CISTER
Research Centre in
Real-Time & Embedded
Computing Systems

Journal Paper

Detection and Mitigation of Position Spoofing Attacks on Cooperative UAV Swarm Formations

Siguo Bi
Kai Li*
Shuyan Hu
Wei Ni
Cong Wang
Xin Wang

*CISTER Research Centre

CISTER-TR-231201

2023

Detection and Mitigation of Position Spoofing Attacks on Cooperative UAV Swarm Formations

Siguo Bi, Kai Li*, Shuyan Hu, Wei Ni, Cong Wang, Xin Wang

*CISTER Research Centre

Polytechnic Institute of Porto (ISEP P.Porto)

Rua Dr. António Bernardino de Almeida, 431

4200-072 Porto

Portugal

Tel.: +351.22.8340509, Fax: +351.22.8321159

E-mail: fdbsg@fudan.edu.cn, kai@isep.ipp.pt, syhu14@fudan.edu.cn, Wei.Ni@data61.csiro.au, congwang@fudan.edu.cn, xwang11@fudan.edu.cn

https://www.cister-labs.pt

Abstract

Detecting spoofing attacks on the positions of unmanned aerial vehicles (UAVs) within a swarm is challenging. Traditional methods relying solely on individually reported positions and pairwise distance measurements are ineffective in identifying the misbehavior of malicious UAVs. This paper presents a novel systematic structure designed to detect and mitigate spoofing attacks in UAV swarms. We formulate the problem of detecting malicious UAVs as a localization feasibility problem, leveraging the reported positions and distance measurements. To address this problem, we develop a semidefinite relaxation (SDR) approach, which reformulates the non-convex localization problem into a convex and tractable semidefinite program (SDP). Additionally, we propose two innovative algorithms that leverage the proximity of neighboring UAVs to identify malicious UAVs effectively. Simulations demonstrate the superior performance of our proposed approaches compared to existing benchmarks. Our methods exhibit robustness across various swarm networks, showcasing their effectiveness in detecting and mitigating spoofing attacks. Specifically, the detection success rate is improved by up to 65%, 55%, and 51% against distributed, collusion, and mixed attacks, respectively, compared to the benchmarks.

Detection and Mitigation of Position Spoofing Attacks on Cooperative UAV Swarm Formations

Siguo Bi, Kai Li, *Senior Member, IEEE*, Shuyan Hu, *Member, IEEE*, Wei Ni, *Fellow, IEEE*, Cong Wang, and Xin Wang, *Fellow, IEEE*

***Abstract*—Detecting spoofing attacks on the positions of unmanned aerial vehicles (UAVs) within a swarm is challenging. Traditional methods relying solely on individually reported positions and pairwise distance measurements are ineffective in identifying the misbehavior of malicious UAVs. This paper presents a novel systematic structure designed to detect and mitigate spoofing attacks in UAV swarms. We formulate the problem of detecting malicious UAVs as a localization feasibility problem, leveraging the reported positions and distance measurements. To address this problem, we develop a semidefinite relaxation (SDR) approach, which reformulates the non-convex localization problem into a convex and tractable semidefinite program (SDP). Additionally, we propose two innovative algorithms that leverage the proximity of neighboring UAVs to identify malicious UAVs effectively. Simulations demonstrate the superior performance of our proposed approaches compared to existing benchmarks. Our methods exhibit robustness across various swarm networks, showcasing their effectiveness in detecting and mitigating spoofing attacks. Specifically, the detection success rate is improved by up to 65%, 55%, and 51% against distributed, collusion, and mixed attacks, respectively, compared to the benchmarks.**

***Index Terms*—Malicious UAV detection, position spoofing attack, cooperative localization, semidefinite programming.**

I. Introduction

Recently, there has been a widespread utilization of unmanned aerial vehicles (UAVs) [1], including parcel delivery [2], radio surveillance [3], [4], and rescue missions [5]. This is due to the affordability and endurance of UAVs, and their flexibly adjustable positions conducive to line-of-sight (LOS) communications, facilitated by rapid technological advancements [6]. The varieties of practical needs for UAV swarms further ignite and necessitate the protection of security for UAV swarms [7]. For instance, the reliability of information propagation has been analyzed in large-scale networks, including UAV swarms [8]. The connectivity of a UAV swarm has been studied in the presence of jamming attacks from the ground [9]. To enhance reliability and mitigate potential flight collisions, it is crucial to establish a formation flight and coordination among UAVs [10]. In the formation flight of a UAV swarm, individual UAVs rely on position reports from their peers and their pairwise distance measurements with neighboring UAVs to maintain inter-UAV distances and avoid collisions. Compromised or malicious UAVs can launch position spoofing attacks, potentially leading to catastrophic consequences for the UAV swarm [11]. A malicious UAV might transmit a deceptive position report, misleading other UAVs while simultaneously concealing its true location, as illustrated in Fig. 1. Such conditions can disrupt the control mechanism that maintains swarm formation, resulting in disorders [12].

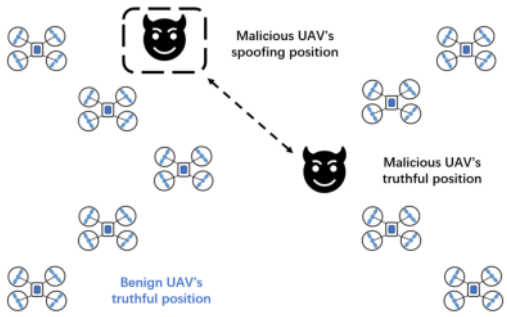

Fig. 1. An illustration of the attack model, where a malicious UAV falsifies its position and broadcasts the fake position to the other benign UAVs.

Detecting and identifying malicious UAVs within a swarm is challenging. This problem seeks to establish whether a feasible position realization for each UAV that aligns with all reported distances and measurements exists. Such a feasibility problem is non-trivial and non-convex, and has never been studied and addressed in the existing literature. As delineated in this paper, the problem can be transformed into a convex semidefinite program (SDP), allowing for efficient use of convex optimization solvers in polynomial time. However, solving the SDP problem alone does not enable the identification of individual malicious UAVs. On the one hand, the number of malicious UAVs is typically unknown and needs to be detected. On the other hand, the effectiveness of SDP can be penalized by the interdependence among the positions of neighboring UAVs.

To address these challenges and precisely identify mali-

Manuscript received July 17, 2023; revised October 18, 2023; accepted December 3, 2023. Work in this paper was supported by the National Natural Science Foundation of China under Grants No. 62231010, No. 62071126, and No. 62101135, and the Innovation Program of Shanghai Municipal Science and Technology Commission Grant No. 21XD1400300. The work of K. Li was supported by the CISTER Research Unit (UIDP/UIDB/04234/2020) and project ADANET (PTDC/EEICOM/3362/2021), financed by National Funds through FCT/MCTES (Portuguese Foundation for Science and Technology).

S. Bi, S. Hu, C. Wang, and X. Wang are with Fudan University, Shanghai, China (emails: {fdbsg, syhu14, congwang, xwang11}@fudan.edu.cn).

K. Li is with the Division of Electrical Engineering, Department of Engineering, University of Cambridge, CB3 0FA Cambridge, U.K., and also with Real-Time and Embedded Computing Systems Research Centre (CISTER), Porto 4249–015, Portugal (E-mail: kaili@ieee.org).

W. Ni is with the Commonwealth Scientific and Industrial Research Organization (CSIRO), Sydney, NSW 2122, Australia (e-mail: wei.ni@data61.csiro.au).

Corresponding author: X. Wang.

cious UAVs, this paper proposes two new algorithms: the Cooperative Detection and Identification (CDI) algorithm and the Enhanced CDI (E-CDI) algorithm. The CDI algorithm initiates its process by creating sets of possible malicious and benign UAVs. Subsequently, it combines the selected potentially malicious UAVs with the benign set, establishing a connected sub-network for the SDP-based position feasibility check. If all the neighboring UAVs of a selected UAV are themselves malicious, the CDI algorithm may misjudge the UAV as malicious, as attempting to localize a sub-network with an entire malicious neighborhood is inherently unfeasible. In contrast, the E-CDI algorithm conducts an additional localization feasibility check on each individual UAV in the neighborhood, compared to the CDI algorithm. By this means, collusion attacks launched by multiple closely located, malicious UAVs can be detected and mitigated.

Compared to the existing relevant works, e.g., [11]–[14], the new contributions of this paper include:

1) To detect position spoofing attacks, we propose a novel mechanism for malicious UAV detection and identification, where we cast the challenging malicious UAV detection problem as a localization feasibility problem.
2) A semidefinite relaxation (SDR) approach is put forth to transform the non-convex feasibility problem into a convex problem. The presence of malicious UAVs can then be efficiently ascertained by evaluating the feasibility of the convex problem.
3) We develop two iterative algorithms, i.e., CDI and E-CDI, to identify malicious UAVs by leveraging the proximity of neighboring UAVs.
   - The CDI algorithm dynamically merges selected potentially malicious UAVs into the benign set to form a connected positioning sub-network. This sub-network is used to determine whether the selected UAV is malicious.
   - The E-CDI algorithm enhances identification efficiency by further assessing each neighboring UAV in the neighborhood of a potentially malicious UAV. As a result, collusion attacks launched by multiple closely located, malicious UAVs can be detected.

   Both algorithms are designed to conclude within a finite number of iterations and exhibit robust performance across various network configurations of UAV swarms.

Extensive simulations demonstrate that the proposed CDI and E-CDI algorithms achieve superior performance on classic metrics compared to the benchmark techniques. Under the proposed algorithms, the detection success rate can be improved by up to 65%, 55%, and 51% against distributed, collusion, and mixed attacks, respectively, compared to their benchmarks.

The rest of this paper is organized as follows. Section II reviews the related works. Section III formulates and convexifies the malicious UAV's misbehavior detection problem. In Section IV, two efficient iterative algorithms are proposed to identify malicious UAVs. Section V provides numerical results to evaluate the proposed algorithm, followed by conclusions in Section VI.

Notation: Upper- and lower-case boldface symbols denote matrices and vectors, respectively; $|\cdot|$ takes the absolute value if a scalar is concerned or the cardinality if a set is concerned; $\|\cdot\|$ denotes ℓ_2-norm; $\hat{(\cdot)}$ indicates a reported, noise-corrupted version of $(\cdot)$. The notation used is collated in Tab. I.

TABLE I
NOTATION AND DEFINITION.

Notation	Definition
$\mathcal{X}$	The set of the 3D coordinates of all the UAVs
N	The total number of UAVs
$\boldsymbol{x}_i$	The actual position of the i-th UAV
$\hat{\boldsymbol{x}}_i$	The reported position of the i-th UAV
r_{ij}	The actual distance between UAVs i and j, $i \neq j$
$\hat{r}_{ij}$	The reported distance between UAVs i and j, $i \neq j$
$\hat{\alpha}_{ij}$	An auxiliary variable
$\boldsymbol{w}_i$	The noise vector for position measurement of UAV i
w_{ij}	The noise in the reported distance measurement between UAVs i and j, $i \neq j$
$\boldsymbol{I}_3$	The 3×3 identity matrix
$\boldsymbol{X}$	The $3 \times N$ matrix with its i-th column being $\boldsymbol{x}_i$
d	The communication range for distance measurement
ϵ	A small constant, e.g., 1×10^{-6}
$\boldsymbol{e}_i$	The vector whose i-th element is one and the rest are zeros.
ρ_{ij}	The indicator of whether UAVs i and j are directly connected.
$\boldsymbol{E}_n$	The matrix of the measured and reported Euclidean distances between directly connected UAVs
$\boldsymbol{E}_r$	The matrix of the Euclidean distances between directly connected UAVs generated based on the reported positions of the UAVs
$\mathbb{N}$	The set of all N UAVs.
$\mathbb{M}$	The set of malicious UAVs
$\mathbb{B}$	The set of benign UAVs
$\mathbb{N}_k$	The set of the one-hop neighbors of UAV k
R_M	The malicious ratio, i.e., the ratio of the number of malicious UAVs to the total number of UAVs in a UAV swarm

II. Related Work

A. Spoofing Attacks on UAVs

Spoofing attacks on UAVs have been extensively investigated in the recent literature. However, most works have focused on the direct hijack of the Global Positioning System (GPS) of a specific single UAV. Aiming at identifying fake GPS coordinates due to the hijack of the GPS communication software, the authors of [15] proposed a convolutional neural network (CNN) integrated with a recurrent neural network (RNN) to predict a vehicle's real-time trajectory based on the data from multiple sensors. With a similar purpose of handling GPS spoofing attacks, the authors of [16] proposed a two-step approach based on data sensed and fused from distributed radar ground stations equipped with a local tracker. The approach consists of spoofing detection and mitigation. In the spoofing detection step, a track-to-track association approach was adopted to detect spoofing attacks with fused data from UAVs and a local tracker. In the mitigation step, the fused data was input to a controller to mitigate the spoofing attack detected. The proposed two-step approach was reported to achieve almost the same accuracy as GPS efficiently.

To enhance the reliability of flight controllers when the UAV is under GPS spoofing attack, the authors of [17] utilized an extended Kalman filter (EKF)-based approach. They investigated the impact of GPS spoofing on the EKF estimation and the UAV itself under different levels of attack strength. It

was reported that the classic EKF-based approach can tolerate small errors from spoofing attacks, but can be inefficient when the attack intensifies. Similar works on GPS-related spoofing attacks on a specific single UAV can be found in [13], [18]–[20], and spoofing attacks related to the time-of-arrival (TOA) or time difference-of-arrival (TDOA) can be found in [21].

The security issue of UAV swarms has attracted increasing attention. In order to mitigate the navigation spoofing attacks on aerial formations, the authors of [22] proposed a cascaded estimation algorithm used for concurrent GPS spoofing detection and localization. An attack detection module was based on the consistency of multimodal measurement to realize threshold tests. A localization module was then used for a decision based on remarkable differences between safe and under-attack conditions of UAV self-localization. The cascaded approach can achieve a safe self-localization for a UAV swarm under a spoofing attack. Aiming at solving the GPS spoofing attack in a UAV swarm, the authors of [23] proposed a security-aware monitoring method to monitor the potential malicious UAVs and protect the benign ones from attacks. The method was implemented by the received-signal-strength-indicator (RSSI)-based triangulation.

B. Cooperative Network Localization

Position-related spoofing attacks destroy the localization of UAVs in a UAV swarm, since a UAV swarm can be considered a cooperative network. SDP, an efficient convex optimization approach, has been extensively applied to cooperative network localization. Employing the SDP, the authors of [24] proposed a novel difference-of-convex (DC)-based algorithm to achieve accurate cooperative localization. The authors of [25] proposed an SDP-based method to estimate the relative transformation of a robot in a cooperative robotic swarm. The SDP-based method could achieve global optimality and scalability. The authors of [26] developed an efficient SDP-based scheduling strategy to optimize UAV deployment in intelligent transportation cooperative networks. More SDP-based cooperative localization techniques can be found in [14], [27], [28].

Unlike existing works that rely heavily on extensive training using historical data, we put forth an SDP-based UAV misbehavior detection mechanism with no need for historical data. The proposed SDP-based mechanism detects and identifies malicious UAVs that misreport their positions by leveraging the proximity of neighboring UAVs. This mechanism is applicable regardless of the specific type of localization signals hijacked and spoofed, including GPS, TDA, or TDOA.

III. System Model and Problem Formulation

In this section, we first provide the threat model considered and formally formulate the malicious UAV detection problem as a localization feasibility problem. By applying the SDR, we convexify the feasibility problem into a convex problem.

A. Threat Model

Consider a swarm of UAVs executing a routine cruising mission, during which the UAVs cooperatively maintain a specific formation to prevent collisions. Each UAV within the swarm communicates its position, ascertained by the GPS, to its counterparts. Each UAV also conducts relative distance measurements with the other UAVs that are within the permissible communication range of the UAV. Random receiver noises or GPS errors can corrupt these distance measurements, rendering the reported positions inaccurate. During the formation flight, each UAV adjusts its flight position based on the reported positions and distance measurements of neighboring UAVs, thereby averting potential flight collisions.

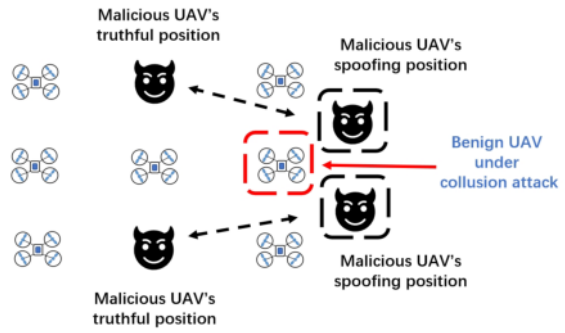

Fig. 2. An illustration of the collusion spoofing attack model, where two malicious UAVs falsify their positions to be within the one-hop neighborhood of the benign UAV.

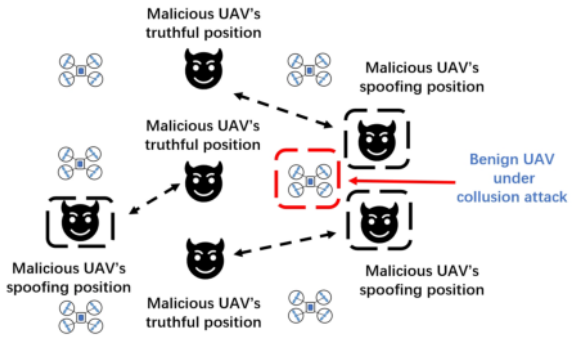

Fig. 3. An illustration of the mixed spoofing attack model, where two malicious UAVs conduct a collusion attack while the other malicious UAVs falsify their positions.

Malicious UAVs, under the control of attackers, have the capability to fabricate their position information and disseminate this information among all other UAVs. More precisely, malicious UAVs can initiate a spoofing attack by falsely reporting their positions within the detection measurement range of benign UAVs. This deliberate misrepresentation of positions can directly disrupt the formation. Moreover, malicious UAVs may target a specific benign UAV by deceptively reporting their positions within the detection measurement range of that UAV, which is a tactic known as a collusion attack; see Fig. 2. This coordinated misrepresentation is aimed at framing a target UAV. Given the substantial evidence presented through this deceptive conspiracy, the swarm may erroneously conclude that the framed UAV is perpetrating a spoofing attack.

The two above-mentioned attacks, i.e., the distributed attack and the collusion attack, can be amalgamated to initiate a mixed spoofing attack; see Fig. 3. In this composite attack,

some malicious UAVs execute a distributed attack while the remaining UAVs engage in a collusion attack. The mixed nature of this attack significantly intensifies its severity, potentially hastening the breakdown of the entire formation.

B. Problem Statement

We propose to formulate the problem of identifying malicious UAVs as a localization feasibility problem. If localization is infeasible under the positions and distance measurements reported, there is at least one malicious UAV attacking the UAV swarm in an attempt to compromise the swarm formation.

Let $\mathcal{X} := \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N\}$ define the three-dimensional (3D) coordinates of the UAVs in an N-UAV swarm studied, where $\boldsymbol{x}_i \in \mathbb{R}^{3\times 1}$ is the unknown actual 3D coordinates of UAV i. Let $\mathbb{N} = \{1, \ldots, N\}$ collect the indexes of the N UAVs. The permissible range for pairwise distance measurement is denoted by d. The reported position of UAV i is given as $\hat{\boldsymbol{x}}_i$, which can be contaminated by the measurement noise, i.e., $\boldsymbol{w}_i \sim \mathcal{N}(0, \sigma_i^2 \boldsymbol{I}_3)$. $\hat{\boldsymbol{x}}_i = \boldsymbol{x}_i + \boldsymbol{w}_i$, $\forall i$. Here, $\mathcal{N}(0, \sigma_i^2 \boldsymbol{I}_3)$ stands for the zero-mean Gaussian distribution with the variance of $\sigma_i^2 \boldsymbol{I}_3$ and $\boldsymbol{I}_3$ is the 3×3 identity matrix.

The feasibility problem of finding a solution of $\mathcal{X}$ can be formulated as

$$\begin{aligned} &\text{find} \quad \mathcal{X} \\ &\text{s.t.} \ \|\boldsymbol{x}_i - \hat{\boldsymbol{x}}_j\|^2 < d^2, \ \forall i \in \mathbb{N}, j \in \mathbb{N}_i, && \text{(1a)} \\ &\quad |\boldsymbol{x}_i - \hat{\boldsymbol{x}}_i\|^2 \le \epsilon, \ \forall i \in \mathbb{N}, && \text{(1b)} \\ &\quad |\hat{r}_{ij}^2 - \|\boldsymbol{x}_i - \hat{\boldsymbol{x}}_j\|^2| < (\frac{d}{2})^2, \ \forall i \in \mathbb{N}, j \in \mathbb{N}_i, && \text{(1c)} \end{aligned}$$

where $\mathbb{N}_i$ collects all one-hop neighbors of UAV i and can be obtained based on the reports of UAV i; $\epsilon \ge 0$ is a small constant; and $\hat{r}_{ij}$ denotes the reported pairwise distance between UAVs i and j contaminated with measurement noise, e.g., $w_{ij} \sim \mathcal{N}(0, \sigma_{ij}^2)$. Here, σ_{ij}^2 is the variance of the distance measurement error.

Constraint (1a) defines that the relative distance measurement between UAV i and the reported position of UAV j, i.e., $\|\boldsymbol{x}_i - \hat{\boldsymbol{x}}_j\|$, has to be within the permissible communication range, d, if UAV i is a one-hop neighbor of UAV j and can hear its ranging signals. Constraint (1b) dictates that the difference between $\boldsymbol{x}_i$ and $\hat{\boldsymbol{x}}_i$ is smaller than a pre-specified threshold ϵ, ensuring that the model must rely on the individual reported position to output a solution (if such a solution does not exist, it is reasonable to suspect there exist misreported UAV positions). Constraint (1c) indicates that the difference between the reported pairwise distance and the Euclidean distance (between the estimated and reported positions) should be smaller than half of the distance measurement range, which is also considered to be the maximum tolerable distance measurement error. Nonetheless, the right-hand side (RHS) of constraint (1c), i.e., $(\frac{d}{2})^2$, can adapt to the needs of different measurement devices.

C. Proposed SDP-based Reformulation

Because of the non-convex constraints (1a)–(1c), finding $\mathcal{X}$ in (1) is a non-convex feasibility checking problem, which is difficult to solve. To convexify (1a)–(1c), auxiliary variables, denoted by α_{ij}, $\forall i, j \in [1, N]$, are introduced to substitute those non-convex parts in (1a)–(1c). As a result, the non-convex feasibility problem in (1) can be rewritten as

$$\begin{aligned} &\text{find} \quad \mathcal{X} \\ &\text{s.t.} \ \alpha_{ij} < d^2, \ \forall i \in \mathbb{N}, j \in \mathbb{N}_i, && \text{(2a)} \\ &\quad \alpha_{ii} \le \epsilon, \ \forall i \in \mathbb{N}, && \text{(2b)} \\ &\quad |\hat{r}_{ij}^2 - \alpha_{ij}| < (\frac{d}{2})^2, \ \forall i \in \mathbb{N}, j \in \mathbb{N}_i, && \text{(2c)} \\ &\quad ||\boldsymbol{x}_i - \hat{\boldsymbol{x}}_j||^2 = \alpha_{ij}, \quad \forall i \in \mathbb{N}, j \in \mathbb{N}_i \cup \{i\}, && \text{(2d)} \end{aligned}$$

where constraints (2a) and (2d) are homogenized from (1a), and (2b) is homogenized from (1b). Constraints (2a)–(2c) are affine and convex. Constraint (2d) is still non-convex. To convexify (2d), we rewrite $||\boldsymbol{x}_i - \hat{\boldsymbol{x}}_j||^2$ in a matrix form as

$$\|\boldsymbol{x}_i - \hat{\boldsymbol{x}}_j\|^2 = [\hat{\boldsymbol{x}}_j^T \ \ -\boldsymbol{e}_i^T] \begin{bmatrix} \boldsymbol{I}_3 & \boldsymbol{X} \\ \boldsymbol{X}^T & \boldsymbol{Y} \end{bmatrix} \begin{bmatrix} \hat{\boldsymbol{x}}_j \\ -\boldsymbol{e}_i \end{bmatrix}, \quad (3)$$

where $\boldsymbol{e}_i \in \mathbb{R}^{N\times 1}$ is a vector whose i-th element is "1" and the rest are all "0". $\boldsymbol{X} \in \mathbb{R}^{3\times N}$ is a $3 \times N$ matrix with its i-th column being $\boldsymbol{x}_i$. Moreover,

$$\boldsymbol{Y} = \boldsymbol{X}^T \boldsymbol{X} \in R^{N\times N}. \quad (4)$$

As a result, finding $\mathcal{X}$ in problem (2) can be equivalently reformulated as

$$\begin{aligned} &\text{find} \ \boldsymbol{X}, \boldsymbol{Y} \\ &\text{s.t.} \ \alpha_{ij} < d^2, \ \forall i \in \mathbb{N}, j \in \mathbb{N}_i, && \text{(5a)} \\ &\quad \alpha_{ii} \le \epsilon, \ \forall i \in \mathbb{N}, && \text{(5b)} \\ &\quad |\hat{r}_{ij}^2 - \alpha_{ij}| < (\frac{d}{2})^2, \ \forall i \in \mathbb{N}, j \in \mathbb{N}_i, && \text{(5c)} \\ &\quad [\hat{\boldsymbol{x}}_j^T \ \ -\boldsymbol{e}_i^T] \begin{bmatrix} \boldsymbol{I}_3 & \boldsymbol{X} \\ \boldsymbol{X}^T & \boldsymbol{Y} \end{bmatrix} \begin{bmatrix} \hat{\boldsymbol{x}}_j \\ -\boldsymbol{e}_i \end{bmatrix} = \alpha_{ij}, \forall i \in \mathbb{N}, j \in \mathbb{N}_i \cup \{i\}, && \text{(5d)} \\ &\quad \boldsymbol{Y} = \boldsymbol{X}^T \boldsymbol{X}. && \text{(5e)} \end{aligned}$$

Here, constraints (5d) and (5e) are non-convex. Yet, constraint (5e) can be relaxed as [24], [29]

$$\boldsymbol{Y} \succeq \boldsymbol{X}^T \boldsymbol{X}, \quad (6)$$

where "$\succeq$" stands for element-wise inequality. According to Schur complement [30], (6) is equivalent to

$$\begin{bmatrix} \boldsymbol{I}_3 & \boldsymbol{X} \\ \boldsymbol{X}^T & \boldsymbol{Y} \end{bmatrix} \succeq 0, \quad (7)$$

Further let $\boldsymbol{\mathcal{Z}}$ denote the left-hand side (LHS) of (7), yielding

$$\boldsymbol{\mathcal{Z}} = \begin{bmatrix} \boldsymbol{I}_3 & \boldsymbol{X} \\ \boldsymbol{X}^T & \boldsymbol{Y} \end{bmatrix} \succeq 0. \quad (8)$$

The relaxation of (5e) to (6) is tight if $\mathrm{Rank}(\boldsymbol{\mathcal{Z}}) = 3$.

Also, define

$$\hat{\boldsymbol{\mathcal{G}}}_{\boldsymbol{ij}} = \begin{bmatrix} \hat{\boldsymbol{x}}_j \\ -\boldsymbol{e}_i \end{bmatrix} [\hat{\boldsymbol{x}}_j^T \ \ -\boldsymbol{e}_i^T]. \quad (9)$$

Based on (8) and (9), (5d) can be rewritten as

$$[\hat{\boldsymbol{x}}_j^T \ \ -\boldsymbol{e}_i^T] \begin{bmatrix} \boldsymbol{I}_3 & \boldsymbol{X} \\ \boldsymbol{X}^T & \boldsymbol{Y} \end{bmatrix} \begin{bmatrix} \hat{\boldsymbol{x}}_j \\ -\boldsymbol{e}_i \end{bmatrix} = \mathrm{Tr}(\hat{\boldsymbol{\mathcal{G}}}_{\boldsymbol{ij}} \boldsymbol{\mathcal{Z}}) = \alpha_{ij}, \quad (10)$$

Based on (6)–(10), the feasibility problem (5) is further equivalently rewritten as the following feasibility problem:

$$\begin{aligned}
&\text{find } \boldsymbol{\mathcal{Z}} \\
&\text{s.t. } \boldsymbol{\mathcal{Z}}_{1:3,1:3} = \boldsymbol{I}_3, && (11a)\\
&\alpha_{ij} < d^2,\ \forall i \in \mathbb{N}, j \in \mathbb{N}_i, && (11b)\\
&\alpha_{ii} \le \epsilon,\ \forall i \in \mathbb{N}, && (11c)\\
&|\hat{r}_{ij}^2 - \alpha_{ij}| < (\frac{d}{2})^2,\ \forall i \in \mathbb{N}, j \in \mathbb{N}_i, && (11d)\\
&\text{Tr}(\hat{\boldsymbol{\mathcal{G}}}_{\boldsymbol{ij}} \boldsymbol{\mathcal{Z}}) = \alpha_{ij},\quad \forall i \in \mathbb{N}, j \in \mathbb{N}_i \cup \{i\}, && (11e)\\
&\boldsymbol{\mathcal{Z}} \succeq 0, && (11f)\\
&\text{Rank}(\boldsymbol{\mathcal{Z}}) = 3. && (11g)
\end{aligned}$$

where constraint (11a) enforces the upper left 3×3 block of $\boldsymbol{\mathcal{Z}}$ to be an identity matrix, ensuring that the rank of the solution is at least three. Constraints (11a), (11f), and (11g) are equivalently derived from (5e). This is because both (11a) and (11f) constrain $\boldsymbol{\mathcal{Z}}$ to be symmetric and in the form of (8), while rank constraint (11g) forces the lower right $N \times N$ block of $\boldsymbol{\mathcal{Z}}$, i.e., $\boldsymbol{Y}$ in (8), to be $\boldsymbol{X}^T\boldsymbol{X}$, according to classic linear algebra theory.

Dropping the rank constraint (11g), we have the following SDR problem:

$$\begin{aligned}
&\text{find } \boldsymbol{\mathcal{Z}} \\
&\text{s.t. } \boldsymbol{\mathcal{Z}}_{1:3,1:3} = \boldsymbol{I}_3, && (12a)\\
&\alpha_{ij} < d^2,\ \forall i \in \mathbb{N}, j \in \mathbb{N}_i, && (12b)\\
&\alpha_{ii} \le \epsilon,\ \forall i \in \mathbb{N}, && (12c)\\
&|\hat{r}_{ij}^2 - \alpha_{ij}| < (\frac{d}{2})^2,\ \forall i \in \mathbb{N}, j \in \mathbb{N}_i, && (12d)\\
&\text{Tr}(\hat{\boldsymbol{\mathcal{G}}}_{\boldsymbol{ij}} \boldsymbol{\mathcal{Z}}) = \alpha_{ij},\quad \forall i \in \mathbb{N}, j \in \mathbb{N}_i \cup \{i\}, && (12e)\\
&\boldsymbol{\mathcal{Z}} \succeq 0. && (12f)
\end{aligned}$$

Problem (12) is convex and can be efficiently solved using off-the-shelf CVX solvers, e.g., MATLAB CVX toolbox [31]. Clearly, problem (12) is a relaxed (but generally tight) version of the original feasibility problem (1), with a larger feasible solution region. If the problem in (12) is infeasible, i.e., no feasible solution exists for the problem in (12), then problem (1) is surely infeasible. As a result, we can detect whether at least one malicious UAV misreports its position by checking the feasibility of the problem in (12).

IV. Proposed approach for malicious UAV identification

Leveraging the SDP problem in (12), we proceed to develop two new algorithms, CDI and E-CDI, to exploit the proximity of adjacent UAVs to facilitate the effective detection of malicious UAVs and eliminate spoofing attacks.

A. Initialization of Malicious UAV Set

Let $\mathbb{M}$ and $\mathbb{B}$ denote the sets of malicious and benign UAVs, respectively. $\mathbb{M} \cup \mathbb{B} = \mathbb{N}$. Based on $\boldsymbol{E}_r$ and $\boldsymbol{E}_n$, we propose to initialize $\mathbb{M}$ and $\mathbb{B}$, as follows.

We come up with two Euclidean matrices, i.e., the generated Euclidean matrix from individual reported positions, denoted by $\boldsymbol{E}_r \in R^{N\times N}$, and the detected Euclidean distances matrix contaminated with noise, denoted by $\boldsymbol{E}_n \in R^{N\times N}$, as

$$\boldsymbol{E}_r = \begin{pmatrix} \rho_{11}\|\hat{\boldsymbol{x}}_1 - \hat{\boldsymbol{x}}_1\| & \cdots & \rho_{1N}\|\hat{\boldsymbol{x}}_1 - \hat{\boldsymbol{x}_N}\| \\ \vdots & \ddots & \vdots \\ \rho_{N1}\|\hat{\boldsymbol{x}_N} - \hat{\boldsymbol{x}}_1\| & \cdots & \rho_{NN}\|\hat{\boldsymbol{x}_N} - \hat{\boldsymbol{x}_N}\| \end{pmatrix}, \quad (13)$$

$$\boldsymbol{E}_n = \begin{pmatrix} \hat{r}_{11} & \cdots & \hat{r}_{1N} \\ \vdots & \ddots & \vdots \\ \hat{r}_{N1} & \cdots & \hat{r}_{NN} \end{pmatrix}, \quad (14)$$

where ρ_{ij} indicates if UAVs i and j are directly connected. $\rho_{ij} = 1$, if UAVs i and j are within each other's permissible communication range, i.e., $\hat{r}_{ij} > 0$; otherwise, $\rho_{ij} = 0$. In this sense, $\boldsymbol{E}_r$ can be a sparse matrix (like $\boldsymbol{E}_n$), depending on the communication range of the UAV.

We can carry out element-wise comparisons between $\boldsymbol{E}_r$ and $\boldsymbol{E}_n$. Specifically, if the (i,j)-th elements of the two matrices have a smaller difference than the pre-specified threshold $\frac{d}{2}$, i.e., (1c) is unsatisfied, then UAVs i and/or j are potentially malicious. Both of the UAVs are added into $\mathbb{M}$, i.e., $\mathbb{M} = \mathbb{M} \cup \{i, j\}$. After all N^2 elements of $\boldsymbol{E}_r$ and $\boldsymbol{E}_n$ are assessed, the initial $\mathbb{M}$ is obtained. $\mathbb{B}$ can be accordingly initialized to be $\mathbb{B} = \mathbb{N} \setminus \mathbb{M}$.

Algorithm 1: The proposed CDI algorithm

Input: $\mathbb{B}$; $\mathbb{M}$; $\hat{\boldsymbol{x}}_i$, $\forall i \in [1, N]$; $\hat{r_{ij}}$, $\forall i, j \in [1, N],\ i \neq j$; d; ϵ.
Output: $\mathbb{M}$

```
Set k ← 1;
while M can be further reduced do
    Select the k-th UAV of M and the set of its one-hop neighbors N_k;
    Construct T ← B ∪ {k, N_k};
    Apply T to (12), and check feasibility using SDP.
    if problem (12) is feasible T then
        M ← M \ {k, N_k};
        B ← B ∪ {k, N_k};
    end
    Set k ← (k + 1) mod |M|;
end
```

B. Proposed CDI Algorithm

As summarized in **Algorithm 1**, we propose to assess the potentially malicious UAVs in $\mathbb{M}$ one after another and move those actually benign from $\mathbb{M}$ to $\mathbb{B}$ until both $\mathbb{M}$ and $\mathbb{B}$ stop changing. When assessing a UAV, i.e., UAV k, from $\mathbb{M}$, we also consider its one-hop neighbors. Part of $\mathbb{N}_k$ may belong to $\mathbb{B}$, and the rest belong to $\mathbb{M}$.

We apply the feasibility checking problem in (12) to the collection of $\mathbb{B}$, $\{k\}$, and $\mathbb{N}_k$, i.e., $\mathbb{B} \cup \{k, \mathbb{N}_k\}$. If the problem is feasible, UAV k and its one-hop neighbors $\mathbb{N}_k$ are benign. They can be removed from $\mathbb{M}$ and added to $\mathbb{B}$; i.e., $\mathbb{M} = \mathbb{M} \setminus \{k, \mathbb{N}_k\}$ and $\mathbb{B} = \mathbb{B} \cup \{k, \mathbb{N}_k\}$. Otherwise, they remain in $\mathbb{M}$. The reason for considering a potentially malicious UAV k together with its one-hop neighbors $\mathbb{N}_k$ is to increase the

chance that UAV k is connected to $\mathbb{B}$. Therefore, the feasibility checking problem can be meaningfully carried out. In the case where UAV k and its one-hop neighbors $\mathbb{N}_k$ are disconnected from $\mathbb{B}$ (in other words, $\mathbb{N}_k$ and their neighbors all belong to $\mathbb{M}$), then UAV k and its one-hop neighbors $\mathbb{N}_k$ remain in $\mathbb{M}$.

In this way, we repeatedly assess the remaining UAVs in $\mathbb{M}$ until $\mathbb{M}$ cannot be further reduced. This algorithm can quickly detect and identify malicious UAVs; but may overkill, i.e., misjudge a benign UAV to be malicious in the situation where the benign UAV only has a malicious one-hop neighbor since they are always assessed together for feasibility and cannot be individually arbitrated. In this sense, the algorithm is conservative and can be overprotective.

C. Proposed E-CDI Algorithm

A key difference between the E-CDI algorithm and the CDI algorithm (**Algorithm 1**) is that the E-CDI algorithm assesses each of the potentially malicious one-hop neighbors of a UAV belonging to $\mathbb{M}$ individually, each time the UAV and its one-hop neighbors fail the feasibility check. Specifically, each of UAV k and its potentially malicious one-hop neighbors in $\mathbb{N}_k$ are assessed by temporarily joining $\mathbb{B}$ for feasibility check again. Those that turn out to be benign are removed from $\mathbb{M}$ and added to $\mathbb{B}$. By this means, each connected malicious UAV can be detected and identified. The details are provided in **Algorithm 2**. The flowchart of the proposed CDI/E-CDI algorithm is provided in Fig. 4.

Another key difference is that the E-CDI algorithm is able to detect collusion attacks, while the CDI algorithm cannot. This is because the E-CDI assesses individual UAVs in a neighborhood $\{k, \mathbb{N}_k\}$ if the neighborhood is detected to be infected by malicious UAVs in the neighborhood. As a result, the malicious UAVs (or UAVs that cannot be confirmed benign due to their poor connectivity to other benign UAVs) can be individually assessed and verified. In contrast, the CDI algorithm may not achieve this since its assessment is based on neighborhoods $\{k, \mathbb{N}_k\}$, $\forall k \in \mathbb{M}$.

Algorithm 2: The proposed E-CDI algorithm

Input: $\mathbb{B}$; $\mathbb{M}$; $\hat{\boldsymbol{x}}_i$, $\forall i \in [1, N]$; $\hat{r_{ij}}$, $\forall i, j \in [1, N],\ i \neq j$; d; ϵ.
Output: M

```
Set k ← 1;
while M can be further reduced do
    Select the k-th UAV in M and the set of its one-hop neighbors N_k;
    Construct T ← B ∪ {k, N_k};
    Apply T to (12), and check feasibility using SDP.
    if problem (12) is feasible upon T then
        M ← M \ {k, N_k};
        B ← B ∪ {k, N_k};
    else
        Set T_1 ← {k, N_k}; i ← 1;
        while i ≤ |T_1| do
            Select the i-th UAV of {k, N_k}, denoted by π_i;
            Construct T_2 ← B ∪ {π_i};
            Apply T_2 to (12) and check feasibility using SDP;
            if problem (12) is feasible upon T_2 then
                M ← M \ {π_i};
                B ← B ∪ {π_i};
            end
            i ← i + 1;
        end
    end
    Set k ← (k + 1) mod |M|;
end
```

V. Simulation Results

In this section, we consider three types of spoofing attacks to gauge the capability of the proposed algorithm to counteract these attacks. We conduct extensive simulations to comprehensively evaluate the proposed algorithms in comparison with the established benchmarks on the key factors, i.e., the number of malicious UAVs, the scale of the network, distance measurement noise, and measurement distance.

A. Simulation Setting

We consider a UAV swarm with the UAVs' positions randomly generated according to a uniform distribution inside a unit cube $[-0.5, +0.5]^3$. The malicious UAVs are randomly chosen from the nodes. The distance measurement range is $d = 0.3$. Note that both the reported positions and reported distance measurements are contaminated with additive Gaussian noises, $\boldsymbol{w}_i \sim \mathcal{N}(0, 10^{-6}\boldsymbol{I}_3)$ [32] and $w_{ij} \sim \mathcal{N}(0, 10^{-6})$, respectively. The key parameters of the simulations are summarized in Tab. II.

TABLE II
Simulation parameters and configuration.

Parameter	Configuration
Simulation environment	Matlab R2020b
Solver	CVX solver
UAV swarm range	Unit cube $[-0.5, +0.5]^3$
Reported position noise	$\boldsymbol{w}_i \sim \mathcal{N}(0, 10^{-6}\boldsymbol{I}_3)$
Distance measurement noise	$w_{ij} \sim \mathcal{N}(0, 10^{-6})$
Distance measurement range	$[0.25, 0.45]^3$

We assess the performances of the proposed algorithms against three types of position spoofing attacks, as follows.

- **Distributed spoofing attack** Under this attack, several malicious UAVs independently misreport their positions in an attempt to compromise the UAV swarm formation.
- **Collusion attack** Under this attack, several malicious UAVs conspire to frame some benign UAVs and make them falsely identified as malicious. Based on the reported positions from targeted benign UAVs, the malicious UAVs misreport their positions to be within the neighborhood of those benign UAVs, though they can be far away from the UAVs under attack.
- **Mixed spoofing attack** Under this attack, malicious UAVs launch attacks in both distributed and collusive fashions. Specifically, some of the malicious UAVs independently carry out distributed spoofing attacks to com-

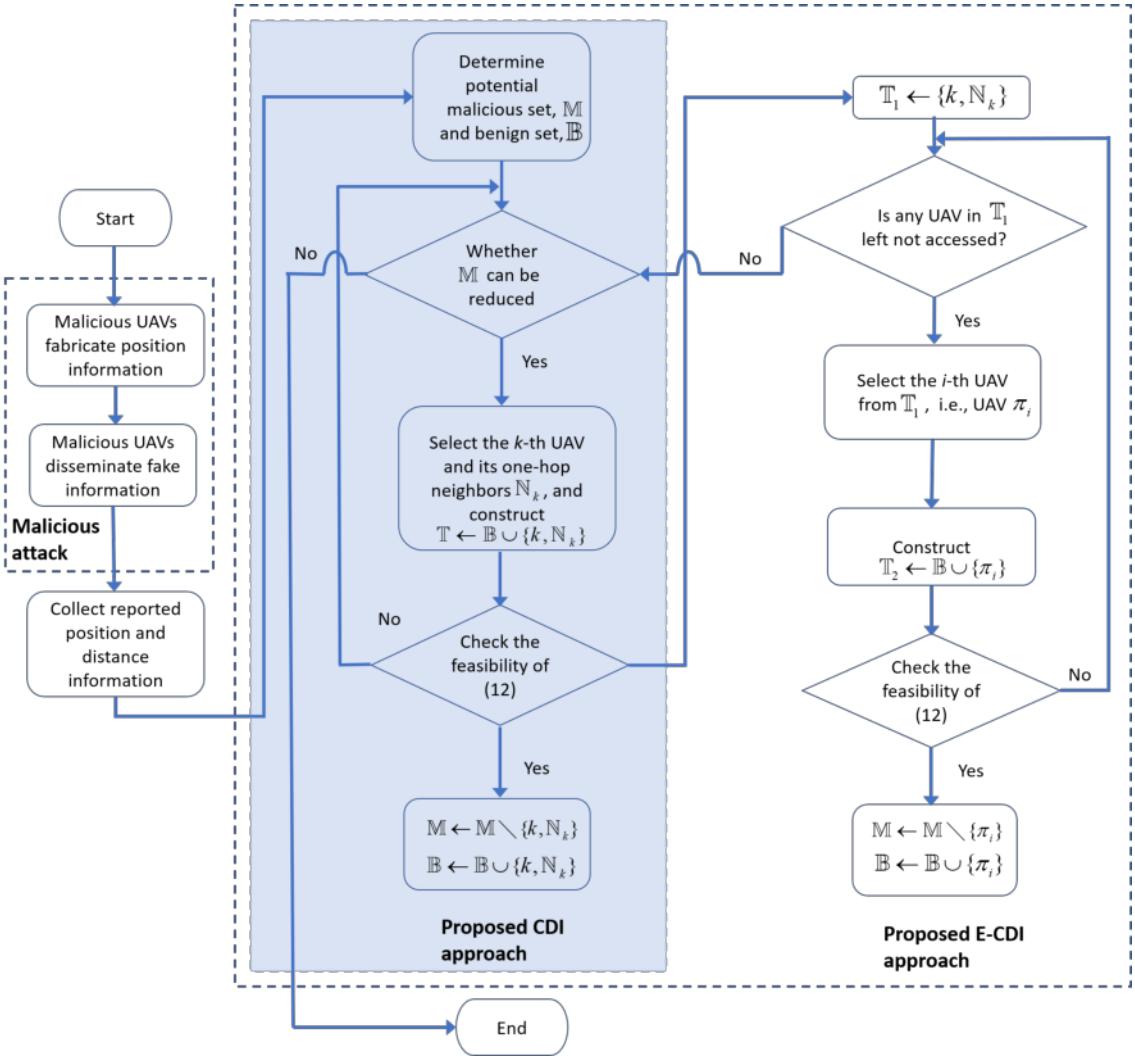

Fig. 4. The flowchart of the proposed CDI/E-CDI algorithm, where the shaded part accounts for the CDI algorithm, which is part of the more comprehensive E-CDI algorithm.

promise the swarm formation. The rest of the malicious UAVs cooperate to further impair or corrode the integrity of the UAV swarm.

The benchmark algorithms considered are

- **NLOS-based approach:** This approach [33] treats errors induced by the misbehavior of malicious UAVs as a variant of NLOS, since NLOS and spoofed positions are alike, i.e., causing considerable deviations from the genuine positions. However, NLOS is a path error involving two UAVs in a swarm. Therefore, we mildly adjust it to suit comparison by random sampling according to the scale of the test sample.
- **Random approach:** This approach directly relies on the earlier potential candidate set of malicious UAVs to conduct random sampling adjusted to the number of malicious UAVs and the sampled UAVs as the output of the approach.

The performance metrics considered are Precision, Recall, and F1. The three classic metrics are given by [34]

$$\text{Precision} = \frac{|Q_p \cap Q_t|}{|Q_p|}, \tag{15a}$$

$$\text{Recall} = \frac{|Q_p \cap Q_t|}{|Q_t|}, \tag{15b}$$

$$\text{F1} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}, \tag{15c}$$

where Q_p stands for the predicted set by a specific algorithm, Q_t denotes the ground-truth test set, and $|\cdot|$ denotes cardinality.

To evaluate the effect of the network topology, we consider two other metrics, including "malicious ratio", i.e., the ratio of the number of malicious UAVs detected initially (as done in Section IV-A) to the total number of UAVs, denoted by $R_M = |\mathbb{M}|/|\mathbb{N}|$. Correspondingly, the "benign ratio", i.e., the ratio of the number of UAVs initially determined as benign to the total number of UAVs, is $R_B = 1 - R_M$.

B. Visualization of Proposed Malicious UAV Detection

Fig. 5 shows the identifications of malicious UAVs in a UAV swarm with $N = 30$ UAVs under distributed spoofing attacks.

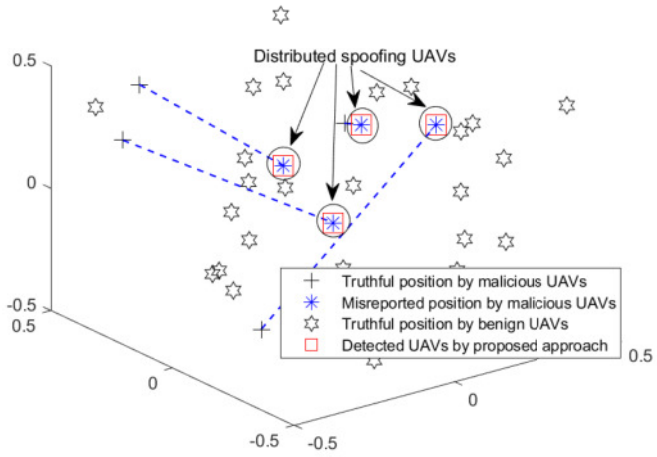

Fig. 5. An identification sample of the proposed approach against distributed spoofing attack in a UAV swarm with $N = 30$ UAVs and $M = 4$ malicious UAVs, where $d = 0.3$. The dashed lines exhibit the misreported distance.

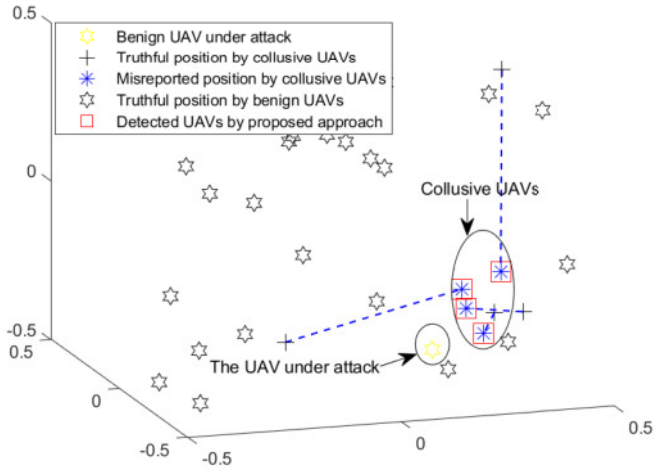

Fig. 6. An identification sample of the proposed approach against collusion spoofing attack, in a UAV swarm with $N = 30$ UAVs and $M = 4$ malicious UAVs, where $d = 0.3$. The dashed lines exhibit the misreported distance.

There are four malicious UAVs launching distributed spoofing attacks. Both the proposed CDI and E-CDI algorithms are simulated. Fig. 6 shows the identifications of malicious UAVs in the 30-UAV swarm under collusion attacks, where four malicious UAVs conspire collusion attacks towards a benign UAV. In Fig. 6, we only simulate the proposed E-CDI algorithm since the CDI algorithm is inapplicable to collusion attacks, as discussed in Section IV-C. Fig. 7 shows the identifications of malicious UAVs in the 30-UAV swarm under mixed attacks, where three malicious UAVs conspire collusion attacks towards a benign UAV, while three other malicious UAVs launch distributed attacks. We only run the proposed E-CDI algorithm in Fig. 7 for the same reason as considered for Fig. 6. From Figs. 5, 6, and 7, we can see that

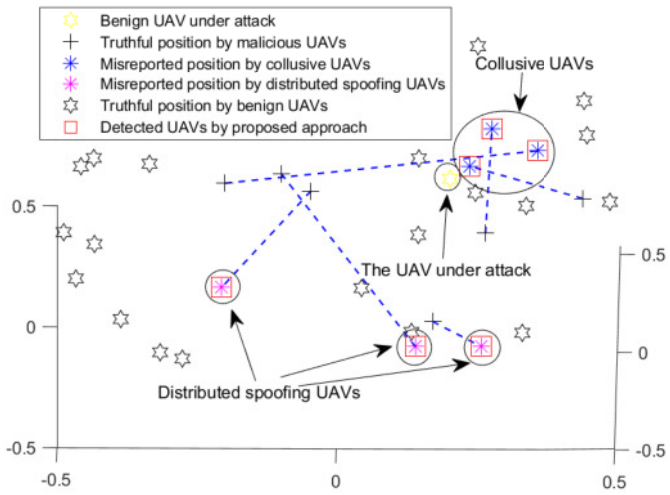

Fig. 7. An identification sample of the proposed approach against mixed spoofing attack, in a UAV swarm with $N = 30$ UAVs and $M = 6$ malicious UAVs, where $d = 0.3$. The dashed lines exhibit the misreported distance.

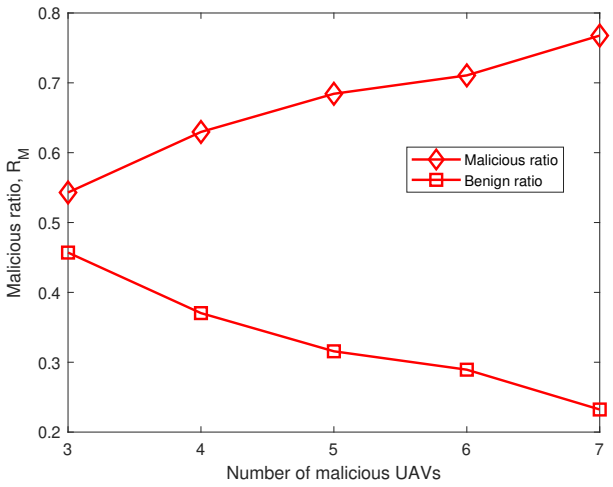

Fig. 8. The variations of malicious ratio.

the proposed CDI and E-CDI algorithms can effectively detect and identify malicious UAVs in applicable scenarios.

C. *Resistance to Distributed Spoofing Attacks*

Fig. 8 plots the malicious ratio and average available degree across different numbers of malicious UAVs, where the average of 100 independently randomly generated swarms with consistent parameters with Fig. 5 is plotted. It is noticed that the malicious ratio is nearly linear to the number of malicious UAVs. When there are seven malicious UAVs, the potential malicious ratio can reach zero, highlighting the presence of multiple malicious UAVs can severely disrupt or even dismantle the normal operation of a swarm.

In Fig. 9(a), we observe the Precision of the proposed algorithms compared to the benchmark methods. It is evident that both the CDI and E-CDI algorithms outperform the others significantly. The difference in Precision between the two

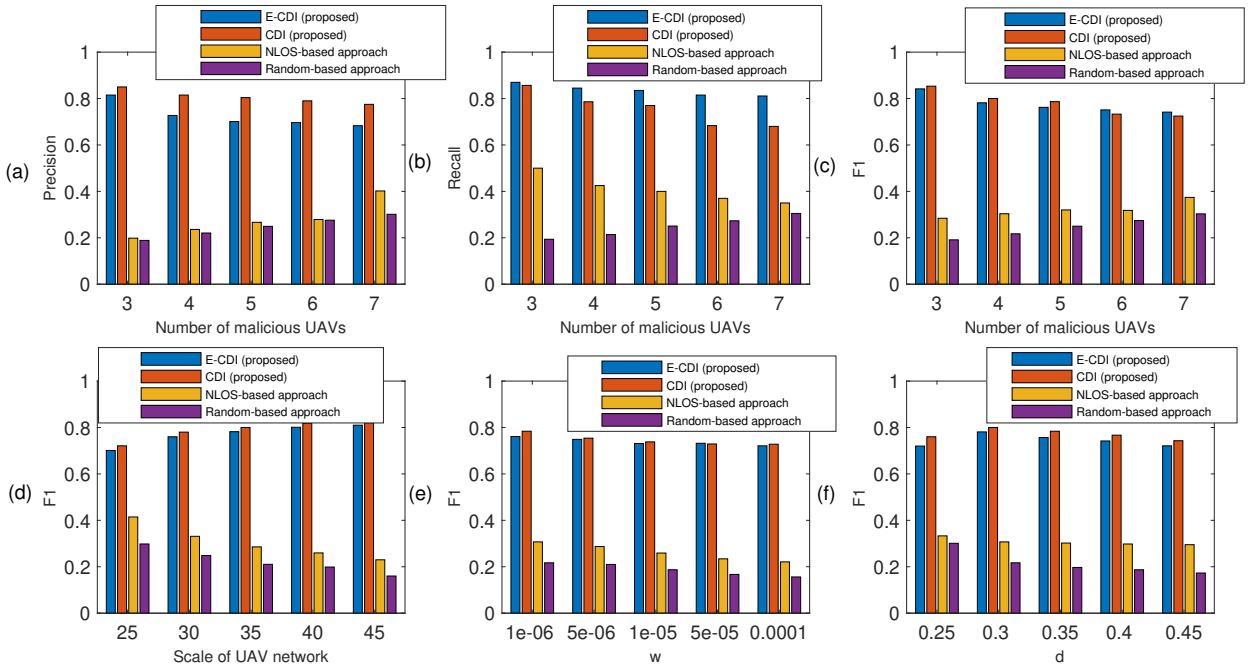

Fig. 9. (a) The performance on Precision of the proposed and baseline approaches. (b) The performance on Recall of the proposed and baseline approaches. (c) The performance on F1 of the proposed and baseline approaches. (d) The performance on F1 of the proposed and baseline approaches under different scales of the swarm network. (e) The performance on F1 of the proposed and baseline approaches under different levels of distance measurement noise. (f) The performance on F1 of the proposed and baseline approaches under different levels of measurement distance.

algorithms can be attributed to the strategy they employ for handling neighboring index sets. The E-CDI algorithm, which selects multiple indices simultaneously, may introduce some redundancies, leading to a slightly inferior Precision compared to the CDI algorithm, which selects one index at a time. Additionally, the decreasing trend in performance of both proposed approaches can be linked to the degradation of the network structure, as indicated by the increasing malicious ratio in Fig. 8.

On the other hand, there is a noticeable upward trend in the detection of malicious UAVs under the NLOS-based approach, especially those with significant distance errors akin to NLOS conditions. The NLOS-based approach, which involves selecting UAVs with the largest distance errors, simultaneously amplifies the likelihood of encountering malicious UAVs. The ascending trend in the Random approach can be explained by the situation where the rate of capturing malicious UAVs surpasses the expansion rate of the malicious set.

In Fig. 9(b), we examine the Recall of the proposed methods compared to the benchmarks across varying numbers of malicious UAVs. Both the CDI and E-CDI algorithms outperform all benchmarks significantly. Moreover, E-CDI offers higher Recall than CDI. The reason is that E-CDI sacrifices some precision, potentially introducing redundancies, to ensure the capture of more malicious UAVs. Given the critical security nature of the problem studied, it is imperative to emphasize high Recall to identify as many malicious UAVs as possible to safeguard the swarm. As also noticed, the Recall of both proposed algorithms declines due to the deteriorating network structure, as discussed in Fig. 9(a). For the same reason, the Recall of the NLOS-based approach also declines, as discussed in Fig. 9(a). As for the Random-based approach, it is intriguing to note that the trends in Precision in Fig. 9(a) and Recall in Fig. 9(b) bear resemblance. The conclusion drawn is that the expansion rate of captured malicious UAVs exceeds that of the malicious set enlargement, leading to this consistent trend.

Fig. 9(c) illustrates the F1 of the proposed methods alongside the benchmarks across varying numbers of malicious UAVs, where the proposed CDI and E-CDI algorithms consistently outperform all other algorithms. It is noticed that the E-CDI algorithm is initially better than the CDI algorithm. However, as the number of malicious UAVs increases, the CDI algorithm gradually surpasses the E-CDI algorithm when the number of malicious UAVs exceeds five. The reason is that when there are only a small number of malicious UAVs in a swarm, the E-CDI algorithm is more likely to misclassify benign UAVs as malicious. As the number of malicious UAVs increases and the network structure deteriorates, the E-CDI algorithm is increasingly advantageous. With a higher number of malicious UAVs, the E-CDI algorithm exhibits a greater likelihood of correctly detecting malicious UAVs.

We also notice in Fig. 9(c) that the NLOS-based approach outperforms the Random approach due to its selection from a relatively smaller malicious set with a higher probability, achieved through sorting based on absolute distance error. In contrast, the Random approach selects from a larger set encompassing all possible malicious UAVs. The increasing trend observed in both benchmark algorithms is attributed to the growing number of malicious UAVs, resulting in a higher probability of detection by both benchmarks.

Fig. 9(d) presents the F1 performance of our proposed algorithms compared to the benchmark algorithms across these varying network scales. Both the proposed CDI and E-CDI algorithms consistently outperform the other algorithms. An intriguing observation is that the CDI algorithm surpasses the E-CDI algorithm across all network scales. This is primarily attributed to the fixed number of malicious UAVs: As the network scales up, a larger number of benign UAVs are likely to be present, offering supporting evidence. However, this also introduces a risk for the E-CDI algorithm, which, while aiming for higher Recall, may inadvertently incorporate benign UAVs. By contrast, the CDI algorithm, which emphasizes higher Precision by meticulously identifying one UAV at a time, mitigates this risk. On the other hand, the declining trend observed in both benchmarks can be attributed to the larger network scale, leading to a lower probability of detection for both benchmarks. In particular, the increased number of malicious UAVs in a larger-scale network makes it hard for the benchmarks, which employ methods like selecting the largest absolute distance error or sampling from the potential malicious set, to identify the malicious UAVs effectively.

Fig. 9(e) presents the F1 performance of the proposed algorithms in comparison to the benchmarks across different levels of distance measurement inaccuracies. It is evident that all the algorithms exhibit a consistent declining trend, resulting from the adverse influence of inaccurate distance measurements on the effectiveness of constraints in (12). Nevertheless, the proposed algorithms maintain efficiency and robustness even in the face of elevated levels of measurement noise. This resilience stems from the fact that the algorithms leverage the entire swarm to aggregate evidence, effectively mitigating the impact of inaccurate distance measurements. On the other hand, the benchmarks face challenges with an increase in noise, as these inaccuracies can lead to greater disparities between the distances computed based on reported positions and the reported distance measurements. This, in turn, expands the candidate set of malicious UAVs, reducing the likelihood of detection by the benchmarks.

Fig. 9(f) provides an overview of the F1 performance of the proposed algorithms and the benchmarks across different measurement distances. In the case of the proposed algorithms, both initially exhibit an ascending trend, followed by a descent after reaching a threshold of 0.35. This is because the increase in measurement distance prompts more UAVs to become neighbors, thereby generating additional evidence for decision-making at the beginning. However, the larger measurement distance relaxes the constraints applied to directly counter-spoofing, permitting more malicious UAVs to evade detection and the F1 declines. In contrast, when considering the benchmark algorithms, the expansion of measurement distance implies that more neighbors are involved in the evidence-gathering process. This can result in a higher number of UAVs reporting pairwise distance measurements, consequently leading to greater disparities between the distances computed based on reported positions and the reported distance measurements. The resulting larger candidate set of malicious UAVs reduces the probability of detection by the benchmarks.

We further compare the proposed CDI and E-CDI algorithms in the number of iterations, as shown in Fig. 10. All parameters are kept consistent with those in Fig. 5, except for the number of malicious UAVs. When the number of malicious UAVs is relatively small, the CDI algorithm outperforms the E-CDI algorithm. As the number of malicious UAVs increases, a shift unfolds: the E-CDI algorithm gradually overtakes the CDI algorithm, and the performance gap between them widens with the growing number of malicious UAVs. This is because, when dealing with a small number of malicious UAVs, the CDI algorithm's scrutiny of each individual UAV is advantageous. But, as the number of malicious UAVs expands, the escalating number of malicious UAVs poses increasing feasibility challenges for the CDI algorithm. On the other hand, by prioritizing high Recall, the E-CDI algorithm aims to identify as many malicious UAVs as possible.

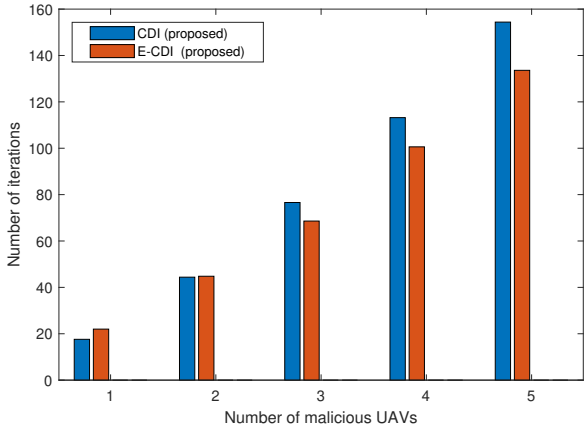

Fig. 10. The number of iterations required by the CDI and E-CDI algorithms.

D. Resistance to Collusion Spoofing Attacks

In line with Fig. 6, we delve into the evaluation of the F1 metric for the proposed E-CDI algorithm in comparison to the benchmarks. The CDI algorithm is not assessed, as explained in Section IV. To maintain consistency, we generate 100 UAV swarms randomly and independently with consistent parameters with those in Fig. 6, except for the number of malicious UAVs. Each data point represents the average of the 100 swarms.

Fig. 11(a) compares the F1 score between the E-CDI algorithm and the benchmarks under a collusion spoofing attack. Unlike the declining trend observed in Fig. 9(c), the proposed E-CDI algorithm exhibits an upward trend as malicious UAVs increase. On the one hand, collusion spoofing attacks have a distinct structure compared to distributed spoofing attacks in the sense that attackers are more likely to be densely concentrated around a targeted UAV. On the other hand, the E-CDI algorithm assesses potentially malicious UAVs individually if their neighborhood is detected to be infected by malicious UAVs, which is particularly effective in the densely populated neighborhood of a collusion attack. Consequently, the E-CDI can exploit the specific characteristics of collusion spoofing attacks.

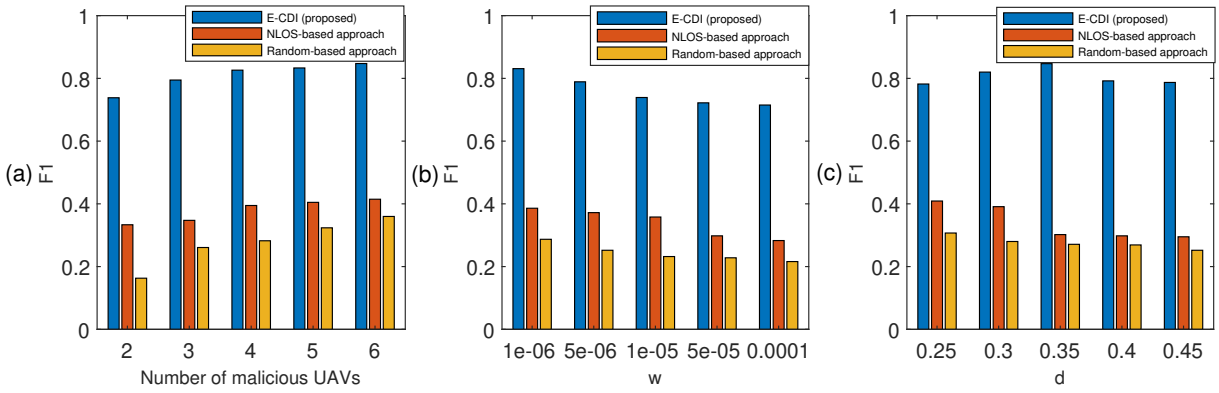

Fig. 11. The performance on F1 of the proposed and baseline approaches in collusion spoofing attack scenario. (a) Under different scales of malicious UAVs. (b) Under different levels of distance measurement noise. (c) Under different levels of measurement distance.

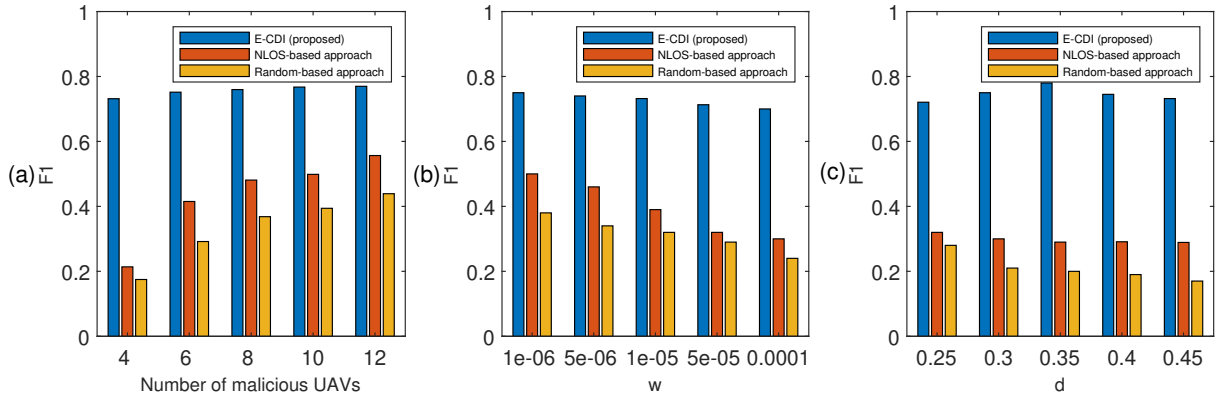

Fig. 12. The performance evaluation on F1 of the proposed and baseline approaches in mixed spoofing attack scenario. (a) Under different scales of malicious UAVs. (b) Under different levels of distance measurement noise. (c) Under different levels of measurement distance.

The ascending trend is also observed under the benchmark algorithms, resulting from the presence of densely concentrated UAVs, which tend to induce fewer disparities between the distance computed based on reported positions and the reported distance measurements. This, in turn, results in smaller candidate sets of malicious UAVs, which are more likely to be detected by the benchmarks.

We proceed to assess the impact of two critical parameters: distance measurement error and the range for distance measurement on the performance of the proposed E-CDI algorithm. With the increasing distance measurement noises, a descending trend of the F1 score can be observed in Fig. 11(b), as done in Fig. 9(e). On the other hand, a descending trend is also noticed with the increasing permissible distance in Fig. 11(c), which is consistent with the observation made in Fig. 9(f). Given that these two parameters exhibit a similar influence in both distributed and collusion scenarios, we can refer to the discussions about distributed spoofing in Section V-C for the sake of brevity.

E. Resistance to Mixed Spoofing Attack

As considered in Fig. 7, we proceed to assess the F1 metric of the proposed E-CDI algorithm, comparing it to the benchmarks. A total of 100 UAV swarms are generated randomly and independently with consistent parameters with those considered in Fig. 7, except for the number of malicious UAVs. Each data point represents the average of the 100 swarms.

In Fig. 12(a), we analyze the F1 performance of the proposed E-CDI algorithm compared to the benchmarks in the context of a mixed spoofing attack. In order to conduct a fair evaluation across various numbers of malicious UAVs, we evenly distribute the malicious UAVs into two distinct groups. For instance, when dealing with six malicious UAVs, we assign three of them to execute distributed attacks. The remaining three are directed toward launching collusion attacks against a benign UAV. It is noted that the mixed spoofing attack cannot be simply regarded as the superposition of distributed and collusion attacks. The amalgamation of these different attack types within the mixed scenario introduces substantial variations in the network structure.

Comparing the trends seen in Fig. 12(a) to those in Figs. 9(c) and 11(a), it is evident that the performance of the proposed E-CDI algorithm follows a similar ascending trend as observed in Fig. 11(a), which is different from the trend in Fig. 9(c). As malicious UAVs increase, the network structure undergoes a notable transformation. Initially, both distributed attacks and collusion attacks contribute evenly. However, with a greater

number of attackers, more malicious UAVs initially involved in distributed attacks inadvertently become participants in collusion attacks. This shift results in the gradual dominance of collusion attacks. Consequently, the performance trend observed in the mixed spoofing attack aligns with the pattern shown in Fig. 11(a), although there can be a slight performance degradation for the same number of malicious UAVs.

In the case of the benchmarks, the ascending trend of their F1 scores can be attributed to the presence of densely concentrated UAVs, which tends to reduce the disparities between the distance computed based on reported positions and the reported distance measurements, as discussed earlier.

Last but not least, we assess the impact of distance measurement error and the permissible distance for distance measurement on the performance of the proposed E-CDI algorithm. It is noticed that Fig. 12(b) yields a declining trend like the one observed in Fig. 9(e), while Fig. 12(c) displays a decreasing pattern like the one shown in Fig. 9(f). Given that these two parameters have consistent effects under the distributed and collusion attacks, the reason underlying the observations in Figs. 12(b) and 12(c) can be established, as discussed in Section V-C. It is worth highlighting that there exists a marginal performance decline for the same number of malicious UAVs when compared to the distributed attacks. This is due to the more intricate degradation of the network structure exacerbated by the interplay of mixed attacks.

VI. Conclusion

In this paper, we judiciously formulated a complicated malicious UAV detection problem based on the reported positions and pairwise distance measurements of the UAVs as a localization feasibility problem. Then, we relied on an SDR approach to recast the formulated non-convex problem into a convex SDP, which is the key to assessing the feasibility of the reported positions and distance measurements. Moreover, we proposed two tailored iterative algorithms based on the proposed SDP approach to detect and identify malicious UAVs in UAV swarms. Extensive simulations demonstrated that the proposed algorithms can achieve superior performance to the existing benchmarks and exhibit robustness across various UAV swarms.

References

[1] S. Hu, W. Ni, X. Wang, A. Jamalipour, and D. Ta, "Joint optimization of trajectory, propulsion, and thrust powers for covert UAV-on-UAV video tracking and surveillance," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1959–1972, Jan. 2021.

[2] B. Liu, W. Ni, R. P. Liu, Y. J. Guo, and H. Zhu, "Decentralized, privacy-preserving routing of cellular-connected unmanned aerial vehicles for joint goods delivery and sensing," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 9, pp. 9627–9641, 2023.

[3] X. Yuan, S. Hu, W. Ni, X. Wang, and A. Jamalipour, "Deep reinforcement learning-driven reconfigurable intelligent surface-assisted radio surveillance with a fixed-wing UAV," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 4546–4560, 2023.

[4] A. V. Savkin, W. Ni, and M. Eskandari, "Effective UAV navigation for cellular-assisted radio sensing, imaging, and tracking," *IEEE Trans. Veh. Technol.*, 2023, early access.

[5] K. Li, R. C. Voicu, S. S. Kanhere, W. Ni, and E. Tovard, "Energy efficient legitimate wireless surveillance of UAV communications," *IEEE Trans. Veh. Tech.*, vol. 68, no. 3, pp. 2283–2293, Mar. 2019.

[6] S. Hu, X. Yuan, W. Ni, and X. Wang, "Trajectory planning of cellular-connected UAV for communication-assisted radar sensing," *IEEE Trans. Commun.*, vol. 70, no. 9, pp. 6385–6396, Sep. 2022.

[7] X. Yuan, Z. Feng, W. Ni, R. P. Liu, J. A. Zhang, and W. Xu, "Secrecy performance of terrestrial radio links under collaborative aerial eavesdropping," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 604–619, 2020.

[8] B. Song, X. Wang, W. Ni, Y. Song, R. P. Liu, G. Jiang, and Y. J. Guo, "Reliability analysis of large-scale adaptive weighted networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 651–665, 2020.

[9] X. Yuan, Z. Feng, W. Ni, Z. Wei, R. P. Liu, and C. Xu, "Connectivity of UAV swarms in 3d spherical spaces under (un)intentional ground interference," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 8792–8804, 2020.

[10] S. Bi, C. Wang, B. Wu, S. Hu, W. Huang, W. Ni, Y. Gong, and X. Wang, "A comprehensive survey on applications of AI technologies to failure analysis of industrial systems," *Eng. Fail. Anal.*, vol. 148, 2023.

[11] Y. E. Yao, P. Dash, and K. Pattabiraman, "May the swarm be with you: Sensor spoofing attacks against drone swarms," in *Proc. ACM SIGSAC CCS*, 2022, p. 3511–3513.

[12] H. Choi, W.-C. Lee, Y. Aafer, F. Fei, Z. Tu, X. Zhang, D. Xu, and X. Deng, "Detecting attacks against robotic vehicles: A control invariant approach," in *Proc. ACM SIGSAC CCS*, 2018, p. 801–816.

[13] I. Buske, A. Walther, D. Fitz, J. Acosta, A. Konovaltsev, and L. Kurz, "Smart GPS spoofing to countermeasure autonomously approaching agile micro UAVs," in *Proc. SPIE*, vol. 12273, 2022.

[14] Y. Liu, Y. Wang, J. Wang, and Y. Shen, "Distributed 3D relative localization of UAVs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, p. 11756 – 11770, 2020.

[15] P. Jiang, H. Wu, and C. Xin, "Deeppose: Detecting GPS spoofing attack via deep recurrent neural network," *Digit. Commun. Netw.*, vol. 8, no. 5, p. 791 – 803, 2022.

[16] B. Pardhasaradhi and L. R. Cenkeramaddi, "GPS spoofing detection and mitigation for drones using distributed radar tracking and fusion," *IEEE Sens. J.*, vol. 22, no. 11, p. 11122 – 11134, 2022.

[17] A. Khan, N. Ivaki, and H. Madeira, "Are UAVs' flight controller software reliable?" in *Proc. IEEE PRDC*, 2022, pp. 194–204.

[18] K. Liu, Y. Zhao, G. Wang, and R. Xue, "Quadrotor visual navigation under GPS spoofing attack," in *Proc. WiSPNET*, 2021, pp. 270–277.

[19] Y. Dang, C. Benzaïd, T. Taleb, B. Yang, and Y. Shen, "Transfer learning based GPS spoofing detection for cellular-connected UAVs," in *Proc. IWCMC*, 2022, pp. 629–634.

[20] W. Chen, Y. Dong, and Z. Duan, "Accurately redirecting a malicious drone," in *Proc. IEEE CCNC*, 2022, pp. 827–834.

[21] Z. Wang, X. Zhang, Z. Zhou, M. Lu, and H. Li, "GNSS spoofer localization for vehicles based on doppler and clock drift double difference," *IEEE Trans. Veh. Technol.*, p. 1–16, 2022.

[22] G. Michieletto, F. Formaggio, A. Cenedese, and S. Tomasin, "Robust localization for secure navigation of UAV formations under GNSS spoofing attack," *IEEE Trans. Autom. Sci. Eng.*, p. 1–14, 2022.

[23] M. Babaghayou, N. Labraoui, A. A. A. Ari, N. Lagraa, M. A. Ferrag, and L. Maglaras, "SAMA: Security-aware monitoring approach for location abusing and UAV GPS-spoofing attacks on Internet of vehicles," *Proc. LNICST*, vol. 427 LNICST, p. 343 – 360, 2022.

[24] S. Bi, J. Cui, W. Ni, Y. Jiang, S. Yu, and X. Wang, "Three-dimensional cooperative positioning for Internet of Things provenance," *IEEE Internet Things J.*, vol. 9, no. 20, pp. 19 945 – 19 958, 2022.

[25] Y. Wang, X. Wen, Y. Cao, C. Xu, and F. Gao, "Bearing-based relative localization for robotic swarm with partially mutual observations," *IEEE Robot. Autom. Lett.*, vol. 8, no. 4, p. 2142 – 2149, 2023.

[26] J. Yang, T. Zhang, X. Wu, T. Liang, and Q. Zhang, "Efficient scheduling in space-air-ground integrated localization networks," *IEEE Internet Things J.*, 2022.

[27] B. Jiang, B. D. O. Anderson, and H. Hmam, "3-D relative localization of mobile systems using distance-only measurements via semidefinite optimization," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 3, p. 1903 – 1916, 2020.

[28] Z. Wu, W. Quan, and T. Zhang, "Resource allocation in UAV-aided vehicle localization frameworks," in *Proc. IEEE ICCC Workshops*, 2019, p. 98 – 103.

[29] P. Biswas, T.-C. Lian, T.-C. Wang, and Y. Ye, "Semidefinite programming based algorithms for sensor network localization," *ACM Trans. Sen. Netw.*, vol. 2, no. 2, p. 188–220, may 2006. [Online]. Available: https://doi.org/10.1145/1149283.1149286

[30] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[31] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming," 2008. [Online]. Available: http://cvxr.com/cvx
[32] I. Um, S. Park, S. Oh, and H. Kim, "Analyzing location accuracy of unmanned vehicle according to RTCM message frequency of RTK-GPS," in *Proc. APCC*, 2019, pp. 326–330.
[33] W. Zhao, R. He, B. Ai, Z. Zhong, and H. Zhang, "Vehicle localization based on hypothesis test in NLOS scenarios," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 2198–2203, 2022.
[34] S. Bi, W. Ni, Y. Jiang, and X. Wang, "Novel recommendation-based approach for multidisciplinary development of future universities," *Sustainability*, vol. 14, no. 10, 2022.

Siguo Bi received the Ph.D. degree in Electronic Science and Technology from Fudan University, Shanghai, China, in 2020. He is now an engineer with Fudan University, China. His research interests include wireless sensor network, convex optimization, network security in UAV swarm, and machine learning applied in communications.

Kai Li (S'09-M'14-SM'20) received his B.E. degree from Shandong University, Weihai, China, in 2009, his M.S. degree from The Hong Kong University of Science and Technology, Hong Kong, in 2010, and his Ph.D. degree in computer science from The University of New South Wales, Sydney, NSW, Australia, in 2014. Currently, he serves as a Visiting Research Scientist within the Division of Electrical Engineering at the Department of Engineering, University of Cambridge, United Kingdom. Additionally, he holds the position of Senior Research Scientist at CISTER Research Centre, Porto, Portugal. He is also a CMU-Portugal Research Fellow, jointly supported by Carnegie Mellon University, Pittsburgh, PA, USA, and The Foundation for Science and Technology (FCT), Lisbon, Portugal. In 2022, he served as a Visiting Research Scholar at the CyLab Security and Privacy Institute, CMU. Prior to this engagement, he was a Postdoctoral Research Fellow at the SUTD-MIT International Design Centre, The Singapore University of Technology and Design, Singapore, from 2014 to 2016. He has also held positions as a Visiting Research Assistant at the ICT Centre, CSIRO, Brisbane, Queensland, Australia, from 2012 to 2013, and as a Research Assistant at the Mobile Technologies Centre, The Chinese University of Hong Kong, Hong Kong, from 2010 to 2011. He has served as an Associate Editor for the Springer Nature Computer Science Journal since 2023, the Elsevier Computer Communications Journal and Elsevier Ad Hoc Networks Journal since 2021, as well as the IEEE Access Journal since 2018.

Shuyan Hu (M'20) received the B.Eng. degree in Electrical Engineering from Tongji University, China, in 2014 and the Ph.D. degree in Electronic Science and Technology from Fudan University, China, in 2019. She is currently a postdoctoral research fellow with the School of Information Science and Technology, Fudan University. She was selected by the Shanghai Postdoctoral Excellence Program in 2019. Her research interests include machine learning and convex optimizations and their applications to unmanned aerial vehicle (UAV) networks and intelligent systems.

Wei Ni (M'09-SM'15-F'24) received the B.E. and Ph.D. degrees in Electronic Engineering from Fudan University, Shanghai, China, in 2000 and 2005, respectively. Currently, he is a Principal Research Scientist at CSIRO, Sydney, Australia, a Conjoint Professor at the University of New South Wales, an Adjunct Professor at the University of Technology Sydney, and an Honorary Professor at Macquarie University. He was a Postdoctoral Research Fellow at Shanghai Jiaotong University from 2005 to 2008, Deputy Project Manager at Bell Labs, Alcatel/Alcatel-Lucent from 2005 to 2008, and Senior Researcher at Devices R&D, Nokia from 2008 to 2009. He has authored eight book chapters, over 300 journal papers, 100 conference papers, 26 patents, and ten standard proposals accepted by IEEE. His research interests include machine learning, online learning, stochastic optimization, and their applications to system efficiency and integrity.

Dr Ni has served as an Editor of IEEE Transactions on Wireless Communications since 2018 and an Editor of IEEE Transactions on Vehicular Technology. He served first as the Secretary, then the Vice-Chair and Chair of the IEEE Vehicular Technology Society (VTS) New South Wales (NSW) Chapter from 2015 to 2022, Workshop Chair for ISCIT 2023, Track Chair for VTC-Spring 2017, Track Co-chair for IEEE VTC-Spring 2016, Publication Chair for BodyNet 2015, and Student Travel Grant Chair for WPMC 2014.

Cong Wang received B.E. and M.S. degrees both from Fudan University, China. Her research interests include machine learning, bioinformatics, and statistics.

Xin Wang (SM'09-F'23) received the B.Sc. and M.Sc.degrees from Fudan University, Shanghai, China, in 1997 and 2000, respectively, and the Ph.D. degree from Auburn University, Auburn, AL, USA, in 2004, all in electrical engineering.

From September 2004 to August 2006, he was a Postdoctoral Research Associate with the Department of Electrical and Computer Engineering, University of Minnesota, Minneapolis. In August 2006, he joined the Department of Electrical Engineering, Florida Atlantic University, Boca Raton, FL, USA, as an Assistant Professor, then was promoted to a tenured Associate Professor in 2010. He is currently a Distinguished Professor and the Chair of the Department of Communication Science and Engineering, Fudan University, China. His research interests include stochastic network optimization, energy-efficient communications, cross-layer design, and signal processing for communications. He served as a Senior Area Editor for the IEEE Transactions on Signal Processing, as an Associate Editor for the IEEE Transactions on Signal Processing, as an Editor for the IEEE Transactions on Wireless Communications, as an Editor for the IEEE Transactions on Vehicular Technology, and as an Associate Editor for the IEEE Signal Processing Letters. He is a member of the Signal Processing for Communications and Networking Technical Committee of IEEE Signal Processing Society, and a Distinguished Speaker of the IEEE Vehicular Technology Society.