Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

An attack-resilient distributed extended Kalman consensus filtering algorithm with applications to multi-UAV tracking problems*

Yuru HU, Wangyan LI†‡, Lifeng WU, Zhensheng YU

College of Science, University of Shanghai for Science and Technology, Shanghai 200093, China

†E-mail: wangyan_li@usst.edu.cn

Received Sept. 14, 2023; Revision accepted Dec. 27, 2023; Crosschecked June 3, 2024; Published online Aug. 8, 2024

Abstract: This study investigates how the events of deception attacks are distributed during the fusion of multi-sensor nonlinear systems. First, a deception attack with limited energy (DALE) is introduced under the framework of distributed extended Kalman consensus filtering (DEKCF). Next, a hypothesis testing-based mechanism to detect the abnormal data generated by DALE, in the presence of the error term caused by the linearization of the nonlinear system, is established. Once the DALE is detected, a new rectification strategy can be triggered to recalibrate the abnormal data, restoring it to its normal state. Then, an attack-resilient DEKCF (AR-DEKCF) algorithm is proposed, and its fusion estimation errors are demonstrated to satisfy the mean square exponential boundedness performance, under appropriate conditions. Finally, the effectiveness of the AR-DEKCF algorithm is confirmed through simulations involving multi-unmanned aerial vehicle (multi-UAV) tracking problems.

Key words: Extended Kalman consensus filtering; Hypothesis testing; Rectification strategy; Multi-UAV tracking
https://doi.org/10.1631/FITEE.2300621 **CLC number:** TP391.4

1 Introduction

State estimation has become increasingly popular due to its wide range of applications in areas such as navigation (Gong and Sun, 2021) and target tracking (Liu D et al., 2020; Ju et al., 2022). Meanwhile, the development of wireless sensor networks (Ge et al., 2022) has spurred research in distributed state estimation (DSE) (Battistelli and Chisci, 2016; Han et al., 2022), attracting growing attention. Unlike centralized state estimation, DSE relies on communication solely between neighbor nodes within the sensor network and achieves consistent estimation by incorporating local information. This approach has several advantages, including wider coverage, reduced bandwidth requirements, improved scalability, and enhanced robustness (Li WY et al., 2020). Among various methods for obtaining system state estimation, the consensus-based distributed estimation algorithm is commonly used and has led to extensive research on the consensus problem (Chen B et al., 2016; Han et al., 2017; Ju et al., 2022; Ning et al., 2023). In recent years, there has been a significant surge in research on the distributed Kalman consensus filtering (DKCF) algorithm, which stands as a classical approach for achieving distributed consensus estimation. For example, Li WY et al. (2020) investigated the uniform error covariance bounds for three significant types of DKCF algorithms for linear time-varying systems at a finite fusion step in terms of a collectively uniformly detectable condition. In Ryu and Back (2022), the DKCF problem was

‡ Corresponding author
* Project supported by the National Natural Science Foundation of China (Nos. 62103283 and 12371308)
ORCID: Yuru HU, https://orcid.org/0009-0003-3797-4802; Wangyan LI, https://orcid.org/0000-0002-0068-1059

redefined as a consensus optimization challenge, and a novel DKCF algorithm was introduced with its stability demonstrated under reasonable assumptions. Recently, more and more researchers have been extending DKCF to the nonlinear system setting. For instance, Battistelli and Chisci (2016) demonstrated that distributed extended Kalman consensus filtering (DEKCF) can guarantee the local stability of all network nodes under conditions of network connectivity and collective observability. In addition, Ren et al. (2023) investigated the DEKCF algorithm with event-triggered (ET) communication and performed its stability analysis.

While the primary objective of sensor fusion is to enhance the accuracy and reliability of state estimation through data integration, the occurrence of malicious attacks, such as deception attacks (Yang W et al., 2019), denial-of-service attacks (Yang FS et al., 2021; Ge et al., 2023), and replay attacks (Chen B et al., 2018; Xie et al., 2022), often involves injecting false data into the sensor network to manipulate the fusion outcomes. This can lead to a deterioration in the estimation performance of the system, consequently undermining its stability. In particular, the deception attack with limited energy (DALE) has recently received research attention due to the fact that it can cleverly circumvent existing detectors with limited energy, thereby leading to additional detrimental effects. For example, for linear systems, Huang et al. (2020) analyzed the worst-case distribution estimates which result from the attacker, and obtained the optimal Kalman gain for each node that maximizes its estimation performance under DALE. Recently, Ren et al. (2023) further designed a unified distributed consensus estimation algorithm for nonlinear systems and established sufficient conditions for the boundedness of estimation error under DALE. Unfortunately, the above-mentioned studies focused only on how to detect DALE but not on how to rectify the impact caused by the false data generated from DALE. Therefore, how to design an integrated detection and rectification mechanism for a system under DALE is one of the motivations of this study.

When a DALE is detected, it is natural to introduce how to design appropriate rectification strategies to improve it, similar to the ET strategies (Wu et al., 2013; Shi et al., 2014; Battistelli et al., 2018; Liu QY et al., 2019; Wang R et al., 2021; Ju et al., 2022; Xiao SY et al., 2022; Chen SQ and Ho, 2023; Ge et al., 2024; Zhang XM et al., 2023). For instance, to preserve the desired performance while conserving limited computational resources and network bandwidth, an ET strategy was introduced by Rezaei and Ghorbani (2022). Recently, Chen SQ and Ho (2023) investigated two edge-based transmit–receive ET strategies for reducing data transmission frequency to decrease the energy consumption of nonlinear systems. However, the aforementioned studies all assumed an ideal environment, whereas, in reality, the systems are inevitably susceptible to attack events. To address this challenge, many researchers have begun to investigate methods for enhancing network security in distributed consensus filtering by employing ET strategies (Yang W et al., 2017; Zhang ZH et al., 2020; Ren et al., 2023). For example, Yang W et al. (2017) proposed a new ET-based distributed estimator by selectively transmitting information based on assessing whether the estimated value of each sensor is affected by DALE. Meanwhile, to address the DALE problem in nonlinear systems, a unified ET-based DEKCF algorithm has been designed by Ren et al. (2023) to improve the computational efficiency. Similar to the ET strategy, the rectification strategy for addressing attacks has garnered widespread attention among researchers; for example, Chong et al. (2015) established a novel state estimation algorithm that reconstructs the initial state using observability Gramian and a finite measurement window to rectify the adverse effects of adversarial attacks. Fawzi et al. (2014) considered the state-space representation of the system and used an l-norm optimization problem to reconstruct state values for attack rectification. Recently, a novel predictive correction (PC) adversarial attack has been proposed through the study of gradient-based attacks and numerical methods for solving ordinary differential equations (ODEs) (Wan and Huang, 2023). However, it should be noted that the exploration of ET strategies and the rectification strategies mentioned above is primarily focused on reducing energy transmission efficiency, paying limited attention to how to rectify the abnormal data that may arise from DALE.

Motivated by the above discussion, it is our intention to address the DALE problem in nonlinear systems by proposing an attack-resilient DEKCF (AR-DEKCF) algorithm. Its resilience is achieved

by an integrated DALE detection and rectification mechanism, where the detection of DALE is evaluated by a simple hypothesis testing method and the rectification is imposed on the state estimation attack by DALE.

This work follows the recent trend of research on DALE problems in nonlinear systems, such as Ren et al. (2023), but in a different manner: (1) following the detection of DALE, a simple detection mechanism based on hypothesis testing is proposed to evaluate the influence of DALE on the predicted state of local nodes; (2) a rectification strategy is proposed to rectify the contaminated state estimate caused by DALE, based on which an AR-DEKCF algorithm is designed; (3) an application to multi-unmanned aerial vehicle (multi-UAV) tracking problems is carried out to validate the effectiveness of the AR-DEKCF algorithm we proposed.

Notation description for this work is provided in Table 1.

Table 1 List of notations

Notation	Description
$\mathbb{R}^n$	n-dimensional Euclidean space
$\|\cdot\|$	Euclidean norm in $\mathbb{R}^n$
M^{T}	Transpose of matrix M
M^{-1}	Inverse of matrix M
$(M)^L$	L^{th} power of matrix M
$M>0$	M is positive definite
$M\geq 0$	M is positive semi-definite
$\mathrm{tr}\{M\}$	Trace of matrix M
$\lambda_{\max}(M)$	Largest eigenvalue of matrix M
$\mathrm{diag}\{\cdot\}$	A diagonal matrix
I_n	Identity matrix of dimension n
$\|\mathcal{N}\|$	Cardinality of set $\mathcal{N}$

2 Problem formulation

2.1 Nonlinear system model

In this work, we focus on the discrete-time nonlinear system described as follows:

$$x_k = f(x_{k-1}) + w_{k-1}, \tag{1}$$

where $x_k \in \mathbb{R}^n$ is the state, $f(x_{k-1})$ is the nonlinear process, and w_k is the zero-mean Gaussian white noise sequence with covariance Q_k.

The observation process is represented using an undirected graph $\mathcal{G}=(\mathcal{N},\mathcal{E})$, with the set of sensor nodes $\mathcal{N}=\{1,2,\cdots,N\}$ and their connections represented by $\mathcal{E}\subseteq\mathcal{N}\times\mathcal{N}$. For each node $i\in\mathcal{N}$, the measurement $y_k^i\in\mathbb{R}^m$ is given by

$$y_k^i = h^i(x_k) + v_k^i, \tag{2}$$

where $h^i(\cdot)$ is the nonlinear measurement function, and v_k^i is the zero-mean Gaussian white noise sequence with covariance R_k^i. w_k and v_k^i are mutually uncorrelated. Moreover, we assume that the nonlinear functions $f(\cdot)$ and $h^i(\cdot), i\in\mathcal{N}$, are twice continuously differentiable.

2.2 Distributed extended Kalman consensus filtering (DEKCF)

In this subsection, we intend to present a popular DEKCF algorithm for the nonlinear system (1)–(2). At first, for each node $i\in\mathcal{N}$, we have the following extended Kalman filtering (EKF) algorithm:

$$\hat{x}_{k|k-1}^i = f(\hat{x}_{k-1}^i), \tag{3}$$

$$P_{k|k-1}^i = F_{k-1}^i P_{k-1}^i (F_{k-1}^i)^{\mathrm{T}} + Q_{k-1}, \tag{4}$$

$$\begin{aligned} P_k^i &= (I_n - K_k^i H_k^i) P_{k|k-1}^i \\ &= \left[(P_{k|k-1}^i)^{-1} + (H_k^i)^{\mathrm{T}}(R_k^i)^{-1} H_k^i\right]^{-1}, \end{aligned} \tag{5}$$

$$\hat{x}_k^i = \hat{x}_{k|k-1}^i + K_k^i(y_k^i - h^i(\hat{x}_{k|k-1}^i)), \tag{6}$$

$$K_k^i = P_{k|k-1}^i (H_k^i)^{\mathrm{T}} \left[H_k^i P_{k|k-1}^i (H_k^i)^{\mathrm{T}} + R_k^i\right]^{-1}, \tag{7}$$

where $F_{k-1}^i = \frac{\mathrm{d}f}{\mathrm{d}x}\mid_{x=\hat{x}_{k-1}^i}$ and $H_k^i = \frac{\mathrm{d}h^i}{\mathrm{d}x}\mid_{x=\hat{x}_{k|k-1}^i}$. $\hat{x}_{k|k-1}^i$ and $\hat{x}_k^i$ are the one-step prediction of the state x_k and the updated estimate, respectively. $P_{k|k-1}^i$ and P_k^i are the error covariance matrices corresponding to $\hat{x}_{k|k-1}^i$ and $\hat{x}_k^i$, respectively.

Next, the consensus on the information mechanism is imposed on local EKFs to construct the DEKCF algorithm (Battistelli and Chisci, 2016; Wei et al., 2020). Specifically, given the fusion step ℓ, at each time step k, the information pair $(\Omega_{\ell,k}^i, q_{\ell,k}^i)$ with the initialization $\Omega_{0,k}^i = (P_k^i)^{-1}$ and $q_{0,k}^i = (P_k^i)^{-1}\hat{x}_k^i$ can be represented by

$$\Omega_{\ell,k}^i = \Omega_{\ell,k|k-1}^i + (H_k^i)^{\mathrm{T}}(R_k^i)^{-1} H_k^i, \tag{8}$$

$$q_{\ell,k}^i = q_{\ell,k|k-1}^i + (H_k^i)^{\mathrm{T}}(R_k^i)^{-1} z_k^i, \tag{9}$$

where $z_k^i = y_k^i - h^i(\hat{x}_{k|k-1}^i) + H_k^i \hat{x}_{k|k-1}^i$.

Then, for $\ell = 0,1,\cdots,L-1$, where L is the number of fusion steps, we apply a covariance intersection fusion rule (Julier and Uhlmann, 1997) to

Eqs. (8) and (9) arriving at

$$\Omega^i_{\ell+1,k} = \sum_{j\in\mathcal{N}^i} \pi^{i,j}_{\ell,k}\Omega^j_{\ell,k}, \tag{10}$$

$$q^i_{\ell+1,k} = \sum_{j\in\mathcal{N}^i} \pi^{i,j}_{\ell,k} q^j_{\ell,k}, \tag{11}$$

where $\pi^{i,j}_{\ell,k}$ is the fused weight satisfying $\sum_{j\in\mathcal{N}^i}\pi^{i,j}_{\ell,k}=1$. At this stage, the main structure of DEKCF is introduced in terms of Eqs. (3)–(11).

It should be noted that for each node i, the prediction $\hat{x}^i_{k|k-1}$ in Eq. (3) is carried out in an ideal environment. However, malicious attacks often occur during the prediction process (3), which significantly degrades the filtering performance.

2.3 Deception attack with limited energy (DALE)

In this study, we consider a common attack strategy, i.e., DALE, which has been insensitively studied by Huang et al. (2020) and Ren et al. (2023). DALE means that attackers can damage the normal function of the sensor network by propagating false data during the prediction phase of the local nodes having limited energy, which results in a decline in its performance. Its model is given by (Ren et al., 2023):

$$\begin{aligned}\hat{x}^{i,\mathrm{d}}_{k|k-1} = {}& \gamma^i_k\left[x_k + \mathcal{B}^i_k\left(\hat{x}^i_{k|k-1}-x_k\right)+\theta^i_k\right]\\ &+(1-\gamma^i_k)\hat{x}^i_{k|k-1},\end{aligned} \tag{12}$$

where $\hat{x}^{i,\mathrm{d}}_{k|k-1}$ is the local state estimate under the DALE for node i. The matrix $\mathcal{B}^i_k$, which is introduced for designing attack strategies, is an arbitrary matrix. The attack vector θ^i_k is characterized as an independent and identically distributed Gaussian random variable, and its covariance is Θ^i_k. Meanwhile, for $i\in\mathcal{N}$, γ^i_k is a random variable characterizing the occurrence of DALE, and the random variables γ^i_k and γ^j_k $(i\neq j)$ are mutually uncorrelated, which obey the following Bernoulli distribution:

$$\mathrm{Prob}\{\gamma^i_k=1\}=p^i, \tag{13}$$

$$\mathrm{Prob}\{\gamma^i_k=0\}=1-p^i, \tag{14}$$

where $p^i\in[0,\ 1]$. When $\gamma^i_k=1$, it means that the system is experiencing DALE.

When the estimation is subjected to DALE, local node i is likely to unavoidably decrease the precision of its estimate while updating, simultaneously impacting the fusion performance. Consequently, it is necessary to devise an effective detection mechanism to promptly identify the injected anomalous data from the attack events.

To deal with this issue, in the following subsection, we will introduce a hypothesis testing method to detect DALE.

2.4 Hypothesis testing-based DALE detection mechanism

Inspiration is drawn by the idea of Huang et al. (2020), who proposed a DALE-based detection mechanism for linear systems using the differences between measurement values and the predicted ones. In this work, we extend this approach to the nonlinear setting and take into account the linearization error. Differently, we choose a hypothesis testing method to detect DALE.

For each node i, denote $\tilde{x}^i_{k|k-1}=x_k-\hat{x}^i_{k|k-1}$ and $\tilde{x}^i_{k-1}=x_{k-1}-\hat{x}^i_{k-1}$ as the prediction error and the estimation error, respectively. The nonlinear functions $f(\cdot)$ and $h^i(\cdot)$ can be expanded as

$$f(x_{k-1})-f\left(\hat{x}^i_{k-1}\right)=F^i_{k-1}\tilde{x}^i_{k-1}+o(|\tilde{x}^i_{k-1}|), \tag{15}$$

$$h^i(x_k)-h^i(\hat{x}^i_{k|k-1})=H^i_k\tilde{x}^i_{k|k-1}+o(|\tilde{x}^i_{k|k-1}|), \tag{16}$$

where the terms $o(|\tilde{x}^i_{k-1}|)=\mathcal{L}^i_{k-1}\mathcal{U}^i_{k-1}\mathcal{T}_{1,k-1}\tilde{x}^i_{k-1}$ and $o(|\tilde{x}^i_{k|k-1}|)=\mathcal{S}^i_k\mathcal{R}^i_k\mathcal{T}^i_{2,k}\tilde{x}^i_{k|k-1}$ represent the high-order terms in the Taylor series expansion. Here, the scaling matrices $\mathcal{L}^i_{k-1}$ and $\mathcal{S}^i_k$ are dependent on the problem setting, and $\mathcal{T}_{1,k-1}$ and $\mathcal{T}^i_{2,k}$ are known tuning matrices. The unknown time-varying matrices $\mathcal{U}^i_{k-1}$ and $\mathcal{R}^i_k$ satisfying $\mathcal{U}^i_{k-1}(\mathcal{U}^i_{k-1})^{\mathrm{T}}\leq I$ and $\mathcal{R}^i_k(\mathcal{R}^i_k)^{\mathrm{T}}\leq I$ are introduced to neutralize the linearization errors (Kai et al., 2010).

Next, taking into account the state estimate under DALE in the form of Eq. (12), we can now rewrite Eq. (16) as follows:

$$\begin{aligned}\tilde{h}^{i,\mathrm{d}}_k &= h^i(x_k)-h^i(\hat{x}^{i,\mathrm{d}}_{k|k-1})+v^i_k\\ &=(H^i_k+\mathcal{S}^i_k\mathcal{R}^i_k\mathcal{T}^i_{2,k})\tilde{x}^{i,\mathrm{d}}_{k|k-1}+v^i_k.\end{aligned} \tag{17}$$

In the following paragraphs, we intend to detect the DALE in terms of $\tilde{h}^{i,\mathrm{d}}_k$ in Eq. (17) using hypothesis testing. To this end, we set up two hypotheses: the null hypothesis H_0 and the alternative hypothesis H_1, which can be described by

$$\begin{cases}H_0: \text{the system is operating normally;}\\ H_1: \text{the estimate } \hat{x}^i_{k|k-1} \text{ is under attacks.}\end{cases} \tag{18}$$

By virtue of Eq. (18), inspired by Huang et al. (2020), we propose a hypothesis testing-based DALE detection mechanism for each node i using the information of measurement estimation error (17) in the following form:

$$\xi_k^{i,\mathrm{d}} \triangleq (\tilde{h}_k^{i,\mathrm{d}})^{\mathrm{T}} \Sigma_h^{-1} \tilde{h}_k^{i,\mathrm{d}} \underset{H_1}{\overset{H_0}{\lessgtr}} \underline{\tau}^i, \tag{19}$$

where $\Sigma_h = \sigma^i || H_k^i P_{k|k-1}^{i,\mathrm{d}} (H_k^i)^{\mathrm{T}} + R_k^i ||$, σ^i is a positive constant, and $\underline{\tau}^i$ is a preset alarm threshold.

The two decisions based on Eq. (19) are then compared to finally decide H_0 and H_1, such that

$$\begin{cases} \text{decide } H_0 \text{ if } \xi_k^{i,\mathrm{d}} \le \underline{\tau}^i, \\ \text{decide } H_1 \text{ if } \xi_k^{i,\mathrm{d}} > \underline{\tau}^i. \end{cases} \tag{20}$$

From Eq. (20), if $\xi_k^{i,\mathrm{d}} > \underline{\tau}^i$, we will reject the null hypothesis H_0 and accept the alternative hypothesis H_1. This indicates that the data from the DALE are unneglectable. Otherwise, we conclude that the system is free of DALEs. However, even if the system is under DALEs, we still hope that the system can keep the normal operation state, i.e., $\xi_k^{i,\mathrm{d}} \le \underline{\tau}^i$. Therefore, we need to design a state estimation rectification strategy to drive the contaminating data $\hat{x}_{k|k-1}^{i,\mathrm{d}}$ until $\xi_k^{i,\mathrm{d}} \le \underline{\tau}^i$ is satisfied. To illustrate this idea, a flowchart of our work is given in Fig. 1.

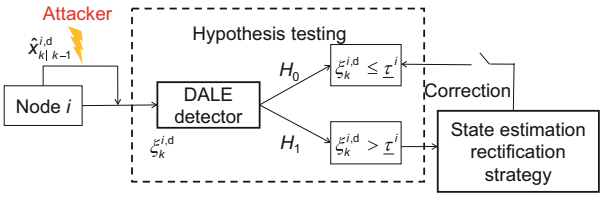

Fig. 1 Flowchart for correcting anomalous data under DALE

Remark 1 Different from the single hypothesis testing, the multiple hypothesis testing (MHT) normally involves the examining of multiple correlated variables of interest. For example, in D'Afflisio et al. (2021), the kinematic abnormalities can become apparent by comparing multiple velocity variables (e.g., spoofed velocity and actual velocity) using MHT. However, when addressing the attacks-detecting problems involving the single decision variable alone, the single hypothesis testing method is usually an efficient choice (Li YZ et al., 2018). In this work, as shown in Eq. (17), DALE detection is carried out in terms of the innovation variable $\tilde{h}_k^{i,\mathrm{d}}$ alone. Therefore, it is natural to adopt a detection mechanism using the single hypothesis testing to decide whether the system is operating normally (i.e., H_0) or is under attacks (i.e., H_1).

2.5 State estimation rectification strategy

For each node i, we can use a hypothesis testing-based DALE detection mechanism to identify the anomalous data resulting in DALE. It is evident that when DALE occurs, the predictive information pair of the local nodes $(\Omega_{k|k-1}^i, q_{k|k-1}^i)$ is susceptible to corruption by Eq. (12) and transformed into information for $(\Omega_{k|k-1}^{i,\mathrm{d}}, q_{k|k-1}^{i,\mathrm{d}})$. Subsequently, it is necessary to rectify the detected anomalous data, making it consistent to the original hypothesis H_0. Despite the fact that the anomalous data generated by a local node under DALE may not immediately affect the state estimation of the system, the accumulation of such data over time can compromise the system performance. In the following, we will design a state estimation rectification strategy to restore the performance of the system.

To this end, the latest time instant δ_k^i of node i is defined as the time elapsed since its most recent transmission. Therefore, the latest recently transmitted data are $(\Omega_{\delta_k^i}^i, q_{\delta_k^i}^i)$. We choose the binary variable ω^i to describe the data rectification procedure under the occurrence of Eq. (18) with

$$\omega^i = \begin{cases} 0, & \delta_k^i = \delta_{k-1}^i,\ \xi_k^{i,\mathrm{d}} > \underline{\tau}^i, \\ 1, & \delta_k^i = k,\ \xi_k^{i,\mathrm{d}} \le \underline{\tau}^i. \end{cases} \tag{21}$$

Embedding Eq. (20) into Eq. (21), we can design the following state estimation rectification strategy:

$$\begin{aligned} \Omega_{\delta_k^i}^i = {} & Q_{k-1}^{-1} - Q_{k-1}^{-1} F_{k-1}^i \Big(\breve{\Omega}_{k-1}^i + (F_{k-1}^i)^{\mathrm{T}} \\ & \cdot Q_{k-1}^{-1} F_{k-1}^i \Big)^{-1} (F_{k-1}^i)^{\mathrm{T}} Q_{k-1}^{-1}, \end{aligned} \tag{22}$$

$$q_{\delta_k^i}^i = \Omega_{\delta_k^i}^i f\left((\breve{\Omega}_{k-1}^i)^{-1} \breve{q}_{k-1}^i \right), \tag{23}$$

where $\breve{\Omega}_{k-1}^i = \omega^i \Omega_{k-1}^i + (1-\omega^i)\Omega_{\delta_{k-1}^i}^i$ and $\breve{q}_{k-1}^i = \omega^i q_{k-1}^i + (1-\omega^i) q_{\delta_{k-1}^i}^i$.

Obviously, if $\xi_k^{i,\mathrm{d}} \le \underline{\tau}^i$, the information pair (Ω_k^i, q_k^i) can be transmitted with $\omega^i = 1$. Otherwise, we will correct the information pair $(\Omega_{k|k-1}^{i,\mathrm{d}}, q_{k|k-1}^{i,\mathrm{d}})$ to $(\Omega_{\delta_{k-1}^i}^i, q_{\delta_{k-1}^i}^i)$ with $\omega^i = 0$.

The main idea of the state estimation rectification strategy (21)–(23) is that when $\omega^i = 0$ for

each node i, the information pair $(\Omega^{i,\mathrm{d}}_{k|k-1}, q^{i,\mathrm{d}}_{k|k-1})$ is not available at this time. However, node i can still access the previous information pair $(\Omega^{i}_{\delta^i_{k-1}}, q^{i}_{\delta^i_{k-1}})$, infer that such information can be close to the real information pair $(\Omega^i_{k-1}, q^i_{k-1})$, and finally update and replace $(\Omega^{i,\mathrm{d}}_{k|k-1}, q^{i,\mathrm{d}}_{k|k-1})$ in the process of information fusion.

Under the state estimation rectification strategy with the DALE for $i \in \mathcal{N}$, given the fusion step ℓ, the fusion information pair $(\Omega^i_{\ell+1,k}, q^i_{\ell+1,k})$ can be obtained by

$$\Omega^i_{\ell+1,k} = \sum_{j\in\mathcal{N}^i} \pi^{i,j}_{\ell,k}\left[\omega^j\Omega^j_{\ell,k} + (1-\omega^j)\Omega^j_{\ell,\delta^j_k}\right], \quad (24)$$

$$q^i_{\ell+1,k} = \sum_{j\in\mathcal{N}^i} \pi^{i,j}_{\ell,k}\left[\omega^j q^j_{\ell,k} + (1-\omega^j) q^j_{\ell,\delta^j_k}\right], \quad (25)$$

where $\pi^{i,j}_{\ell,k}$ can be calculated according to the Metropolis weight rule (Xiao L et al., 2005).

By exploiting the DEKCF defined in Eqs. (3)–(11), a hypothesis testing-based DALE detection mechanism, and a state estimation rectification strategy, we are ready to introduce an AR-DEKCF algorithm in Algorithm 1.

Algorithm 1 AR-DEKCF

1: **Input:** $\hat{x}^j_{k-1}$, P^j_{k-1}, F^j_{k-1}, Q_{k-1}, $\underline{\tau}^i$, L
2: **Prediction:** calculate the information pair $(\Omega^j_{k|k-1}, q^j_{k|k-1})$ via Eqs. (3) and (4)
3: **Rectification:** for $\ell = 0, 1, \cdots, L-1$, $j \in \mathcal{N}^i$, consider that the attack events occur
4: **if** $\xi^{i,\mathrm{d}}_k > \underline{\tau}^i$ **then**
(1) trigger $\omega^j = 0$
(2) correct the information pair $(\Omega^{j,\mathrm{d}}_{\ell,k|k-1}, q^{j,\mathrm{d}}_{\ell,k|k-1})$ by Eqs. (22) and (23)
(3) update the information pair $(\Omega^j_{\ell,\delta^j_k}, q^j_{\ell,\delta^j_k})$
else
(1) trigger $\omega^j = 1$
(2) compute the information pair $(\Omega^j_{\ell,k|k-1}, q^j_{\ell,k|k-1})$ by Eqs. (3) and (4)
(3) update the information pair $(\Omega^j_{\ell,k}, q^j_{\ell,k})$
5: **Fusion:** set $L = \ell + 1$, update $P^i_k = (\Omega^i_{L,k})^{-1}$, $\hat{x}^i_k = P^i_k q^i_{L,k}$ by Eq. (24)
6: **Update:** set $k = k + 1$, and repeat lines 3–5
7: **Output:** P^i_k, $\hat{x}^i_k$

3 Stability analysis

This section focuses on assessing the stability performance of Algorithm 1 in terms of the boundedness of the estimation errors. To begin with, we present the following assumptions:

Assumption 1 (Li WY et al., 2020) System (1)–(2) is said to be uniformly collectively observable if (F_k, H_k) is uniformly observable, where $F_k \triangleq \mathrm{col}(F^i_k)_{i\in\mathcal{N}}$ and $H_k \triangleq \mathrm{col}(H^i_k)_{i\in\mathcal{N}}$.

Assumption 2 For $i \in \mathcal{N}$, $k \geq 0$, there are positive reals $\underline{f}, \overline{f}, \overline{h}, \bar{\beta}, \underline{r}, \overline{r}, \underline{q}, \overline{q}$, such that the following bound conditions hold:

$$\begin{aligned} &\underline{f} \leq \|F^i_k\| \leq \overline{f},\ \|H^i_k\| \leq \overline{h},\ \|\Theta^i_k\| \leq \bar{\beta}, \\ &\underline{r} I_m \leq R^i_k \leq \overline{r} I_m,\ \underline{q} I_n \leq Q_k \leq \overline{q} I_n. \end{aligned} \quad (26)$$

Assumption 3 For $i \in \mathcal{N}$ and $k > 0$, the error covariance P^i_k satisfies $(P^i_k)^{-1} \leq (\mathcal{T}^i_{1,k-1})^{\mathrm{T}}\mathcal{T}^i_{1,k-1} \leq 2(P^i_k)^{-1}$.

Assumption 4 Consider that the system given by Eqs. (1) and (2) satisfies Assumptions 1 and 2. There exist positive scalars $\underline{p}$, $\overline{p}$, such that $\forall k \geq 0$, the error covariances of Algorithm 1 are uniformly bounded:

$$\underline{p} I_n \leq P^i_k \leq \overline{p} I_n. \quad (27)$$

With the above assumptions, it is possible to show the main result of this work.

Theorem 1 For every $k \geq 0$, $\forall i \in \mathcal{N}$, let Assumptions 1–4 hold. Consider the system (1)–(2) under DALE and Algorithm 1, the estimation errors $\tilde{x}^i_{k+1} = x_{k+1} - \hat{x}^i_{k+1}$ are exponentially bounded in mean square.

Proof See the appendix.

Remark 2 It is worth noting that Assumptions 3 and 4 provided in this work are reasonable. Assumption 3 holds because the tuning matrices $\mathcal{T}^i_{1,k-1}$ and $\mathcal{T}^i_{2,k}$ are known and can be preset (Ren et al., 2023). As for Assumption 4, its uniform lower bound can be guaranteed with the aid of Assumption 2, while the uniform upper bound can be obtained through Assumptions 1 and 2. Both uniform bounds for the linear system have been extensively researched in our prior works (Li WY et al., 2018, 2020; Wei et al., 2020).

4 An illustration example

In this section, a multi-UAV cooperative tracking problem using range-bearing sensors in a two-dimensional scenario (Arasaratnam and Haykin, 2009) will be studied to verify our proposed algorithm.

The target motion model is described by the following state-space system:

$$x_{k+1} = f(x_k) + w_k, \tag{28}$$

where $x_k = [p_{x_k}, v_{x_k}, p_{y_k}, v_{y_k}, \vartheta_k]^{\mathrm{T}}$ denotes the state of the target, p_{x_k} and p_{y_k} are the positions, v_{x_k} and v_{y_k} are the velocities of the target in the x and y directions respectively, and ϑ_k is a constant but unknown turning rate.

Meanwhile, the covariance of process noise w_k is $Q = \mathrm{diag}\{g_1\Delta, g_1\Delta, g_2\Delta\}$ with

$$\Delta = \begin{bmatrix} \Gamma^3/3 & \Gamma^2/2 \\ \Gamma^2/2 & \Gamma \end{bmatrix}, \tag{29}$$

where Γ is the sampling interval, and g_1 and g_2 are the noise intensities of the process.

The target position is measured using range-bearing sensors mounted on the multiple UAVs with the model:

$$z_k^i = \begin{bmatrix} \tan^{-1}\left(\dfrac{p_{y_k} - s_{y_k}^i}{p_{x_k} - s_{x_k}^i}\right) \\ \sqrt{\left(p_{x_k} - s_{x_k}^i\right)^2 + \left(p_{y_k} - s_{y_k}^i\right)^2} \end{bmatrix} + \begin{bmatrix} v_\theta^i \\ v_s^i \end{bmatrix}, \quad i = 1, 2, \cdots, 5, \tag{30}$$

where $(s_{x_k}^i, s_{y_k}^i)$ represents the position of the range-bearing sensor i in x and y directions, and v_θ^i and v_s^i are the measurement noises.

The values of the above-mentioned parameters are given in Table 2.

To validate the effectiveness of the AR-DEKCF algorithm, we selected five UAVs with range-bearing sensors to cooperatively track the target. As shown in Fig. 2, we assume that the DALEs persistently affect the data transmitted between UAV 2 and UAV 3, as well as between UAV 4 and UAV 5.

Furthermore, we evaluate the performance of tracking by using the position root mean square error ($\mathrm{RMSE_P}$), velocity RMSE ($\mathrm{RMSE_V}$), and turning rate RMSE ($\mathrm{RMSE_{TR}}$) of the targets from the i^{th} UAV for each time step k. All simulation results are derived over 300 independent Monte Carlo runs with the same condition, which can be defined as (Wang S et al., 2023)

$$\mathrm{RMSE}_Z = \sqrt{\frac{1}{N}\sum_{j=1}^{N}\psi_Z}, \quad Z = \mathrm{P}, \mathrm{V}, \mathrm{TR}, \tag{31}$$

Table 2 List of parameters

Parameter	Value
Γ	1 s
g_1	$0.1\ \mathrm{m^2/s^3}$
g_2	$1.75 \times 10^{-4}\ \mathrm{s^{-3}}$
v_θ^i	$\sqrt{10}$ m · rad
v_s^i	10 m
ϑ_k	-3 (°)/s

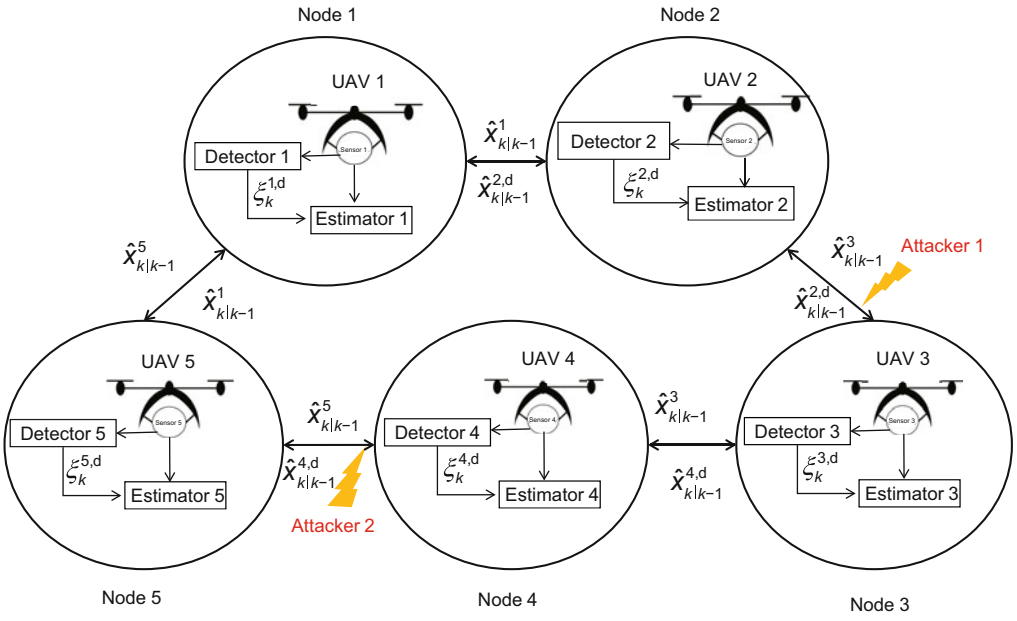

Fig. 2 UAV topology under DALE

where

$$\psi_{\mathrm{P}}=\left(p_{x_k}^j-\hat{p}_{x_{k,\mathrm{f}}}^{i,j}\right)^2+\left(p_{y_k}^j-\hat{p}_{y_{k,\mathrm{f}}}^{i,j}\right)^2,$$
$$\psi_{\mathrm{V}}=\left(v_{x_k}^j-\hat{v}_{x_{k,\mathrm{f}}}^{i,j}\right)^2+\left(v_{y_k}^j-\hat{v}_{y_{k,\mathrm{f}}}^{i,j}\right)^2,$$
$$\psi_{\mathrm{TR}}=\left(\vartheta_k^j-\hat{\vartheta}_{k,\mathrm{f}}^{i,j}\right)^2.$$

Here, N is the number of Monte Carlo runs, $[\hat{p}_{x_{k,\mathrm{f}}}^{i,j},\hat{p}_{y_{k,\mathrm{f}}}^{i,j}]$, $[\hat{v}_{x_{k,\mathrm{f}}}^{i,j},\hat{v}_{y_{k,\mathrm{f}}}^{i,j}]$, and $\hat{\vartheta}_{k,\mathrm{f}}^{i,j}$ are the fused estimates of the position, velocity, and turning rate of the i^{th} UAV, respectively. The initial state and the initial error covariance of the target trajectory are $x_0=[1000\ \mathrm{m},200\ \mathrm{m/s},1000\ \mathrm{m},0\ \mathrm{m/s},-3\ \mathrm{rad/s}]^{\mathrm{T}}$ and $P_0=\mathrm{diag}\{100\ \mathrm{m}^2,15\ \mathrm{m}^2/\mathrm{s}^2,100\ \mathrm{m}^2,15\ \mathrm{m}^2/\mathrm{s}^2,100\ \mathrm{rad}^2/\mathrm{s}^2\}$, respectively.

Next, we provide detailed discussion of the following two cases:

1. Case 1

In this case, the target trajectory follows a constant velocity motion, where

$$f(x_k)=F_k^i x_k=\begin{bmatrix}1&\Gamma&0&0&0\\0&1&0&0&0\\0&0&1&\Gamma&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}x_k.$$

The corresponding attack signals of attacker 1 and attacker 2 are respectively given by

$$\Theta_k^2=\begin{cases}0.015, & 20\le k\le 30,\\ 0, & \text{otherwise},\end{cases}$$
$$\Theta_k^4=\begin{cases}0.018, & 60\le k\le 70,\\ 0, & \text{otherwise}.\end{cases}\tag{32}$$

Then, we assess the performance of the AR-DEKCF algorithm in terms of $\mathrm{RMSE_P}$ and $\mathrm{RMSE_V}$ of UAVs. As depicted in Figs. 3 and 4, UAV 2 and UAV 4 experience a significant increase in their respective $\mathrm{RMSE_P}$ and $\mathrm{RMSE_V}$ when subjected to DALE in Eq. (32). Given the distributed fusion nature, their neighboring UAV 3 and UAV 5 also exhibit increased $\mathrm{RMSE_P}$ and $\mathrm{RMSE_V}$ during this period.

Fortunately, our proposed algorithm can rectify the abnormal $\mathrm{RMSE_P}$ and $\mathrm{RMSE_V}$ to the normal status and then they remain stable. Moreover, Fig. 5 depicts the time intensity of state estimation corrections for five UAVs. Notably, it reveals that the state estimation rectification strategy is triggered during the attack period to mitigate the transmission of abnormal data resulting from the DALE, aiming to rectify the impact on the fusion estimation.

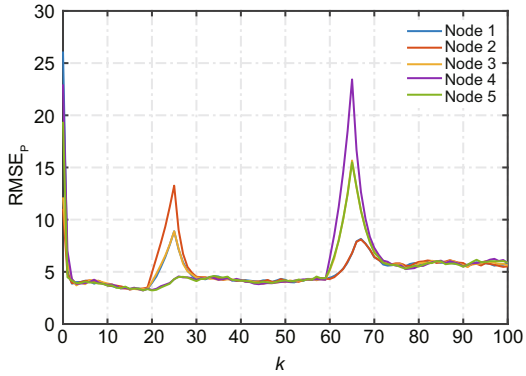

Fig. 3 $\mathrm{RMSE_P}$ of the AR-DEKCF algorithm for $L=4$

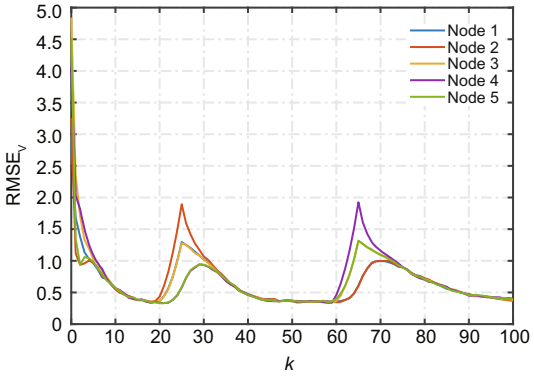

Fig. 4 $\mathrm{RMSE_V}$ of the AR-DEKCF algorithm for $L=4$

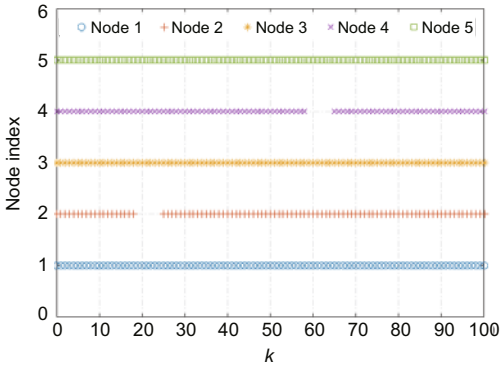

Fig. 5 State estimation rectification time under DALE

2. Case 2

In this case, the initial position of the target is situated within 20 m by 1500 m area, and is assumed to follow a trajectory with a constant but unknown turning rate, as shown in Fig. 6.

For every $k>0$, consider the linearized system

as follows:

$$f(x_k)\approx\frac{\partial f(x_k)}{\partial x_k}x_k = \begin{bmatrix} 1 & \frac{\sin(\vartheta_k\Gamma)}{\vartheta_k} & 0 & -\left(\frac{1-\cos(\vartheta_k\Gamma)}{\vartheta_k}\right) & 0 \\ 0 & \cos(\vartheta_k\Gamma) & 0 & -\sin(\vartheta_k\Gamma) & 0 \\ 0 & \frac{1-\cos(\vartheta_k\Gamma)}{\vartheta_k} & 1 & \frac{\sin(\vartheta_k\Gamma)}{\vartheta_k} & 0 \\ 0 & \sin(\vartheta_k\Gamma) & 0 & \cos(\vartheta_k\Gamma) & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} x_k,$$

where ϑ_k is the constant angular speed under the DALE signal $\Theta_k^2=0.02$ with the probability $p^i=0.1$ for attacker 1.

In particular, five UAVs follow and steadily approach the target, aiming to achieve a higher tracking accuracy. To investigate the performance of UAV 2 when subjected to DALE, we compare our algorithm with the distributed EKCF algorithm without/with DALE (A-DEKCF) of UAV 2. The A-DEKCF algorithm experiences a sudden increase in the corresponding RMSE_Z ($Z=\mathrm{P},\mathrm{V},\mathrm{TR}$) when under DALE, whereas our proposed algorithm can significantly reduce the relative RMSE_Z. Furthermore, owing to the incessant accumulation of rectification errors, RMSE_Z of our proposed algorithm has not reached but is close to the performance of the DEKCF algorithm. It can gradually regain stability in the absence of DALE with increasing k, as shown in Figs. 7–9.

5 Conclusions

In this study, the issue of DALE encountered in distributed multi-sensor fusion state estimation has been addressed, considering it in two crucial steps: DALE detection and rectification. First, we proposed a hypothesis testing-based mechanism for detecting DALE to identify anomalous data generated by it. Second, to effectively mitigate the adverse effects of DALE on local node prediction values, we have developed a state estimation rectification strategy to correct abnormal data caused by DALE. Finally, we have introduced an AR-DEKCF algorithm and validated its effectiveness through simulations of multi-UAV cooperative target

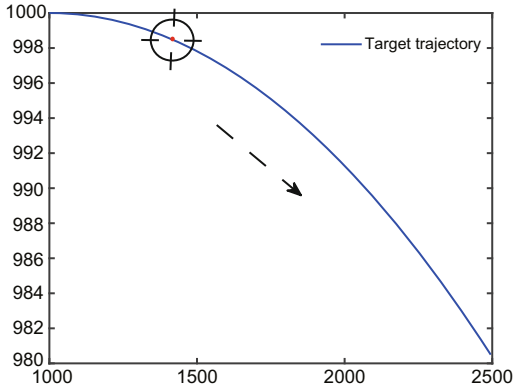

Fig. 6 Target unspecified constant turning rate trajectory within 20 m by 1500 m area

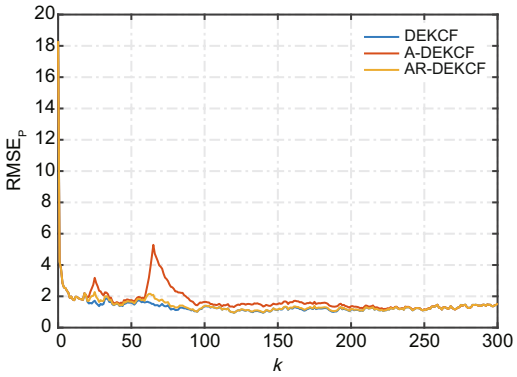

Fig. 7 $\mathrm{RMSE_P}$ comparison among different algorithms for UAV 2

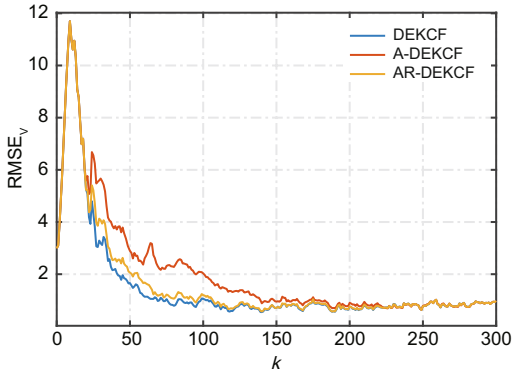

Fig. 8 $\mathrm{RMSE_V}$ comparison among different algorithms for UAV 2

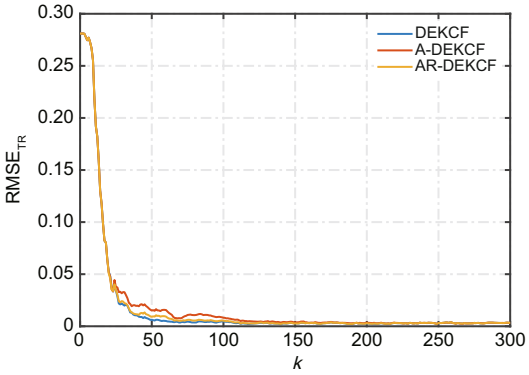

Fig. 9 $\mathrm{RMSE_{TR}}$ comparison among different algorithms for UAV 2

tracking. Future work includes (1) considering the simultaneous occurrence of multiple types of attacks and employing an MHT approach to classify and discuss the possible scenarios when attacks occur and (2) applying the proposed algorithm to a real UAV experimental platform for testing and enhancing the algorithm performance based on the experimental results.

Contributors

Yuru HU designed the research and drafted the paper. Wangyan LI supervised the research. Lifeng WU assisted in the algorithm development. Zhensheng YU assisted in the development of the proposed approach. Yuru HU and Wangyan LI revised and finalized the paper.

Conflict of interest

All the authors declare that they have no conflict of interest.

Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

Arasaratnam I, Haykin S, 2009. Cubature Kalman filters. *IEEE Trans Autom Contr*, 54(6):1254-1269. https://doi.org/10.1109/TAC.2009.2019800

Battistelli G, Chisci L, 2016. Stability of consensus extended Kalman filter for distributed state estimation. *Automatica*, 68:169-178. https://doi.org/10.1016/j.automatica.2016.01.071

Battistelli G, Chisci L, Selvi D, 2018. A distributed Kalman filter with event-triggered communication and guaranteed stability. *Automatica*, 93:75-82. https://doi.org/10.1016/j.automatica.2018.03.005

Chen B, Hu GQ, Ho DWC, et al., 2016. Distributed covariance intersection fusion estimation for cyber-physical systems with communication constraints. *IEEE Trans Autom Contr*, 61(12):4020-4026. https://doi.org/10.1109/TAC.2016.2539221

Chen B, Ho DWC, Hu GQ, et al., 2018. Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks. *IEEE Trans Cybern*, 48(6):1862-1876. https://doi.org/10.1109/TCYB.2017.2716115

Chen SQ, Ho DWC, 2023. Edge-based sender-receiver event-triggered schemes for distributed filtering. *IEEE Trans Circ Syst I Reg Papers*, 70(5):2143-2155. https://doi.org/10.1109/TCSI.2023.3242974

Chong MS, Wakaiki M, Hespanha JP, 2015. Observability of linear systems under adversarial attacks. Proc American Control Conf, p.2439-2444. https://doi.org/10.1109/ACC.2015.7171098

D'Afflisio E, Braca P, Willett P, 2021. Malicious AIS spoofing and abnormal stealth deviations: a comprehensive statistical framework for maritime anomaly detection. *IEEE Trans Aerosp Electron Syst*, 57(4):2093-2108. https://doi.org/10.1109/TAES.2021.3083466

Fawzi H, Tabuada P, Diggavi S, 2014. Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Trans Autom Contr*, 59(6):1454-1467. https://doi.org/10.1109/TAC.2014.2303233

Ge XH, Xiao SY, Han QL, et al., 2022. Dynamic event-triggered scheduling and platooning control co-design for automated vehicles over vehicular ad-hoc networks. *IEEE/CAA J Autom Sin*, 9(1):31-46. https://doi.org/10.1109/JAS.2021.1004060

Ge XH, Han QL, Wu Q, et al., 2023. Resilient and safe platooning control of connected automated vehicles against intermittent denial-of-service attacks. *IEEE/CAA J Autom Sin*, 10(5):1234-1251. https://doi.org/10.1109/JAS.2022.105845

Ge XH, Han QL, Zhang XM, et al., 2024. Communication resource-efficient vehicle platooning control with various spacing policies. *IEEE/CAA J Autom Sin*, 11(2):362-376. https://doi.org/10.1109/JAS.2023.123507

Gong XL, Sun YH, 2021. An innovative distributed filter for airborne distributed position and orientation system. *Aerosp Sci Technol*, 119:107155. https://doi.org/10.1016/j.ast.2021.107155

Han F, Wei GL, Ding DR, et al., 2017. Local condition based consensus filtering with stochastic nonlinearities and multiple missing measurements. *IEEE Trans Autom Contr*, 62(9):4784-4790. https://doi.org/10.1109/TAC.2017.2689722

Han F, Wang ZD, Dong HL, et al., 2022. A local approach to distributed H_∞-consensus state estimation over sensor networks under hybrid attacks: dynamic event-triggered scheme. *IEEE Trans Signal Inform Process Netw*, 8:556-570. https://doi.org/10.1109/TSIPN.2022.3182273

Huang JH, Tang Y, Yang W, et al., 2020. Resilient consensus-based distributed filtering: convergence analysis under stealthy attacks. *IEEE Trans Ind Inform*, 16(7):4878-4888. https://doi.org/10.1109/TII.2019.2960042

Ju YM, Ding DR, He X, et al., 2022. Consensus control of multi-agent systems using fault-estimation-in-the-loop: dynamic event-triggered case. *IEEE/CAA J Autom Sin*, 9(8):1440-1451. https://doi.org/10.1109/JAS.2021.1004386

Julier SJ, Uhlmann JK, 1997. A non-divergent estimation algorithm in the presence of unknown correlations. Proc American Control Conf, p.2369-2373. https://doi.org/10.1109/ACC.1997.609105

Kai X, Wei CL, Liu LD, 2010. Robust extended Kalman filtering for nonlinear systems with stochastic uncertainties. *IEEE Trans Syst Man Cybern Part A Syst Hum*, 40(2):399-405. https://doi.org/10.1109/TSMCA.2009.2034836

Li WY, Yang FW, Wei GL, 2018. A novel observability Gramian-based fast covariance intersection rule. *IEEE Signal Process Lett*, 25(10):1570-1574. https://doi.org/10.1109/LSP.2018.2867741

Li WY, Wang ZD, Ho DWC, et al., 2020. On boundedness of error covariances for Kalman consensus filtering problems. *IEEE Trans Autom Contr*, 65(6):2654-2661. https://doi.org/10.1109/TAC.2019.2942826

Li YZ, Shi L, Chen TW, 2018. Detection against linear deception attacks on multi-sensor remote state estimation. *IEEE Trans Contr Netw Syst*, 5(3):846-856. https://doi.org/10.1109/TCNS.2017.2648508

Liu D, Zhao YB, Yuan ZQ, et al., 2020. Target tracking methods based on a signal-to-noise ratio model. *Front Inform Technol Electron Eng*, 21(12):1804-1814. https://doi.org/10.1631/FITEE.1900679

Liu QY, Wang ZD, He X, et al., 2019. Event-based distributed filtering over Markovian switching topologies. *IEEE Trans Autom Contr*, 64(4):1595-1602. https://doi.org/10.1109/TAC.2018.2853570

Ning BD, Han QL, Zuo ZY, et al., 2023. Fixed-time and prescribed-time consensus control of multiagent systems and its applications: a survey of recent trends and methodologies. *IEEE Trans Ind Inform*, 19(2):1121-1135. https://doi.org/10.1109/TII.2022.3201589

Reif K, Gunther S, Yaz E, et al., 1999. Stochastic stability of the discrete-time extended Kalman filter. *IEEE Trans Autom Contr*, 44(4):714-728. https://doi.org/10.1109/9.754809

Ren HR, Cheng ZJ, Qin JH, et al., 2023. Deception attacks on event-triggered distributed consensus estimation for nonlinear systems. *Automatica*, 154:111100. https://doi.org/10.1016/j.automatica.2023.111100

Rezaei H, Ghorbani M, 2022. Event-triggered resilient distributed extended Kalman filter with consensus on estimation. *Int J Robust Nonl Contr*, 32(3):1303-1315. https://doi.org/10.1002/rnc.5881

Ryu K, Back J, 2022. Consensus optimization approach for distributed Kalman filtering: performance recovery of centralized filtering with proofs. https://doi.org/10.48550/arXiv.2208.09328

Shi DW, Chen TW, Shi L, 2014. An event-triggered approach to state estimation with multiple point- and set-valued measurements. *Automatica*, 50(6):1641-1648. https://doi.org/10.1016/j.automatica.2014.04.004

Wan C, Huang FJ, 2023. Adversarial attack based on prediction-correction. https://doi.org/10.48550/arXiv.2306.01809

Wang R, Li YH, Sun H, et al., 2021. Freshness constraints of an age of information based event-triggered Kalman consensus filter algorithm over a wireless sensor network. *Front Inform Technol Electron Eng*, 22(1):51-67. https://doi.org/10.1631/FITEE.2000206

Wang S, Li YY, Qi GQ, et al., 2023. Diffusion nonlinear estimation and distributed UAV path optimization for target tracking with intermittent measurements and unknown cross-correlations. *Drones*, 7(7):473. https://doi.org/10.3390/drones7070473

Wei GL, Li WY, Ding DR, et al., 2020. Stability analysis of covariance intersection-based Kalman consensus filtering for time-varying systems. *IEEE Trans Syst Man Cybern Syst*, 50(11):4611-4622. https://doi.org/10.1109/TSMC.2018.2855741

Wu JF, Jia QS, Johansson KH, et al., 2013. Event-based sensor data scheduling: trade-off between communication rate and estimation quality. *IEEE Trans Autom Contr*, 58(4):1041-1046. https://doi.org/10.1109/TAC.2012.2215253

Xiao L, Boyd SP, Lall S, 2005. A scheme for robust distributed sensor fusion based on average consensus. Proc Fourth Int Symp on Information Processing in Sensor Networks, p.63-70. https://doi.org/10.1109/IPSN.2005.1440896

Xiao SY, Ge XH, Han QL, et al., 2022. Dynamic event-triggered platooning control of automated vehicles under random communication topologies and various spacing policies. *IEEE Trans Cybern*, 52(11):11477-11490. https://doi.org/10.1109/TCYB.2021.3103328

Xie ML, Ding DR, Ge XH, et al., 2022. Distributed platooning control of automated vehicles subject to replay attacks based on proportional integral observers. *IEEE/CAA J Autom Sin*, early access. https://doi.org/10.1109/JAS.2022.105941

Yang FS, Liang XH, Guan XH, 2021. Resilient distributed economic dispatch of a cyber-power system under DoS attack. *Front Inform Technol Electron Eng*, 22(1):40-50. https://doi.org/10.1631/FITEE.2000201

Yang W, Lei L, Yang C, 2017. Event-based distributed state estimation under deception attack. *Neurocomputing*, 270:145-151. https://doi.org/10.1016/j.neucom.2016.12.109

Yang W, Zhang Y, Chen GR, et al., 2019. Distributed filtering under false data injection attacks. *Automatica*, 102:34-44. https://doi.org/10.1016/j.automatica.2018.12.027

Zhang XM, Han QL, Ge XH, et al., 2023. Sampled-data control systems with non-uniform sampling: a survey of methods and trends. *Annu Rev Contr*, 55:70-91. https://doi.org/10.1016/j.arcontrol.2023.03.004

Zhang ZH, Liu D, Deng C, et al., 2020. A dynamic event-triggered resilient control approach to cyber-physical systems under asynchronous DoS attacks. *Inform Sci*, 519:260-272. https://doi.org/10.1016/j.ins.2020.01.047

Appendix: Proof of Theorem 1

Proof The following proof is inspired by our previous research, and interested readers could refer to Wei et al. (2020) for detailed information.

To begin with, we denote $\tilde{x}_{k+1|k}$ and $\tilde{x}_k$ by $\tilde{x}_{k+1|k}=\mathrm{col}(\tilde{x}^i_{k+1|k})$ and $\tilde{x}_k=\mathrm{col}(\tilde{x}^i_k), i\in\mathcal{N}$.

Consider the following stochastic process:

$$\mathcal{V}_{k+1}(\tilde{x}_{k+1|k})=\max_{i\in\mathcal{N}}(\tilde{x}^i_{k+1|k})^{\mathrm{T}}(P^i_{k+1|k})^{-1}\tilde{x}^i_{k+1|k}. \tag{A1}$$

On the other hand, according to Assumption 2 and Eq. (4) and inequality (27), one has

$$\left(\bar{q}+\bar{p}\bar{f}^2\right)^{-1}I_n\le(P^i_{k+1|k})^{-1}\le\left(\underline{q}+\underline{pf}^2\right)^{-1}I_n. \tag{A2}$$

Substituting inequality (A2) into Eq. (A1) results in

$$\frac{\left\|\tilde{x}_{k+1|k}\right\|^2}{N(\bar{q}+\bar{p}\bar{f}^2)} \leq \mathcal{V}_{k+1}\left(\tilde{x}_{k+1|k}\right) \leq \frac{\left\|\tilde{x}_{k+1|k}\right\|^2}{\underline{q}+\underline{p}\underline{f}^2}. \quad \text{(A3)}$$

Furthermore, the prediction error $\tilde{x}^i_{k+1|k}$ ($\forall i \in \mathcal{N}$) can be written as

$$\begin{aligned}\tilde{x}^i_{k+1|k} &= f\left(x_k\right) - f\left(\hat{x}^i_k\right) + w_k \\ &= \left(F^i_k + \mathcal{L}^i_k \mathcal{U}^i_k \mathcal{T}_{1,k}\right)\tilde{x}^i_k + w_k \\ &\triangleq \mathcal{M}^i_k \tilde{x}^i_k + w_k.\end{aligned} \quad \text{(A4)}$$

As the estimation error $\tilde{x}^i_k$ denotes the fused estimate resulting from the state estimation rectification strategy, we have

$$\begin{aligned}\tilde{x}^i_k &= x_k - P^i_k\Bigg[\sum_{j\in\mathcal{N}}\pi^{i,j}_{L,k}\Big(\omega^j(P^j_k)^{-1}\hat{x}^j_k + \\ &\quad \cdot (1-\omega^j)(P^j_{\delta^j_k})^{-1}\hat{x}^j_{\delta^j_k}\Big)\Bigg] \\ &= P^i_k\Big[\sum_{j\in\mathcal{N}}\pi^{i,j}_{L,k}\omega^j(P^j_k)^{-1}\tilde{x}^j_k\Big] + P^i_k \\ &\quad \cdot\Big[\sum_{j\in\mathcal{N}}\pi^{i,j}_{L,k}(1-\omega^j)(P^j_{k|k-1})^{-1}\tilde{x}^j_{k|k-1}\Big] \\ &= P^i_k\Bigg[\sum_{j\in\mathcal{N}}\pi^{i,j}_{L,k}\omega^j(P^j_k)^{-1}(I_n - K^j_k H^j_k - K^j_k\mathcal{S}^j_k\mathcal{R}^j_k \\ &\quad \cdot \mathcal{T}^j_{2,k})\tilde{x}^j_{k|k-1} + \Big[\sum_{j\in\mathcal{N}}\pi^{i,j}_{L,k}(1-\omega^j) \\ &\quad \cdot (P^j_{k|k-1})^{-1}\tilde{x}^j_{k|k-1} - \sum_{j\in\mathcal{N}}\pi^{i,j}_{L,k}(P^j_k)^{-1}K^j_k v^j_k\Big]\Bigg] \\ &= P^i_k\Bigg[\sum_{j\in\mathcal{N}}\pi^{i,j}_{L,k}\omega^j(P^j_k)^{-1}(I_n - K^j_k\mathcal{H}^j_k) \\ &\quad + \sum_{j\in\mathcal{N}}\pi^{i,j}_{L,k}(1-\omega^j)(P^j_{k|k-1})^{-1}\tilde{x}^j_{k|k-1} \\ &\quad - \sum_{j\in\mathcal{N}}\pi^{i,j}_{L,k}(P^j_k)^{-1}K^j_k v^j_k\Bigg],\end{aligned} \quad \text{(A5)}$$

where

$$\mathcal{H}^j_k = H^j_k + \mathcal{S}^i_k\mathcal{R}^i_k\mathcal{T}^i_{2,k}.$$

Merging Eq. (A5) into Eq. (A4), we obtain

$$\tilde{x}^i_{k+1|k} \triangleq \mathcal{G}^{i,j}_k\tilde{x}^j_{k|k-1} + \varrho^{i,j}_k, \quad \text{(A6)}$$

where

$$\begin{aligned}\mathcal{G}^{i,j}_k \triangleq \mathcal{M}^i_k P^i_k\Bigg(&\sum_{j\in\mathcal{N}}\pi^{i,j}_{L,k}\omega^j(P^j_k)^{-1}(I_n - K^j_k\mathcal{H}^j_k) \\ &+ \sum_{j\in\mathcal{N}}\pi^{i,j}_{L,k}(1-\omega^j)(P^j_{k|k-1})^{-1}\Bigg),\end{aligned} \quad \text{(A7)}$$

$$\varrho^{i,j}_k \triangleq w_k - \mathcal{M}^i_k P^i_k\sum_{j\in\mathcal{N}}\pi^{i,j}_{L,k}(P^j_k)^{-1}K^j_k v^j_k. \quad \text{(A8)}$$

Then we can calculate the expected value of the random process $\mathcal{V}_{k+1}(\tilde{x}_{k+1|k})$ to yield

$$\mathbb{E}\left\{\mathcal{V}_{k+1}\left(\tilde{x}_{k+1|k}\right) \mid \tilde{x}_{k|k-1}\right\} = \Phi^{\mathcal{G}}_{k+1} + \Phi^{\varrho}_{k+1}, \quad \text{(A9)}$$

where

$$\begin{aligned}\Phi^{\mathcal{G}}_{k+1} \triangleq \mathbb{E}\Bigg\{&\max_{i\in\mathcal{N}}\left(\mathcal{G}^{i,j}_k\tilde{x}^j_{k|k-1}\right)^{\mathrm{T}}(P^i_{k+1|k})^{-1} \\ &\cdot\left(\mathcal{G}^{i,j}_k\tilde{x}^j_{k|k-1}\right)\Big|\tilde{x}_{k|k-1}\Bigg\},\end{aligned} \quad \text{(A10)}$$

$$\Phi^{\varrho}_{k+1} \triangleq \mathbb{E}\left\{\max_{i\in\mathcal{N}}(\varrho^{i,j}_k)^{\mathrm{T}}(P^i_{k+1|k})^{-1}\varrho^{i,j}_k\Big|\tilde{x}_{k|k-1}\right\}. \quad \text{(A11)}$$

In what follows, let us consider the boundedness of $\Phi^{\mathcal{G}}_{k+1}$ and Φ^{ϱ}_{k+1}.

According to Assumption 3 and Theorem 1 in Ren et al. (2023), there exist positive real numbers $\upsilon_{1,k}$ and $\eta \leq 1$ satisfying

$$P^i_{k+1|k} \geq \mathcal{M}^i_k\left[(P^i_k)^{-1} - \upsilon_{1,k}\mathcal{T}^{\mathrm{T}}_{1,k-1}\mathcal{T}_{1,k-1}\right]^{-1}(\mathcal{M}^i_k)^{\mathrm{T}}, \quad \text{(A12)}$$

$$\begin{aligned}(P^i_k)^{-1} \leq \eta(I_n - K^j_k\mathcal{H}^j_k)^{-\mathrm{T}}(P^i_{k|k-1})^{-1} \\ \cdot (I_n - K^j_k\mathcal{H}^j_k)^{-1}.\end{aligned} \quad \text{(A13)}$$

Substituting inequality (A12) into Eq. (A10), we

have

$$\begin{aligned}\Phi_{k+1}^{\mathcal{G}} \leq \mathbb{E}\Bigg\{ & \max_{i\in\mathcal{N}}\Bigg[\mathcal{M}_k^i P_k^i\Big(\sum_{j\in\mathcal{N}}\pi_{L,k}^{i,j}\omega^j(P_k^j)^{-1}(I_n \\ & -K_k^j\mathcal{H}_k^j)+\sum_{j\in\mathcal{N}}\pi_{L,k}^{i,j}(1-\omega^j)(P_{k|k-1}^j)^{-1}\Big) \\ & \cdot\,\tilde{x}_{k|k-1}^j\Bigg]^{\mathrm{T}}(\mathcal{M}_k^i)^{-\mathrm{T}}\left[(P_k^i)^{-1}-\upsilon_{1,k}\mathcal{T}_{1,k-1}^{\mathrm{T}}\right. \\ & \cdot\,\left.\mathcal{T}_{1,k-1}\right](\mathcal{M}_k^i)^{-1}\Bigg[\mathcal{M}_k^i P_k^i\Big(\sum_{j\in\mathcal{N}}\pi_{L,k}^{i,j}\omega^j \\ & \cdot\,(P_k^j)^{-1}(I_n-K_k^j\mathcal{H}_k^j)+\sum_{j\in\mathcal{N}}\pi_{L,k}^{i,j}(1-\omega^j) \\ & \cdot\,(P_{k|k-1}^j)^{-1}\Big)\tilde{x}_{k|k-1}^j\Bigg]\Big|\tilde{x}_{k|k-1}\Bigg\} \\ \leq (1-\upsilon_{1,k})\mathbb{E}\Bigg\{ & \max_{i\in\mathcal{N}}\Bigg[\Big(\sum_{j\in\mathcal{N}}\pi_{L,k}^{i,j}\omega^j(P_k^j)^{-1} \\ & \cdot\,(I_n-K_k^j\mathcal{H}_k^j)+\sum_{j\in\mathcal{N}}\pi_{L,k}^{i,j}(1-\omega^j) \\ & \cdot\,(P_{k|k-1}^j)^{-1}\Big)\tilde{x}_{k|k-1}\Bigg]^{\mathrm{T}}P_k^i\Bigg[\Big(\sum_{j\in\mathcal{N}}\pi_{L,k}^{i,j}\omega^j \\ & \cdot\,(P_k^j)^{-1}(I_n-K_k^j\mathcal{H}_k^j)+\sum_{j\in\mathcal{N}}\pi_{L,k}^{i,j}(1-\omega^j) \\ & \cdot\,(P_{k|k-1}^j)^{-1}\Big)\,\tilde{x}_{k|k-1}^j\Bigg]\Big|\tilde{x}_{k|k-1}\Bigg\}. \end{aligned} \tag{A14}$$

Furthermore, due to the fact $P_k^i = (\sum_{j\in\mathcal{N}}\pi_{L,k}^{i,j}(P_k^j)^{-1})^{-1}$, integrating inequality (A13) into inequality (A14), we have

$$\begin{aligned}\Phi_{k+1}^{x} \leq\ & \eta(1-\upsilon_{1,k})\mathbb{E}\Bigg\{\max_{i\in\mathcal{N}}\sum_{j\in\mathcal{N}}\pi_{L,k}^{i,j}\omega^j\left(\tilde{x}_{k|k-1}^j\right)^{\mathrm{T}} \\ & \cdot\,(P_{k|k-1}^j)^{-1}\tilde{x}_{k|k-1}^j+\sum_{j\in\mathcal{N}}\pi_{L,k}^{i,j}(1-\omega^j) \\ & \cdot\left(\tilde{x}_{k|k-1}^j\right)^{\mathrm{T}}(P_{k|k-1}^j)^{-1}\tilde{x}_{k|k-1}^j\Big|\tilde{x}_{k|k-1}\Bigg\} \\ \leq\ & \eta(1-\upsilon_{1,k})\mathbb{E}\Big\{\max_{i\in\mathcal{N}}\left(\tilde{x}_{k|k-1}^i\right)^{\mathrm{T}}(P_{k|k-1}^i)^{-1} \\ & \cdot\,\tilde{x}_{k|k-1}^i\Big|\tilde{x}_{k|k-1}\Big\} \\ =\ & (1-\upsilon_{1,k})\mathbb{E}\left\{V\left(\tilde{x}_{k|k-1}\right)\right\}. \end{aligned} \tag{A15}$$

Embedding $\varrho_k^{i,j}$ into Φ_{k+1}^{ϱ} of Eq. (A11), we have

$$\begin{aligned}\Phi_{k+1}^{\varrho} = & \mathbb{E}\Big\{\max_{i\in\mathcal{N}}\ w_k^{\mathrm{T}}\left(P_{k+1|k}^i\right)^{-1}w_k\Big\} \\ & +\mathbb{E}\Bigg\{\max_{i\in\mathcal{N}}\left(\mathcal{M}_k^i P_k^i\sum_{j\in\mathcal{N}}\pi_{L,k}^{i,j}(P_k^j)^{-1}K_k^j v_k^j\right)^{\mathrm{T}} \\ & \cdot\left(P_{k+1|k}^i\right)^{-1}\left(\mathcal{M}_k^i P_k^i\sum_{j\in\mathcal{N}}\pi_{L,k}^{i,j}(P_k^j)^{-1}\ K_k^j v_k^j\right)\Bigg\}. \end{aligned} \tag{A16}$$

Simultaneously, by reorganizing Eq. (7), we obtain an alternative expression for the Kalman gain:

$$K_k^j = P_k^j(H_k^j)^{\mathrm{T}}(R_k^j)^{-1}. \tag{A17}$$

Substituting Eq. (A17) into Eq. (A16), one has

$$\begin{aligned}\Phi_{k+1}^{\varrho} \leq\ & N(\underline{q}+\underline{pf^2})^{-1}\mathrm{tr}\{Q_k\}+\bar{p}\overline{h}^2(1-2\upsilon_{1,k})Nm \\ & \cdot\mathrm{tr}\Bigg\{\mathbb{E}\Big\{\sum_{j\in\mathcal{N}}(v_k^j)^{\mathrm{T}}(R_k^j)^{-\mathrm{T}}(R_k^j)^{-1}v_k^j\Big\}\Bigg\} \\ =\ & N(\underline{q}+\underline{pf^2})^{-1}\overline{q}n+\bar{p}\overline{h}^2(1-2\upsilon_{1,k})Nm \\ \triangleq\ & \mu_s. \end{aligned} \tag{A18}$$

At this point, the upper bounds of Φ_{k+1}^{x} and Φ_{k+1}^{ϱ} have been presented in inequalities (A15) and (A18), respectively. According to in Lemma 7 in Reif et al. (1999), we can observe that $\tilde{x}_{k+1|k}^i$ is exponentially bounded in mean square. Furthermore, by applying similar procedures as detailed in Eqs. (68) and (69) in Wei et al. (2020), we can deduce that $\tilde{x}_{k+1}^i$ is exponentially bounded in mean square as well.