Resilient Range-Only Cooperative Positioning of Multiple Smart Unmanned Aerial Systems

Yajie Bao[1(✉)], Dan Shen[1], Genshe Chen[1], Khanh Pham[2], and Erik Blasch[3]

[1] Intelligent Fusion Technology, Inc., Germantown, MD 20876, USA
{yajie.bao,dshen,gchen}@intfusiontech.com
[2] Air Force Research Lab, Kirtland AFB, Albuquerque, NM 87117, USA
khanh.pham.1@spaceforce.mil
[3] Air Force Office of Scientific Research, Arlington, VA 22203, USA

Abstract. Deploying multiple Unmanned Aerial Systems (UASs) is beneficial for applications that survey large regions and require cooperative redundancy. Range-only cooperative navigation has been proposed to enhance positioning precision by exchanging navigation information, especially in Global Navigation Satellite Systems (GNSS)-denied environments. However, existing works do not consider the possible attacks on range-only positioning in exceptionally adverse environments and do not investigate the resilience of cooperative navigation. In this paper, we consider the attacks on range measurements in the context of distributed range-only positioning using the Extended Kalman Filter (EKF) and present an anti-attack approach by integrating the Inertial Measurement Units (IMU) with the distributed position estimator. Moreover, this paper evaluates the resilience of the cooperative navigation system under Gaussian and non-Gausisian attacks. Extensive simulations on a cooperative task for multiple UASs to survey a target area demonstrate that the range-only positioning by EKF is vulnerable to non-Gaussian attacks and that the proposed anti-attack approach can detect the attacks with a high probability and mitigate the performance degradation caused by attacks.

Keywords: Resilient positioning · range-only positioning · distance manipulation attacks · cooperative positioning

1 Introduction

Positioning is an essential utility for many cyber-physical system operations such as smart vehicles and intelligent transportation. The Global Positioning Sys-

This material is partially based upon work supported by the AFRL under Contract No. FA9453-23-P-A019. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the United States Air Force or the U.S. Government.

Y. Chen et al. (Eds.): SmartSP 2023, LNICST 552, pp. 130–147, 2024.
https://doi.org/10.1007/978-3-031-51630-6_9

tem (GPS) and other Global Navigation Satellite Systems (GNSS) are accurate sources for positioning but may be vulnerable to intentional attacks [5,14,15]. There are two main types of attacks for GNSS systems: a) jamming [3] to affect the availability of the GNSS satellite signals by generating powerful signals in the GNSS band; and b) spoofing to deceive the GNSS user navigation by transmitting signals that share the same characteristics with the legitimate GNSS satellite signals [13]. GNSS spoofing can even take over the control of UASs that rely on GNSS for navigation [20]. To detect attacks, signal processing techniques based on the characterization of the attacks have been developed by checking distortions or disruptions of signals [19]. Furthermore, the integration of independent measurements and information has been considered for attack detection by monitoring drifts of the receiver position and/or clock. Moreover, simultaneously using complementary strategies has been proposed to compensate for the weaknesses of an individual attack detection technique that might be exploited by a sophisticated spoofer.

Other methods to provide security for communications include blockchain security, data encryption, user authentication, message hiding, and signal analysis. Monitoring the signals analysis can only detect spoofing and cannot correct the error [24]. A hidden message would require a larger channel capacity and methods to resolve the true signal [9]. While authentication could be a solution [26], if the signal is spoofed, it would require protocols that cause timing delays amongst many sources requiring ID-based signature message recovery [31]. Since navigation methods like GPS and automatic dependent surveillance-Broadcast (ADS-B) could add authentication, there are still ways to send incorrect messages. Encryption is challenging as it is not backward compatible and would require a fundamental alteration of the signals with standardized approaches [25]. Currently, there are efforts towards secure distributed edge-based methods [8] that could use blockchain which is popular for smart sensors [28]. Analysis of blockchain for avionics shows promise, but increases the message size, reduces timing, and requires more memory [27], and efforts are underway to make the system lighter [29]. Hence the only current solution is to have another massage source such as a designated radar signal that is typically only located at designated airports. Using another onboard edge sensing source to detect and correct the spoofing as well as be available for GNSS jamming would provide a practical solution for continuous navigation.

Range-only positioning provides an alternate source of position estimations using relative distances to fixed or dynamic beacons [2]. In the case of multiple UASs, cooperative navigation/positioning where individual UASs exchange information to improve their own position estimation has been developed for robust positioning [21]. For example, the authors [12] proposed a distributed consensus-based distributed EKF approach for collaborative relative navigation. Furthermore, observability for range-only cooperative localization using extended/unscented Kalman filters (KF) has been established [6] as well as bearings-only tracking [10]. Trajectory planning for favorable network configuration in terms of optimality measures has been studied to control the statistical

properties of the localization error [17,30]. However, the existing works do not consider the attacks on the range sensors or information exchange in adverse environments which may cause large errors in range measurements besides the normal measurement noise and thus degrade the positioning performance [22]. Moreover, since the commonly used extended/unscented KF assumes Gaussian noise for range-only positioning, non-Gaussian attacks may cause severe performance degradation and escape attack detections like the innovation testing [1]. In this paper, we investigate the performance of distributed range-only positioning systems under both Gaussian and non-Gasussian attacks.

To detect and mitigate the attacks on the range-only positioning, we use inertial measurement units (IMU) as another source of positioning, similar to the integration of GNSS and IMU for anti-attacks [7,19]. It is noted that dead reckoning based on IMU measurements cannot provide precise positioning without an accurate previously determined position. However, the IMU is less susceptible to signal/data attacks. Therefore, we can combine the range-only positioning and IMU to detect attacks. By discarding the attacked UASs, the rest UASs may still achieve accurate positioning when the unattacked nodes can ensure the observability of the cooperative positioning system.

The main contribution of this paper lies in presenting a distributed EKF-based approach integrated with IMU-based positioning for the detection and mitigation of distance manipulation attacks on the range-only cooperative positioning of multiple UASs in GNSS-denied environments. The remainder of the paper is organized as follows: Sect. 2 gives the problem formulation, including the dynamic models and the preliminaries of the distributed EKF (DEKF); Sect. 3 introduces the distance manipulation attacks and anti-attack approach based on DEKF and IMU; Sect. 4 provides experimental results; and finally, Sect. 5 summarizes this paper.

2 Problem Formulation

Consider a system of multiple UASs that consist of a leader node N_0 and N_s follower nodes where $s = 1, \cdots, S$; the leader node is hovering at a position/maintains high-precision positioning while the follower nodes need to fly through a potential GPS-denied region towards a target area. Each UAS can obtain the relative distance to the leader node and the neighboring UASs using the time of arrival (TOA) mode via a data link during the flight. Moreover, the data link may be spoofed and transmit misleading range measurements. Additionally, the UASs can obtain measurements of gyro rate and acceleration from the onboard low-cost IMU, azimuth from the magnetometer, air speed measured from a Pitot tube, and height (from the ground) from a baro-altimeter.

The problem addressed in this work is how to design a resilient scheme for employing the range measurements and internal measurements to achieve an acceptable estimation of positions in the GPS-denied and/or spoofing environments, as shown by Fig. 1.

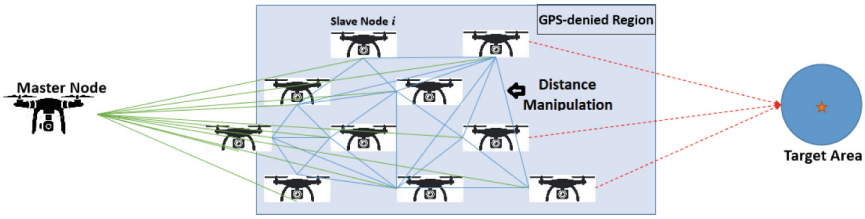


Fig. 1. Range-only positioning in GPS-denied environments under distance manipulation attacks.

2.1 Dynamic Models and Measurements

Denote x_0 as the 3-D coordinates of the leader node. Without loss of generality, we use a global coordinate/frame without considering the transition from the local frame to the global frame and $x_0 = [0, 0, 0]^\top$. The dynamic process and the local observation of each node i can be described using the following state-space model:

$$x_i(k+1) := \left[x_{i,1}(k+1)\ x_{i,2}(k+1)\ x_{i,3}(k+1)\right]^\top \tag{1a}$$

$$= \begin{bmatrix} x_{i,1}(k) \\ x_{i,2}(k) \\ x_{i,3}(k) \end{bmatrix} + \begin{bmatrix} u_{i,1}(k) \\ u_{i,2}(k) \\ u_{i,3}(k), \end{bmatrix} \mathrm{d}t + \omega_i(k), \tag{1b}$$

$$y_{i,j}(k) = \sqrt{(x_i(k) - x_j(k))^\top (x_i(k) - x_j(k))} + \nu_i(k), \tag{1c}$$

$$i = 1, \cdots, N_s, j \in \mathcal{N}_i(k), \tag{1d}$$

where x_i and u_i denote the coordinates and velocities of the i-th node, respectively; $k \in \mathbb{N}$ is the time instant and $\mathrm{d}t$ is the time increment; $\omega_i \in \mathbb{R}^3$ is the process noise with covariance matrix denoted by $Q(k)$; $y_{i,j}$ is the range measurements between node i and j and $\nu_i \in \mathbb{R}^3$ is measurement noise with covariance matrix denoted by $R(k)$ which is assumed to follow normal distribution; $\mathcal{N}_i$ is the set of neighboring nodes for the node i. It is noted that $\mathcal{N}_i$ is varying as a result of the dynamics of UASs. Moreover, the cardinality $|\mathcal{N}_i|$ (i.e., the number of neighbors) is a tuning parameter, which can be determined based on the verification of the measurement data for resilience.

It is noted that $y_{i,j} = y_{j,i}$ may not hold due to measurement errors. One approach for positioning is a centralized method, i.e., the follower nodes transmit the measurements to the leader and the leader uses the extended/unscented Kalman filter to estimate the positions. However, regardless of the computational and communication cost, this approach may not work in case parts of the nodes fail to transmit reliable measurements to the leader node due to interruptions of communications or spoofing.

Instead, we consider a distributed approach where each follower node uses the range measurements w.r.t. the leader node and neighboring nodes for positioning such that an acceptable estimation can still be achieved in case of failures

of partial nodes. It is assumed that the leader node is far enough away, has anti-jamming and anti-spoofing extra analytic capabilities, and otherwise is resilient to attacks. Moreover, the follower node can use internal measurements and previous estimations for positioning when attacks are detected and reliable range measurements are not available.

2.2 Distributed Extended Kalman Filter

Range-only positioning requires a nonlinear state estimator due to the nonlinearity of Eq. (1c). EKF is an efficient approach for nonlinear state estimation. In particular, the EKF linearizes the nonlinear measurement and/or state transition functions using the first-order Taylor series at the current best state estimate for filtering and predictions of states. Specifically, the linearized model at time instant k is

$$x(k+1) = F(k)x(k) + G(k)\omega(k) + u(k), \tag{2a}$$

$$\bar{y}(k) \approx H(k)x(k) + \nu(k), \tag{2b}$$

where $x = [x_1^\top, \cdots, x_S^\top]^\top$ represents the augmented states that consist of the states of all the follower nodes, $F(k) = \frac{\partial f}{\partial x}|_{\hat{x}(k|k-1)}$ with $x(k+1) = f(x(k)) + G(k)\omega(k) + u(k)$ denoting the state transition function; $H(k) = \frac{\partial h}{\partial x}|_{\hat{x}(k|k-1)}$ with $y = h(x)$ denoting the nonlinear measurement functions; $\bar{y}(k) = y(k) - h(\hat{x}(k|k-1)) + H(k)\hat{x}(k|k-1)$. Then, at time instant k, the correct step based on the measurements is

$$P(k|k) = (P^{-1}(k|k-1) + H^\top(k)R^{-1}(k)H(k))^{-1}, \tag{3a}$$

$$\hat{x}(k|k) = \hat{x}(k|k-1) + P(k|k)H^\top(k)R^{-1}(k)\left(\bar{y}(k) - H(k)\hat{x}(k|k-1)\right); \tag{3b}$$

the prediction step is

$$\hat{x}(k+1|k) = f(\hat{x}(k|k)), \tag{4a}$$

$$P(k+1|k) = F(k)P(k|k)F^\top(k) + G(k)Q(k)G^\top(k). \tag{4b}$$

Instead, the distributed EKF uses the local measurements for correction and prediction and obtains an accurate estimate of the entire system state variables based on consensus [4]. In particular, the consensus-based correct step [23] for

the i-th node in a network of homogeneous nodes is

$$\hat{\mathbf{x}}_i^l(k|k) = \left(\frac{1}{N_s^+}P_i^{-1}(k|k-1) + H_i^\top(k)R_i^{-1}(k)H_i(k)\frac{|\mathcal{N}_i^+|}{\mu}I\right)^{-1} \cdot \left[H_i^\top(k)R_i^{-1}(k)\bar{y}_i(k) + \frac{1}{N_s^+}P_i^{-1}(k|k-1)\hat{\mathbf{x}}_i(k|k-1) + \sum_{j\in\mathcal{N}_i^+}\left(\frac{z_j(k)^{l-1}}{\mu} + \lambda_{ij}^{l-1}\right)\right] \tag{5a}$$

$$z_i(k)^l = \frac{\mu}{|\mathcal{N}_i^+|}\sum_{j\in\mathcal{N}_i^+}\left(\frac{1}{\mu}\hat{\mathbf{x}}_j^l(k|k) - \lambda_{ji}^{l-1}\right), \tag{5b}$$

$$\lambda_{ij}^l = \lambda_{ij}^{l-1} - \frac{1}{\mu}\left(\hat{\mathbf{x}}_i^l(k) - z_j^l(k)\right), \tag{5c}$$

$$\forall\ i = 1, \cdots, N_s,\ j \in \mathcal{N}_i^+,\ l = 1, \cdots, L \tag{5d}$$

where $\hat{\mathbf{x}}_i^l$ is Node i's estimate of x using local P_i,H_i, and R_i at Node i for the l-th iteration, and $P_i(0|0) = P_0$; z_i^l is the auxiliary variable with initialization $z_i^0(k) = \hat{\mathbf{x}}_i(k|k-1)$, $\lambda_{i,j}^l$ is the Lagrange multiplier with initialization $\lambda_{i,j}^0 = 0$, and μ is a scalar penalty parameter; z_j, $\hat{\mathbf{x}}_j, j \in \mathcal{N}_i$ are transmitted from the $|\mathcal{N}_j|$ nearest neighbors of Node i based on the noisy range measurements; $N_s^+ = N_s + 1$, and $\mathcal{N}_i^+ = \mathcal{N}_i \cup \{i\}$; the correction of the covariance matrix is

$$P_i(k|k) = \left(P_i^{-1}(k|k-1) + \sum_{i=1}^{N_s} H_i^\top(k)R_i^{-1}(k)H_i(k)\right)^{-1}; \tag{6}$$

The prediction step for the i-th node is

$$\hat{x}_i(k+1|k) = f(\hat{x}_i(k|k)), \tag{7a}$$

$$P_i(k+1|k) = F_i(k)P_i(k|k)F_i^\top(k) + G(k)Q(k)G^\top(k). \tag{7b}$$

The main advantage of the DEKF approach is that it can reduce the computational burden and communication overhead as compared to a centralized approach. The DEKF can be more scalable and robust versus a centralized (CEKF), especially in systems with a large number of sensors distributed across different locations and limited, unreliable, or costly communication between nodes.

3 Distance Manipulation Attacks

In this section, we introduce the distance manipulation attacks on the range-only cooperative positioning and present the proposed approaches to detecting and preventing the attacks.

3.1 Attacks on Range Measurements

The demand for ranging information is increasing for autonomous and cyber-physical systems in various applications such as positioning and navigation, which makes it a target of attackers with different motivations. Existing ranging systems such as ultra-wideband (UWB) ranging systems are vulnerable to distance manipulation attacks. Distance manipulation attacks can be performed by manipulating the logical or physical layer. Logical-layer attacks manipulate message bits while physical-layer attacks involve manipulating signal characteristics to incorrectly measure the signal's phase, amplitude, frequency, or arrival time [22]. Additionally, distance manipulation attacks can be divided into distance reduction and enlargement attacks. An attacker may reduce the measured distance by manipulating the time of arrival (ToA) estimation of the preamble (via cicada attack [18]) and the payload (via Early Detect Late Commit (ED/LC) attack) [11] and enlarge the measured distance by preventing legitimate payload detection by increasing the bit error by adding noise in the channel or canceling some of the pulses. The availability of affordable radio devices like the software-defined radio has opened up vast possibilities for cybersecurity and infosec professionals to explore radio frequency (RF) communication and control devices, enabling them to delve into hacking in this domain.

In the case of range-only positioning, we consider the distance manipulation attacks introducing extra range measurement disturbances. Specifically, the attacked range measurements

$$\tilde{y}_{i,j}(k) = \begin{cases} y_{i,j}(k) + b_{i,j}(k), \, i \in \mathcal{A}_V(k), k \in \mathcal{A}_T \\ y_{i,j}(k) \qquad\qquad\quad \text{otherwise} \end{cases}, \tag{8}$$

where $b_{i,j}(k)$ denotes the modification of Node i's measurement of the range between Node i and j at time k; $\mathcal{A}_V(k)$ is the set of attacked nodes and $\mathcal{A}_T$ is the set of attacked time steps. Then, the centralized/distributed EKF use $\tilde{y}_{i,j}(k)$ at each time step to correct positioning estimation, which may cause large deviations from the real positioning.

3.2 Attack Detection and Mitigation

Using alternative positioning sources is a common strategy to detect and mitigate attacks. In addition to the range measurements, IMU measurements can be used for positioning. In particular, the raw IMU measurements can be utilized to calculate position relative to a global reference frame via a method known as dead reckoning. Using a previously determined position, dead reckoning can provide an accurate current position by $\hat{x}(k) = \hat{x}(k-1) + \delta\hat{x}(k-1)$ where $\delta\hat{x}$ denotes the displacement computed by the data of IMU sensors. Moreover, the IMU is less vulnerable to attacks than range-only positioning for which communications between nodes are required. However, dead reckoning is subject to cumulative errors over time and causes significant drifts over great distances.

For attack detection of GNSS and IMU, innovation testing [1] is widely used. However, the EKF may mitigate the effects of attacks such that the differences

between the position estimates of range and IMU measurements are unreliable for detecting attacks on range measurements. In consequence, accumulating the faults within a time window is needed to detect the slowly drifting faults introduced by GNSS spoofing attacks [16], which may disable the in-time detection and mitigation of attacks. Instead, we use the differences between the range measurements and the range estimates based on the IMU measurements to detect the attacks, as the dead reckoning can maintain high accuracy for a short period and is less vulnerable to communication attacks. In particular,

$$\mathbb{1}_i^a(k) = \begin{cases} 1, \text{ if } \exists j \text{ s.t. } |\hat{y}_{i,j}(k) - y_{i,j}(k)| > \gamma \\ 0 \qquad\qquad\qquad \text{otherwise} \end{cases} \tag{9}$$

where $\mathbb{1}_i^a$ indicates whether the i-th node is attacked and γ is a predefined threshold and $\hat{y}_{i,j}(k)$ is the range estimates between Node i and Node j based on the IMU measurements. It is noted that there can be detection errors including false alarms and mis-detections.

Then, we combine range-based positioning and dead reckoning of IMU to enhance the resilience of the positioning system. In particular, we use the range-only positioning in the normal environment and IMU when attacks occur. To avoid the drifts of IMU-based positioning, the IMU is calibrated using the range-only positioning at a predefined frequency, when no attacks are detected. However, the IMU will not be calibrated once the attacks are detected, and dead reckoning will be used for positioning until the attack alarms cease. The difference between the range measurements and estimates will be monitored in real-time to detect attacks.

Furthermore, we consider two cases of reducing performance degradation when the attacks are detected. First, when the number of unattacked nodes based on the detection is greater than the number of nodes required for distributed EKF, the information from the attacked nodes will be discarded to prevent the adverse effects of incorrect measurements. The second case is when the number of unattacked nodes is less than the number of nodes required for DEKF, the attacked nodes use the IMU-based position estimates as their position estimates. Additionally, the procedures for attack detection and mitigation are summarized in Algorithm 1.

4 Experimental Results and Validation

4.1 Scenario Description

Table 1. Specifications of the UVA

Cruising Speed	Range	Endurance	Height	Field of View
30 km/h	10 km	1–1.5 h	0.15 km	31.5°–6.7°

Algorithm 1. Detecting and Mitigating Distance Manipulation Attacks

Input: S: number of follower nodes; $x(0)$: initial positions; x_{target}: target coordinates; ϵ: target radius; $\hat{P}_i(0)$, initial estimate of state covariance matrix; Q: process noise covariance matrix; R: measurement noise covariance matrix; $|\mathcal{N}_i|$: the number of neighboring nodes for Node i; N_{DEKF}: the number of neighboring nodes required for DEKF; T: maximum time step.
Output: $x_i(k), i = 1, \cdots, S, k = 0, \cdots, T$.

Initialization: $k = 0$, $\mathbb{1}_{\text{IMU}} = \text{False}$ ▷ $\mathbb{1}_{\text{IMU}} = \text{False}$ if calibrating IMU with the range-only positioning, and $\mathbb{1}_{\text{IMU}} = \text{True}$ otherwise.
while $\max_i \|x_i(k) - x_{\text{target}}\| > \epsilon$ and $k < T$ **do**
  Initialize $\mathcal{N}^a(k) = \varnothing$ at time instant k ▷ $\mathcal{N}^a(k)$: the set of attacked nodes.
  for $i \leftarrow 1$ to S **do**
    Compute and apply control input $u_i(k)$ based on $\hat{x}_i(k)$
    Obtain range and IMU measurements
    if $\mathbb{1}_{\text{IMU}}$ **then**
      Obtain IMU-based position estimates $\hat{x}_i^{\text{IMU}}(k)$ using $\hat{x}_i^{\text{IMU}}(k-1)$
    else
      Obtain IMU-based position estimates $\hat{x}_i^{\text{IMU}}(k)$ using $\hat{x}_i(k-1)$
    end if
    Obtaining IMU-based distance estimates based on $\hat{x}_i^{\text{IMU}}(k)$
    if $\mathbb{1}_i^a$ **then** ▷ Attack detection by Eq. (9).
      $\mathcal{N}_a(k) = \mathcal{N}_a(k) \cup \{i\}$
      $\mathbb{1}_{\text{IMU}} = \text{True}$
    else
      $\mathbb{1}_{\text{IMU}} = \text{False}$
    end if
  end for
  if $|\mathcal{N}^{\bar{a}}(k)| \geq N_{\text{DEKF}}$ **then** ▷ $|\mathcal{N}^{\bar{a}}(k)|$: the number of unattacked nodes.
    for $i \leftarrow 1$ to S **do**
      Estimate $\hat{x}_i(k)$ using the DEKF with $\mathcal{N}_i^{\bar{a}} \cap \mathcal{N}_i$
    end for
  else
    for $i \leftarrow 1$ to S **do**
      $\hat{x}_i(k) = \hat{x}_i^{\text{IMU}}(k)$
    end for
  end if
  $k \leftarrow k + 1$
end while

We assume each UAS to be a point UAS and that there are no kinematic restrictions on a UAS's movement, similar to [17]. The UAV specifications[1] are summarized in Table 1. The leader node stays at $x_0 = [0\ 0\ 0]^\top$(m). The initial positions of the follower nodes $x_i(0) = [x_{i,1}(0)\ x_{i,2}(0)\ x_{i,3}(0)]^\top + [0\ 0\ 150]^\top$ where $x_{i,j}(0)$ are randomly drawn from the normal distribution $\mathcal{N}(0, 0.1)$. The target is $x_{\text{target}} = [5000\ 5000\ 150]^\top$(m). There are S^2 range measurements, including

[1] We refer to Raven® B RQ-11 at https://www.avinc.com/images/uploads/product_docs/Raven_Datasheet_05_220825.pdf for the specifications.

the measurements between the leader node and follower nodes and between each two follower nodes. Each node adjusts the control inputs u_i by

$$u_i(k) = \frac{\hat{x}_i(k|k) - x_{\text{target}}}{\|\hat{x}_i(k|k) - x_{\text{target}}\|_2} \times 8 \text{ (m/s)}, \tag{10}$$

where $\hat{x}_i(k|k)$ is the position estimate at time k based on the measurements and $\|\cdot\|_2$ denotes the Euclidean norm. dt = 9 s. The covariance matrix R of the measurement noises is diagonal and $R = \text{diag}([\sigma_{1,0}, \cdots, \sigma_{S,S-1}])$ where $\sigma_{i,j}$ denotes the standard deviation of the noise for node i's range measurement w.r.t. node j. A follower node finishes the task if $\|x_i(k) - x_{\text{target}}\| \leq 16$ (m). The maximal time steps for the task is 100. Additionally, the process noise is not considered.

Moreover, spoofing can take place on the data during the flights. To thoroughly test the performance of the range-only cooperative positioning and anti-attack techniques under various types of attacks, we consider both (1) non-Gaussian attacks which add a fixed y_a to the measurements of the $|\mathcal{A}_V|$ attacked follower nodes with a probability p_a during the attack period from time step 21 to 30; and (2) Gaussian attacks which add i.i.d. Gaussian noise with $y_a \sim \mathcal{N}(0, \sigma_a)$ to the measurements of the $|\mathcal{A}_V|$ attacked follower nodes during the attack period. The non-Gaussian attacks are supposed to cause more performance degradation and bring more challenges for anti-attacks than the Gaussian attacks, as the EKF assumes Gaussian process and measurement noise. Furthermore, since we assume homogeneous follower UAV nodes, the attacked UAV nodes are randomly selected given a number of attacked nodes.

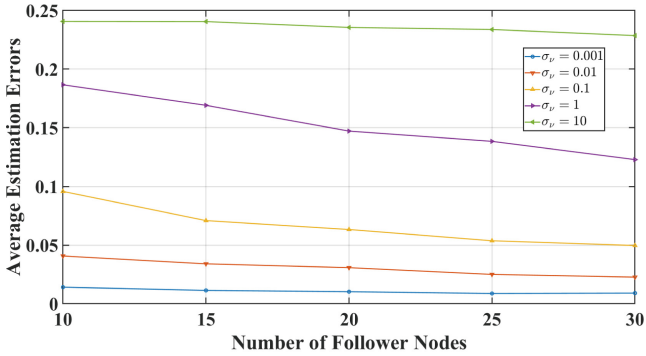
We use a measurement-level simulator which is sufficient for attack detection and impact moderation of spoofing. To evaluate the range-only positioning approach, we use the average estimation errors computed by

$$\bar{e} = \frac{1}{M}\sum_{l=1}^{M}\frac{1}{S}\sum_{i=1}^{S}\frac{1}{K}\sum_{k=1}^{K}\left\|\hat{x}_i^{(l)}(k|k) - x_i^{(l)}(k)\right\|_2, \tag{11}$$

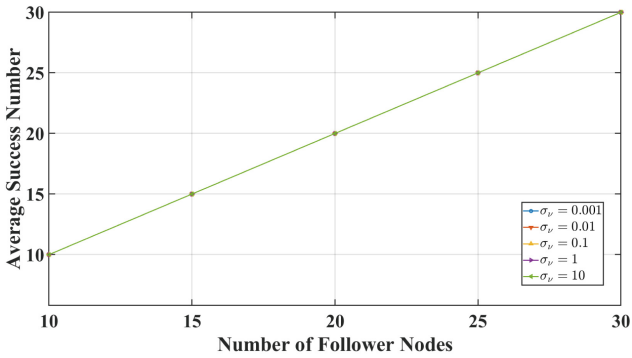
where M is the number of Monte Carlo (MC) simulations, and K is the number of time steps for the i-th node. Moreover, we evaluate the *success rate* which is defined as the ratio of the number of follower nodes that reach the target area over the total number of follower nodes in a simulation, and the average success rate is the average of the success rates of M MC simulations.

4.2 Performance of Centralized EKF

The Centralized EKF (CEKF) requires the follower nodes to send their range measurements to the leader node to estimate the positions of all the nodes. Then, the leader node sends the position estimates to the follower nodes. In the experiments, we assume the timing is synchronized for all the nodes and omit the processing and communicating time to focus on the positioning problem. First, we evaluate the performance of CEKF for different numbers of follower nodes and different σ_ν's.



(a) Average estimation errors of CEKF.



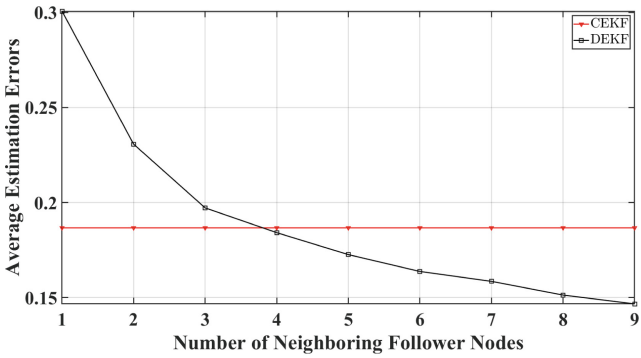
(b) Average success number of CEKF.

Fig. 2. The performance of CEKF for different numbers of follower nodes.

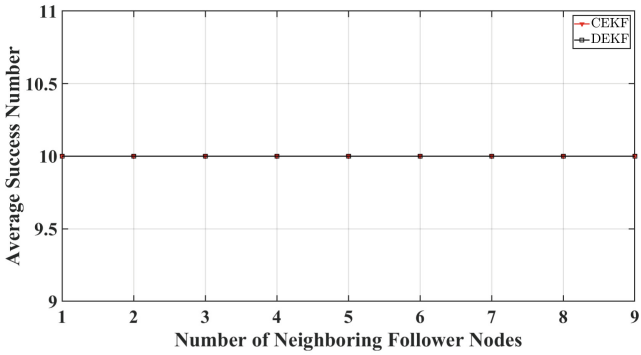
Results. Figure 2 shows the results of evaluating CEKF. The average estimation errors decrease as the number of follower nodes increases and increase as the standard deviation of the measurement noise increases. All the follower nodes fulfilled the tasks for different measurement noises when no attacks took place, which demonstrates the good performance of CEKF when its assumptions are satisfied.

4.3 Performance of Distributed EKF

The distributed EKF (DEKF) requires each follower node to estimate positions based on the consensus with the neighboring follower nodes. In particular, Node i needs to update and transmit $\hat{x}_i^l(k|k)$ and $z_i^l(k|k), l = 1, \cdots, L$ for consensus. We consider $S = 10$ for the following simulations. The parameters for consensus in (5) are determined as $L = 40$,$\mu = 0.1$. We assume all the follower nodes can maintain the range measurements w.r.t. the leader node. First, we evaluate the performance of the DEKF using different numbers of neighboring nodes.



(a) Average estimation errors of DEKF.



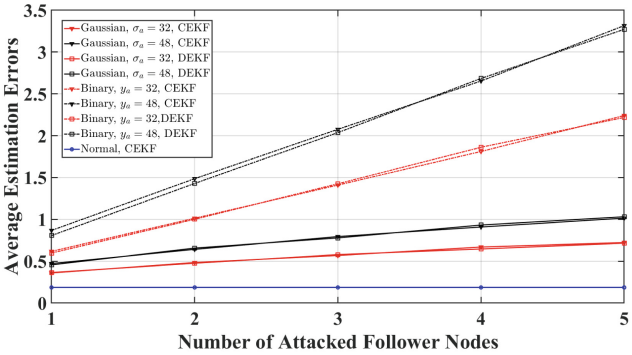
(b) Average success number of DEKF.

Fig. 3. The performance of DEKF for different numbers of neighboring nodes.

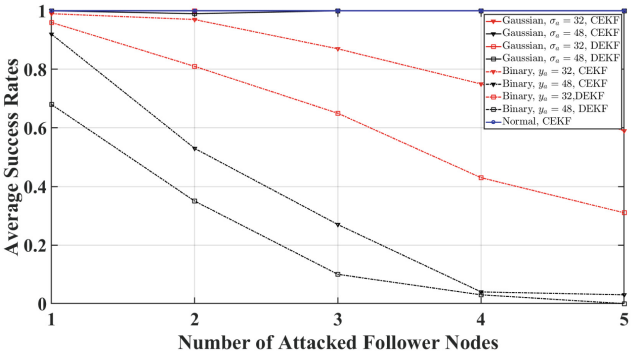
Results. Figure 3 shows the results of evaluating DEKF. The average estimation errors decrease as the number of neighboring follower nodes increases and are smaller than those of CEKF when the number of neighboring nodes is greater than 3. All the follower nodes fulfilled the tasks for different measurement noises when no attacks took place, which demonstrates that DEKF can achieve acceptable precision without using all the measurements as CEKF.

4.4 Resilience Against Attacks

In this subsection, we evaluate the performance of range-only positioning under attacks. First, we evaluate the performance degradation under different realizations of attacks and show the performance of dead reckoning using IMU. Then, we validate the proposed attack detection and mitigation approach. Additionally, the number of neighboring follower nodes for the experiments in this subsection was set to 4 which is sufficient for DEKF to achieve comparable precision with CEKF based on the results in Sect. 4.3 (Fig. 4).



(a) The comparison between the estimation errors of CEKF and DEKF for different $|\mathcal{A}_V|$.



(b) The comparison between the average success rates of CEKF and DEKF for different $|\mathcal{A}_V|$.

Fig. 4. The comparison between the performance of CEKF and DEKF under attacks.

Performance Under Attacks. As the number of attacked follower nodes increases, the average estimation errors increase. Non-Gaussian attacks cause more significant decreases in performance. The differences between the average estimation errors of CEKF and DEKF were not significant. However, CEKF achieved higher average success rates than DEKF without anti-attack techniques.

Performance of Dead Reckoning. Since the considered attacks only impact the range measurements, the IMU will not be affected but still suffer from the drifts by dead reckoning. For simulations, we assume that the velocity estimated from the IMU measurements suffers from an additive Gaussian noise with $\sigma_{\text{IMU}} = 0.1(m/s)$. The red line with downward-pointing triangle marks in Fig. 5 shows the average estimation errors over time using only IMU in one simulation. The average estimation errors at a time step are the average of the estimation

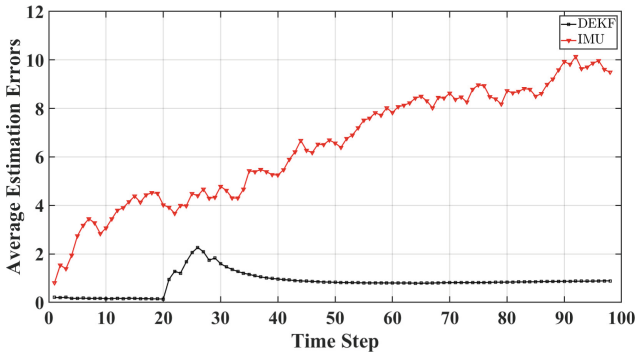
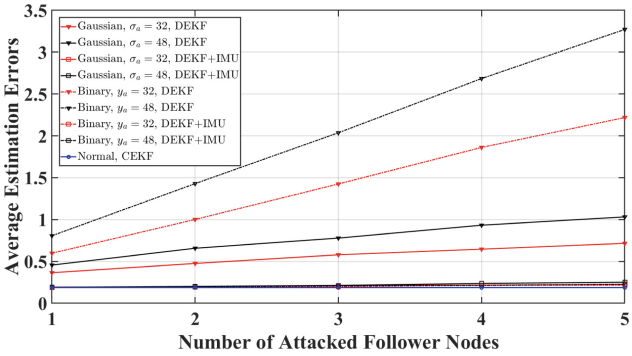


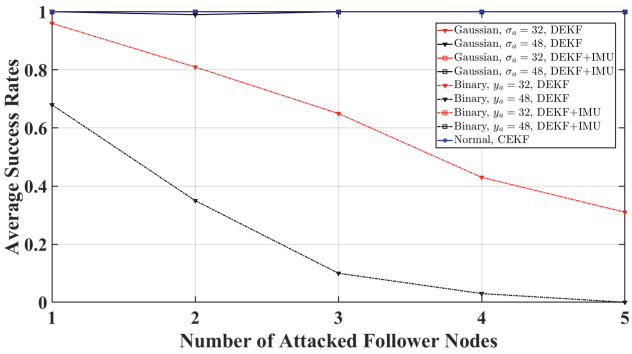
Fig. 5. The average estimation errors over time using only IMU for positioning.

errors of the 10 follower nodes at that time step. Additionally, the black line with the square marks shows the result of DEKF without using the anti-attack technique in one simulation under non-Gaussian attacks with $y_a = 48$ and $|\mathcal{A}_V| = 5$. 10 follower nodes finished the task using DEKF in that simulation.

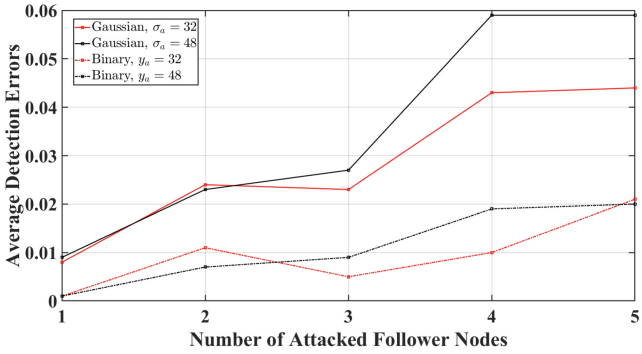
Performance of the Anti-attack Approach. Figure 6 shows the validation results of the anti-attack approach. We evaluated the detection errors of the proposed attack detection approach. The detection error is the number of false detections (including false positives and false negatives) in a simulation and the average detection errors are the average of the detection errors of M simulations. The average detection errors for Gaussian attacks were larger than those of non-Gaussian attacks. The proposed detection approach correctly detected the attacked nodes with a high probability (that is greater than 0.94 for all the attacks), selected the unattacked neighboring nodes for consensus-based DEKF, and achieved similar performance to the CEKF without attacks (black lines with square marks).



(a) The comparison between the estimation errors of DEKF without and with anti-attack for different $|\mathcal{A}_V|$.



(b) The comparison between the average success rates of DEKF without and with anti-attack for different $|\mathcal{A}_V|$.



(c) The detection errors for different $|\mathcal{A}_V|$, attack types, and attack strength.

Fig. 6. Validation results of the anti-attack approach.

5 Concluding Remarks

This paper presented a DEKF approach to detecting and mitigating distance manipulation attacks on range-only positioning of multiple smart UASs with IMU-based positioning. In particular, both Gaussian and non-Gaussian types of attacks were considered. The attacks were detected based on the differences between the IMU-based distance estimates and the range measurements and the UAS exchanged information with adjacent UASs that were free of attacks to enhance positioning precision. Experiments demonstrated that DEKF were more robust to attacks than CEKF and using the anti-attack approach based on DEKF and IMU further reduced the positioning errors and improved the probability of fulfilling tasks.

In future works, we will consider other types of distance manipulation attacks and enhance the attack detection and mitigation performance by statistical analysis and machine learning algorithms.

References

1. Anderson, B.D., Moore, J.B.: Optimal Filtering. Courier Corporation, Chelmsford (2012)
2. Bahr, A., Leonard, J.J., Martinoli, A.: Dynamic positioning of beacon vehicles for cooperative underwater navigation. In: 2012 IEEE/RSJ International Conference on Intelligent Robots and Systems, pp. 3760–3767. IEEE (2012)
3. Bao, Y., et al.: PID-based automatic gain control for satellite transponder under partial-time partial-band AWGN jamming. In: Sensors and Systems for Space Applications XVI, vol. 12546, pp. 61–68. SPIE (2023)
4. Battistelli, G., Chisci, L., Mugnai, G., Farina, A., Graziano, A.: Consensus-based linear and nonlinear filtering. IEEE Trans. Autom. Control **60**(5), 1410–1415 (2014)
5. Blasch, E., et al.: Cyber awareness trends in avionics. In: 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC), pp. 1–8. IEEE (2019)
6. Burchett, B.T.: Unscented Kalman filters for range-only cooperative localization of swarms of munitions in three-dimensional flight. Aerosp. Sci. Technol. **85**, 259–269 (2019)
7. Ceccato, M., Formaggio, F., Laurenti, N., Tomasin, S.: Generalized likelihood ratio test for GNSS spoofing detection in devices with IMU. IEEE Trans. Inf. Forensics Secur. **16**, 3496–3509 (2021)
8. Chen, N., Chen, Y., Blasch, E., Ling, H., You, Y., Ye, X.: Enabling smart urban surveillance at the edge. In: 2017 IEEE International Conference on Smart Cloud (SmartCloud), pp. 109–119. IEEE (2017)
9. Cheng, X.J., Xu, J.n., Cao, K.J., Wang, J.: An authenticity verification scheme based on hidden messages for current civilian GPS signals. In: 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology, pp. 345–352. IEEE (2009)
10. Dunik, J., Straka, O., Simandl, M., Blasch, E.: Random-point-based filters: analysis and comparison in target tracking. IEEE Trans. Aerosp. Electron. Syst. **51**(2), 1403–1421 (2015)

11. Flury, M., Poturalski, M., Papadimitratos, P., Hubaux, J.P., Le Boudec, J.Y.: Effectiveness of distance-decreasing attacks against impulse radio ranging. In: Proceedings of the Third ACM Conference on Wireless Network Security, pp. 117–128 (2010)
12. Gong, B., Wang, S., Hao, M., Guan, X., Li, S.: Range-based collaborative relative navigation for multiple unmanned aerial vehicles using consensus extended kalman filter. Aerosp. Sci. Technol. **112**, 106647 (2021)
13. Ioannides, R.T., Pany, T., Gibbons, G.: Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques. Proc. IEEE **104**(6), 1174–1194 (2016)
14. Kassas, Z.M., Closas, P., Gross, J.: Navigation systems panel report navigation systems for autonomous and semi-autonomous vehicles: current trends and future challenges. IEEE Aerosp. Electron. Syst. Mag. **34**(5) (2019)
15. Kassas, Z.M., Khalife, J., Abdallah, A.A., Lee, C.: I am not afraid of the Gps jammer: resilient navigation via signals of opportunity in GPS-denied environments. IEEE Aerosp. Electron. Syst. Mag. **37**(7), 4–19 (2022)
16. Liu, Y., Li, S., Fu, Q., Liu, Z., Zhou, Q.: Analysis of Kalman filter innovation-based GNSS spoofing detection method for INS/GNSS integrated navigation system. IEEE Sens. J. **19**(13), 5167–5178 (2019)
17. Papalia, A., Thumma, N., Leonard, J.: Prioritized planning for cooperative range-only localization in multi-robot networks. In: 2022 International Conference on Robotics and Automation (ICRA), pp. 10753–10759. IEEE (2022)
18. Poturalski, M., Flury, M., Papadimitratos, P., Hubaux, J.P., Le Boudec, J.Y.: The cicada attack: degradation and denial of service in IR ranging. In: 2010 IEEE International Conference on Ultra-Wideband, vol. 2, pp. 1–4. IEEE (2010)
19. Psiaki, M.L., Humphreys, T.E.: GNSS spoofing and detection. Proc. IEEE **104**(6), 1258–1270 (2016)
20. Sathaye, H., Strohmeier, M., Lenders, V., Ranganathan, A.: An experimental study of GPS spoofing and takeover attacks on UAVs. In: 31st USENIX Security Symposium (USENIX Security 22), pp. 3503–3520 (2022)
21. Shen, D., Chen, G., Cruz, J.B., Blasch, E.: A game theoretic data fusion aided path planning approach for cooperative UAV ISR. In: 2008 IEEE Aerospace Conference, pp. 1–9. IEEE (2008)
22. Singh, M.: Securing distance measurement against physical layer attacks. Ph.D. thesis, ETH Zurich (2021)
23. Wang, S., Dekorsy, A.: Distributed consensus-based extended Kalman filtering: a Bayesian perspective. In: 2019 27th European Signal Processing Conference (EUSIPCO), pp. 1–5. IEEE (2019)
24. Wen, H., Huang, P.Y.R., Dyer, J., Archinal, A., Fagan, J.: Countermeasures for GPS signal spoofing. In: Proceedings of the 18th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2005), pp. 1285–1290 (2005)
25. Wesson, K., Rothlisberger, M., Humphreys, T.: Practical cryptographic civil GPS signal authentication. NAVIGATION: J. Inst. Navig. **59**(3), 177–193 (2012)
26. Wesson, K.D., Rothlisberger, M.P., Humphreys, T.E.: A proposed navigation message authentication implementation for civil gps anti-spoofing. In: Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011), pp. 3129–3140 (2011)

27. Xu, R., Chen, Y., Blasch, E., Aved, A., Chen, G., Shen, D.: Hybrid blockchain-enabled secure microservices fabric for decentralized multi-domain avionics systems. In: Sensors and Systems for Space Applications XIII, vol. 11422, pp. 150–164. SPIE (2020)
28. Xu, R., Nikouei, S.Y., Chen, Y., Blasch, E., Aved, A.: Blendmas: a blockchain-enabled decentralized microservices architecture for smart public safety. In: 2019 IEEE International Conference on Blockchain (Blockchain), pp. 564–571. IEEE (2019)
29. Xu, R., Wei, S., Chen, Y., Chen, G., Pham, K.: Lightman: a lightweight microchained fabric for assurance-and resilience-oriented urban air mobility networks. Drones **6**(12), 421 (2022)
30. Yang, C., Kaplan, L., Blasch, E., Bakich, M.: Optimal placement of heterogeneous sensors for targets with Gaussian priors. IEEE Trans. Aerosp. Electron. Syst. **49**(3), 1637–1653 (2013)
31. Yang, H., Huang, R., Wang, X., Deng, J., Chen, R.: EBAA: an efficient broadcast authentication scheme for ads-b communication based on IBS-MR. Chin. J. Aeronaut. **27**(3), 688–696 (2014)