-coplanar observer configurations) lead to ill-conditioned covariance matrices, producing elongated ellipsoids that reflect increased uncertainty along certain directions.

B. Trajectory Planner

The trajectory planner implemented in this paper, introduced in [9], formulates the decision-making problem as a Markov decision process (MDP). A significant update to the current planner, compared to [9], is the use of chance-constrained formulation presented in Section V-A for collision avoidance with the true location of the spoofer aircraft.

The state transition function and the action set used in the MDP formulation are the aircraft model and the control actions presented in Section III-B. Therefore, in this section, we focus on how the reward function is designed.

1) *Reward Function*: The reward function is the primary mechanism for controlling the behavior of an MDP agent. In this work, we utilize both positive and negative rewards, as presented in Table I, to guide the aircraft to their destination while avoiding potential collisions with the spoofer aircraft and other nearby benign aircraft. As shown in Table I, the positive rewards are placed at the assigned destinations, and the negative rewards are assigned within the chance-constrained unsafe

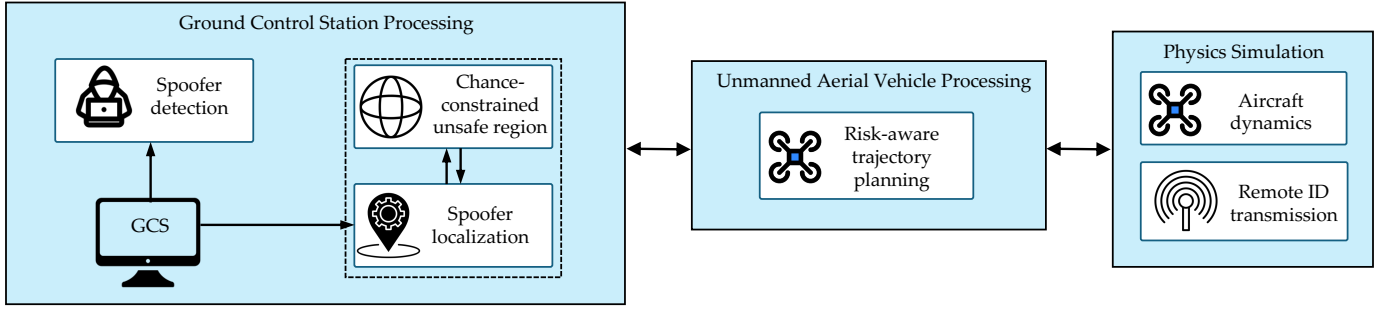


Fig. 2: System architecture.

TABLE I: Reward Function for Each Aircraft

Component	Reward	Region	Decay
Goal attraction	200	Goal state	0.999
Collision (benign)	$-(100t + 500)$	$d_{ij} \leq d_{\text{safe}}$	0.97
Collision (spoofer)	-1000	$\mathbf{x}_t \in \mathcal{X}_{\text{unsafe}}(\alpha)$	0.97

region of the spoofer aircraft. In addition, to prevent benign-to-benign aircraft collision, we placed a negative reward in the vicinity of nearby benign aircraft whenever the safe inter-aircraft distance threshold ($d_{ij} \leq d_{\text{safe}}$) is violated.

At each planning update, an aircraft generates a set of possible future states using its dynamic model and action set in a receding horizon manner. It then computes the value of each projected future state using the positive and negative rewards defined in Section I. Finally, it selects the control action from the action set that maximizes the total reward.

VI. SYSTEM ARCHITECTURE

The proposed spoofing-aware trajectory planning framework is implemented in the OMNeT++ simulator. OMNeT++ is a discrete-event simulator [20] with the INET Framework [21] that simulates physical-layer signal propagation while accounting for factors that affect signal propagation, including distance, transmission power, and environmental conditions. However, multipath effects, channel throughput, and packet loss are not modeled in this work and are left for future investigation.

To facilitate the simulation, all parameters relevant to signal propagation, including the path loss model and the aircraft model, are implemented in OMNeT++ using the C++ programming language. Meanwhile, the risk-aware MDP-based trajectory planner is implemented in Python and re-plans the trajectories of each aircraft every 0.5 s. To avoid coupling downstream behavior to variable detector trigger times, we use a forced spoofing alert for the designated serial number of the adversarial aircraft at 5 s. As discussed in [5], open-loop detector timing depends strongly on scenario geometry; fixing the alert time isolates subsequent localization and planning effects for the experiments reported here.

Each aircraft transmits RID beacons at 1 Hz, and RSSI observations are forwarded to the GCS for spoofing detection

and localization. The GCS executes periodic updates every 0.25 s and propagates a per-spoof IMM state estimate at each decision-making step. The chance-constrained formulation is then used to convert the probabilistic estimate of the spoofer location into a deterministic unsafe region. The resulting unsafe-region parameters are broadcast to the aircraft and incorporated into onboard planning through reward functions designed to avoid unsafe areas. A schematic diagram depicting the system architecture is shown in Fig. 2.

VII. RESULTS AND DISCUSSION

A. Scenario Description

We evaluate the proposed spoofing-aware trajectory planning framework in a drone package-delivery operation with multiple benign drones and one active spoofer. The operation is implemented within a 1 km $\times$ 1 km urban environment modeled after the FAA UTM framework for low-altitude airspace integration [22]. In this setting, there are three depot locations, which serve as hubs where drones are stationed for charging, maintenance, and package loading. A single scenario in this operation includes a varying number of traffic densities for the benign aircraft (4, 8, 12, 16), starting at the hubs and crossing the airspace to delivery sites. In addition, in each scenario, there is a single spoofer aircraft whose dynamic model and intended trajectory are unknown. In this scenario, the spoofer follows a straight-line trajectory to its goal while broadcasting a constant position offset from its true state in its RID messages and performing no collision avoidance.

To better evaluate the efficacy of the proposed framework, we use a trajectory planner that assumes all RID broadcast messages are truthful as a baseline. For each scenario, we run 30 experiments with matched seeds for the two planners². These 30 runs enable us to statistically isolate the effects of randomness arising from communication (e.g., communication timing and radio frequency (RF) signal noise) and scenario-specific variabilities (e.g., random assignments of delivery destinations).

B. Metrics

The goal of this study is to develop a multi-agent trajectory planning framework that enables safe movement of aircraft

²A sample video of the simulation for 8 aircraft can be found here: <https://youtu.be/LTTAv5DEp5U>

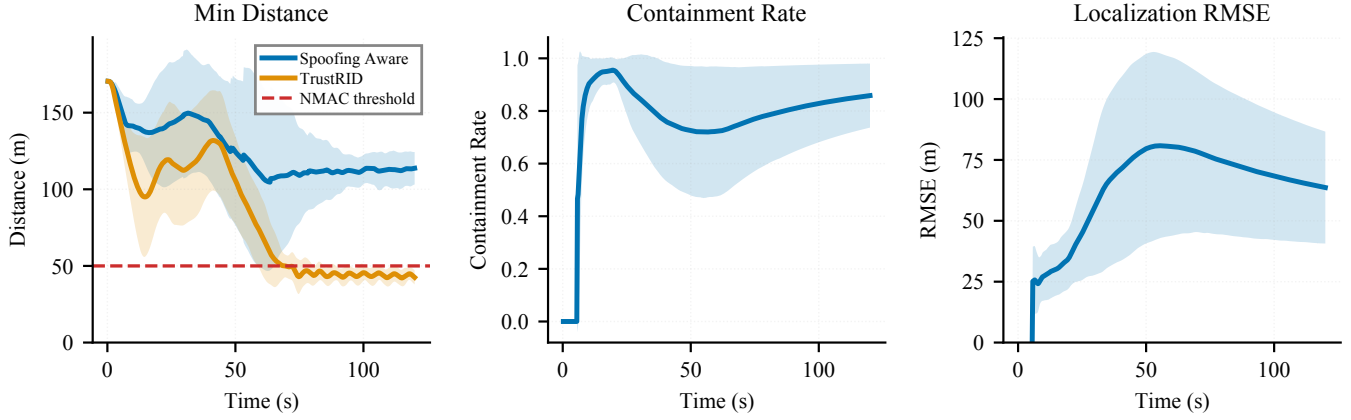


Fig. 3: Performance metrics over time for the scenario with 16 agents. (Left) minimum distance to the spoofer; (Middle) containment rate; (Right) localization accuracy. Solid lines represent the mean values, while shaded regions indicate the range between the minimum and maximum values.

in the presence of location spoofing attacks. To that end, the framework is expected (i) to effectively identify the true location of the spoofer and track it throughout the entire duration of the operation, (ii) to perform risk-aware trajectory planning for each aircraft with a user-defined risk threshold, and (iii) to achieve this in a scalable manner. As such, we use the following metrics to evaluate the proposed framework and compare its performance with a baseline trajectory planner:

- **Localization containment rate (LCR):** indicates the fraction of time the true spoofer position is contained within the estimated chance-constrained ellipsoid. This is the primary performance indicator for the spoofer localization component of the framework.
- **Near mid-air collisions (NMACs):** indicates events where separation is below 50 m. This threshold is chosen based on a maximum aircraft speed of 8 m/s and a minimum separation time of 3 seconds for two aircraft heading towards each other. We report three variants of NMAC: (i) benign–benign pairwise proximity, (ii) benign–true-spoofers proximity, and (iii) benign entry into the spoofing unsafe (chance-constrained) ellipsoid.
- **Computational cost:** the time taken by the framework to complete a flight mission for all aircraft involved.

C. Results and Discussion

1) *Safety:* We evaluated our proposed framework across different traffic levels, and in the presence of a single spoofer. The NMAC results are provided in Table II. From the results, it can be seen that our approach showed substantial NMAC performance improvement compared to the baseline. Specifically, the total NMAC means were lower under our approach for every scenario. In addition, the strongest safety improvement appears in the benign–spoofers interaction metric. In the moderate- and high-density cases, our proposed approach substantially suppresses close encounters with the malicious aircraft.

This traffic density-dependent widening of the performance gap observed between our approach and the baseline indicates that risk-aware avoidance is most beneficial precisely when interaction pressure is highest. The 4-agent case remains a low-event regime (near-zero benign–spoofers NMACs in both planners due to sparse geometry), suggesting that the principal advantage of our approach emerges as traffic and encounter opportunities increase.

2) *Localization Containment:* Localization quality, measured by the spoofer containment rate, improved with observer density, as presented in Table II. This trend is consistent with improved RSSI observer geometry as more benign agents contribute measurements. This phenomenon is also supported by the accuracy of the localization scheme, assessed through root mean squared error (RMSE) and mean absolute error (MAE) values with respect to the ground truth. These results indicate that position error improves with density and that the largest geometric and observability limitations occur in the minimum-observer case. The results are consistent with the previous observation, i.e., the more the number of aircraft in the environment, the better the localization accuracy.

Furthermore, the maximum unsafe-ellipsoid radius remains relatively stable across scenarios, with a modest increase in size as the number of aircraft increases. Together, these results suggest that while four observers satisfy the minimum requirement for RSSI NLLS multilateration, this configuration is underconstrained in practice and yields high-variance localization; hence, adding observers substantially improves both localization accuracy and containment reliability.

Finally, in Fig. 3, we report the progression of these safety and spoofer localization performance metrics over time for 16 aircraft to better illustrate the performance of the proposed framework. As shown in the figure, the minimum distance to the spoofer remains above the NMAC threshold for the proposed framework. In contrast, the baseline trajectory planner incurs significant safety violations once the environment becomes crowded. In addition, the containment rate and the lo-

TABLE II: Safety and spoofer-localization metrics across different traffic densities

Metric	4 Agents	8 Agents	12 Agents	16 Agents
Safety Metrics (SA)				
Total NMACs	0.300 $\pm$ 0.466	1.733 $\pm$ 1.230	4.067 $\pm$ 2.545	7.000 $\pm$ 3.311
Benign–Benign	0.267 $\pm$ 0.450	1.633 $\pm$ 1.273	3.700 $\pm$ 2.409	6.767 $\pm$ 3.245
Benign–Spoofer	0.033 $\pm$ 0.183	0.100 $\pm$ 0.305	0.367 $\pm$ 0.556	0.233 $\pm$ 0.568
Unsafe violations	2.700 $\pm$ 3.669	0.933 $\pm$ 1.230	1.533 $\pm$ 2.177	3.033 $\pm$ 2.965
Safety Metrics (RID)				
Total NMACs	0.267 $\pm$ 0.450	1.933 $\pm$ 1.507	4.933 $\pm$ 1.929	8.967 $\pm$ 3.264
Benign–Benign	0.267 $\pm$ 0.450	1.200 $\pm$ 1.064	3.533 $\pm$ 1.655	6.767 $\pm$ 2.967
Benign–Spoofer	0.000 $\pm$ 0.000	0.733 $\pm$ 0.691	1.400 $\pm$ 0.814	2.200 $\pm$ 0.805
Unsafe violations	–	–	–	–
Localization Metrics (SA only)				
Containment rate	0.478 $\pm$ 0.259	0.804 $\pm$ 0.186	0.894 $\pm$ 0.109	0.839 $\pm$ 0.106
RMSE (m)	334.394 $\pm$ 434.679	71.953 $\pm$ 32.075	57.274 $\pm$ 22.065	63.649 $\pm$ 15.694
MAE (m)	239.724 $\pm$ 308.027	61.286 $\pm$ 26.111	48.596 $\pm$ 16.370	51.190 $\pm$ 11.357
Ellipsoid radius (m)	81.687 $\pm$ 6.848	87.534 $\pm$ 2.338	87.334 $\pm$ 2.075	87.885 $\pm$ 1.184

TABLE III: Computation time (sec)

Agents	Total wall-clock		GCS compute	
	SA	Trust-RID	SA	Trust-RID
4	40.07 $\pm$ 3.70	31.53 $\pm$ 4.61	5.42 $\pm$ 0.68	0.14 $\pm$ 0.02
8	83.60 $\pm$ 21.94	82.57 $\pm$ 14.72	4.66 $\pm$ 0.33	0.36 $\pm$ 0.06
12	188.40 $\pm$ 48.08	153.70 $\pm$ 27.35	6.27 $\pm$ 0.92	0.58 $\pm$ 0.12
16	221.77 $\pm$ 39.36	108.23 $\pm$ 13.56	7.24 $\pm$ 1.11	0.39 $\pm$ 0.04

Total wall-clock is the full single-process simulation time over 120 s of flight; GCS compute isolates the spoofing-aware detection, localization, and chance-constrained processing.

calization performances indicate that the proposed framework was able to consistently track the true location of the spoofer over time.

3) *Computational Cost*: Simulations were conducted on a dual-socket Intel Xeon Silver 4314 platform (2 $\times$ 16 cores, 64 logical CPUs at 2.4 GHz) with 64 GB of RAM. Runtime statistics are reported in Table III. Computational cost was evaluated by measuring wall-clock runtime for each scenario while keeping the simulation horizon fixed at 120 simulated seconds. We additionally report the GCS compute time, which isolates the spoofing-aware processing (detection, localization, and chance-constrained unsafe-region construction) from the cost of the full simulation. This setup isolates how computational cost scales with problem size.

The results show that the proposed approach incurs additional overhead relative to the baseline due to the inclusion of spoofing detection, localization, and risk-aware decision-making within the planning loop. Nevertheless, the framework exhibits near-linear scaling of runtime with respect to the number of aircraft in the environment. Furthermore, although absolute runtime increases with traffic density for both planners, the relative overhead of the proposed approach decreases at higher agent counts. The GCS compute time remains small and nearly flat across densities (roughly 5–7 s over 120 s of flight), indicating that the spoofing-aware

computation contributes little to the overall runtime.

Overall, the results indicate that the proposed spoofing-aware trajectory planning improves safety under RID spoofing while remaining practical for real-time use. Relative to the baseline trajectory planner that assumes all RID messages are truthful, our approach consistently lowers both total and spoofing-specific NMACs and increases separation from the malicious transmitter. Moreover, although four observers satisfy the minimum requirement of the localization pipeline, this case is often poorly conditioned geometrically, leading to large localization errors and impacting safety.

D. Practical Considerations

1) *Channel modeling fidelity*: The physical-layer simulation models distance-dependent attenuation through the free-space path loss model in (8), but does not yet capture multipath propagation, finite channel throughput, or packet loss. In urban environments, reflections and shadowing introduce bias and variance into RSSI measurements, which would increase the range errors entering the multilateration in (9) and degrade the localization accuracy reported in Table II. Packet loss can also reduce the number of synchronized reports below the four-receiver minimum, worsening the geometric conditioning already observed in the low-density cases. The chance-constrained formulation mitigates this risk by inflating the unsafe region in proportion to the estimate covariance, so degraded measurements yield more conservative avoidance regions rather than silent failures. Accounting for these effects in the propagation and estimation models is therefore a natural next step toward deployment.

2) *Real-time feasibility*: While the total wall-clock runtimes in Table III exceed the 120 s simulation horizon, they measure the cost of the full discrete-event simulation, including OMNeT++/INET event processing, dynamics integration, GCS estimation, and the planners for all agents, executed sequentially within a single process. They therefore reflect simulation cost rather than the per-component latency that

governs real-time execution. The spoofing-aware computation introduced in this work resides in the GCS; in the 16-agent scenario it consumes only 7.24 ± 1.11 s over 120 s of flight, which, at the 0.25 s update interval, corresponds to roughly 15 ms per update and is well within the GCS cycle time. The remaining wall-clock time is dominated by the serialized network and dynamics simulation and the per-agent planners, which in deployment execute in parallel on separate onboard computers rather than on a single host. The aggregate simulation runtime therefore does not bound flight-time feasibility, and the spoofing-aware additions operate comfortably in real time.

3) *Adaptive adversaries*: The spoofer in our evaluation follows a straight-line trajectory, but the localization pipeline is not specialized to this case. The IMM filter runs constant-velocity and constant-acceleration hypotheses with a model transition matrix, so it is designed to track maneuvering, nonlinear trajectories by reweighting and switching between motion models as the target accelerates or turns; the straight-line spoofer is thus a representative evaluation choice rather than an assumption required by the method. Tracking a more aggressively maneuvering adversary would, however, require re-tuning the IMM parameters in Table IV, such as the process-noise covariances and the model transition probabilities, to match the expected maneuver dynamics. Beyond its own motion, a strategic adversary could attempt to degrade observer geometry, for example positioning itself so that the contributing receivers become near-coplanar, which ill-conditions the covariance P_t and elongates the unsafe ellipsoid. We expect the chance-constrained design to remain fail-safe under such behavior, since poor geometry inflates P_t and enlarges the avoided region, consistent with the ellipsoid radius trend in Table II.

VIII. CONCLUSION

In this work, we present a spoofing-aware trajectory planning framework that enables safe movement of sUAS aircraft in the presence of RID spoofing attacks. The framework is comprised of three tightly interconnected components: spoofing detection, spoofing localization, and risk-aware trajectory planning. The results indicate that the proposed method achieves substantial safety performance improvements compared with a baseline trajectory planner that assumes all RID broadcast messages are truthful. In addition, although the proposed approach incurs additional computational overhead compared to the baseline trajectory planner, it remains scalable and able to support a high number of aircraft in the environment. Future works include incorporating optimal observer allocation and trajectory planning for efficient and accurate spoofer localization. Furthermore, additional physical layer properties, such as the Doppler shift and angle of arrival, will be incorporated for better spoofer localization accuracy.

ACKNOWLEDGMENT

This material is based upon work supported by the NASA Aeronautics Research Mission Directorate (ARMD) Univer-

sity Leadership Initiative (ULI) under cooperative agreement number 80NSSC24M0070. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Aeronautics and Space Administration.

REFERENCES

- [1] I. Sharifi, M. Ghazanfari, A. Taye, P. Wei, M. Ahmed, H. Tae Kim, M. Ghasemi, V. Gupta, N. W. Dahle, R. Canady *et al.*, "A survey of security challenges and solutions for uas traffic management (utm) and small unmanned aerial systems (suas)," in *AIAA SCITECH 2026 Forum*, 2026, p. 2892.
- [2] E. Blasch, R. Sabatini, A. Roy, K. A. Kramer, G. Andrew, G. T. Schmidt, C. C. Insaurralde, and G. Fasano, "Cyber awareness trends in avionics," in *2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC)*. IEEE, 2019, pp. 1–8.
- [3] M. Keizer, S. Sciancalepore, and G. Oligeri, "Ghostbuster: Detecting misbehaving remote id-enabled drones," in *2024 IEEE 21st Consumer Communications & Networking Conference (CCNC)*. IEEE, 2024, pp. 324–332.
- [4] S. Sciancalepore, F. Davidovic, and G. Oligeri, "Orion: Verification of drone trajectories via remote identification messages," *Future Generation Computer Systems*, vol. 160, pp. 869–878, 2024.
- [5] B. Bjorkman, S. Zheng, A. Coursey, C. Lemieux-Mack, S. Gonzalez, A. Diaz-Gonzalez, N. W. Dahle, N. Koroma, R. E. Canady, X. Koutsoukos *et al.*, "Remote id spoofing attacks and defenses," in *AIAA SCITECH 2026 Forum*, 2026, p. 2665.
- [6] X. Tian, Z. Tian, J. Wang, G. Chen, K. Pham, and E. Blasch, "Gnss spoofing identification with receiver motion-induced doppler (gsir-mid)," in *Proceedings of the 38th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2025)*, 2025, pp. 2085–2098.
- [7] A. Shafique, A. Mehmood, and M. Elhadef, "Detecting signal spoofing attack in uavs using machine learning models," *IEEE access*, vol. 9, pp. 93 803–93 815, 2021.
- [8] P. Wu, J. Xie, Y. Liu, and J. Chen, "Risk-bounded and fairness-aware path planning for urban air mobility under uncertainty," *Aerospace Science and Technology*, vol. 127, p. 107738, 2022.
- [9] A. G. Taye, R. Valenti, A. Rajhans, A. Mavrommati, P. J. Mosterman, and P. Wei, "Safe and scalable real-time trajectory planning framework for urban air mobility," *Journal of Aerospace Information Systems*, vol. 21, no. 8, pp. 641–650, 2024.
- [10] P. Fiorini and Z. Shiller, "Motion planning in dynamic environments using velocity obstacles," in *IEEE International Conference on Robotics and Automation*, 1998, pp. 560–565.
- [11] J. Van den Berg, S. J. Guy, M. Lin, and D. Manocha, "Reciprocal n-body collision avoidance," *Robotics Research*, pp. 3–19, 2011.
- [12] G. Sharon, R. Stern, A. Felner, and N. R. Sturtevant, "Conflict-based search for optimal multi-agent path finding," in *Artificial Intelligence*, vol. 219, 2015, pp. 40–66.
- [13] A. P. Vinod, S. Safaoui, T. H. Summers, N. Yoshikawa, and S. Di Cairano, "Decentralized, safe, multiagent motion planning for drones under uncertainty via filtered reinforcement learning," *IEEE Transactions on Control Systems Technology*, 2024.
- [14] B. Lindqvist, P. Sopasakis, and G. Nikolakopoulos, "A scalable distributed collision avoidance scheme for multi-agent uav systems," in *2021 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. IEEE, 2021, pp. 9212–9218.
- [15] Federal Aviation Administration, "Remote identification of unmanned aircraft," Code of Federal Regulations, Title 14, Part 89, 2021. [Online]. Available: <https://www.ecfr.gov/current/title-14/chapter-I/subchapter-F/part-89>
- [16] M. Corbetta, P. Banerjee, W. Okolo, G. Gorospe, and D. G. Luchinsky, "Real-time uav trajectory prediction for safety monitoring in low-altitude airspace," in *Aiaa aviation 2019 forum*, 2019, p. 3514.
- [17] Y. Bar-Shalom, X. R. Li, and T. Kirubarajan, *Estimation with Applications to Tracking and Navigation*. Wiley, 2001.
- [18] T. S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Prentice Hall, 2002.

- [19] SciPy Developers, “scipy.optimize.least_squares: Nonlinear least-squares solver with trust region reflective method,” https://docs.scipy.org/doc/scipy/reference/generated/scipy.optimize.least_squares.html, 2024, accessed: 2026-05-01.
- [20] A. Varga, “The omnet++ discrete event simulation system,” *Proceedings of the European Simulation Multiconference (ESM’2001)*, June 2001.
- [21] “Inet framework,” 2024, [Accessed 01-05-2024]. [Online]. Available: <https://inet.omnetpp.org/>
- [22] Federal Aviation Administration, “Unmanned aircraft system (uas) traffic management (utm) concept of operations v2.0,” Federal Aviation Administration, Washington, DC, Tech. Rep., Aug. 2022. [Online]. Available: https://www.faa.gov/sites/faa.gov/files/2022-08/UTM_ConOps_v2.pdf

APPENDIX

The parameters used in the IMM filter and aircraft dynamic model are summarized in the following tables.

TABLE IV: IMM Filter Parameters

Parameter	Value	Description
Δt	0.25 s	Time step
μ_0	[0.45, 0.55]	Initial model probabilities
Π	$\begin{bmatrix} 0.98 & 0.02 \\ 0.16 & 0.84 \end{bmatrix}$	Model transition matrix
$Q^{(CV)}$	diag(2, 2, 2, 120, 120, 120)	CV process noise (pos, vel)
$Q^{(CA)}$	diag(4, 4, 4, 50, 50, 50, 20, 20, 20)	CA process noise (pos, vel, acc)
$R^{(CV)}$	400 $\mathbf{I}_3$	CV measurement noise
$R^{(CA)}$	50 $\mathbf{I}_3$	CA measurement noise

TABLE V: Aircraft Model Parameters

Parameter	Value	Description
I_{xx}	0.2506 kg·m ²	Moment of inertia about x -axis
I_{yy}	0.2506 kg·m ²	Moment of inertia about y -axis
I_{zz}	1.0024 kg·m ²	Moment of inertia about z -axis
l	0.635 m	Arm length
m_t	12.66 kg	Total mass of the aircraft