IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 27 September 2023, accepted 16 October 2023, date of publication 23 October 2023, date of current version 1 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3326874

RESEARCH ARTICLE

Trust-Based Distributed H∞ Diffusion Filtering for Target Tracking Under Cyber Attacks

YANSHEN GAO, HONGBO ZHU, XUEYANG LI, AND MINANE JOEL VILLIER AMURI
School of Electrical and Information Engineering, Anhui University of Science and Technology, Huainan 232001, China

Corresponding author: Hongbo Zhu (hbzhu@aust.edu.cn)

This work was supported in part by the National Nature Science Foundation of China under Grant No. 62003001, in part by the Natural Science Research Project of Anhui Educational Committee under Grant No. 2023AH040157, in part by the Anhui Provincial Natural Science Foundation under Grant No. 2008085QF298, in part by the Open Research Grant of Joint National-Local Engineering Research Centre for Safe and Precise Coal Mining under Grant No. 2022KLMI01, and in part by the Graduate Innovation Fund Project of the Anhui University of Science and Technology under Grant No. 2023cx2093.

ABSTRACT Concerning the problem of target tracking in wireless sensor networks under cyber attacks, this paper proposes a trust-based distributed $H\infty$ diffusion filtering method, designed to maintain resilience against diverse types of cyber attacks. Firstly, the distributed $H\infty$ filtering equation for a linear discrete system is implemented for iterative updates of state estimation and error covariance. Secondly, to address the impact of cyber attacks, the K-means-based trust set extracting algorithm is employed to identify and remove attacked untrusted nodes. Subsequently, the data from trusted nodes is fused based on a diffusion strategy, leading to recalculations of state estimation and covariance, thus improving the overall target tracking performance. Experimental results demonstrate the effectiveness of our method in resisting denial of service attacks and deception attacks, such as random, replay, and false data injection attacks. The proposed approach offers robustness and adaptability, making it suitable for practical applications in distributed sensor networks under cyber attacks.

INDEX TERMS Cyber attacks, distributed $H\infty$ diffusion filtering, wireless sensor networks, target tracking.

I. INTRODUCTION

With the blessing of wireless communication and micro-electromechanical systems technology, sensor nodes are becoming all the more minute and cost-effective, as well as integrating various sensors, embedded microprocessors, and radio frequency transceivers with a high level of intelligence. Wireless sensor network (WSN) is composed of a good deal of such affordable, low-power, and multifunctional miniature sensor nodes, which can not only collect information, but also perform data processing and wireless communication, and are widely applied to collaborative positioning with mobile robots [1], [2], [3], target tracking [4], [5], [6], [7], [8], monitoring [9], [10], etc. In these common applications, multi-sensor information fusion is one of the indispensable enablers.

In WSN, there exist three primary multi-sensor fusion frameworks: centralized fusion, decentralized fusion, and distributed fusion. Centralized fusion connects all nodes to the fusion hub, and decentralized fusion assigns sensor nodes statically or dynamically to multiple fusion centers. In distributed fusion, however, each sensor node communicates exclusively with its directly connected neighbor nodes in a peer-to-peer fashion [11]. The distributed structure is adopted in this paper as it offers several advantages over the previous two fusion structures. It not only improves the adaptability to the network topology and reduces the communication burden, but also enhances the robustness of the sensor networks. In addition, different from the communication mode of the distributed consensus fusion strategy in [5], each sensor node iteratively communicates with all its connected neighbors, while in the distributed diffusion fusion strategy, each sensor node communicates with all connected neighbors once, thus reducing the communication burden. Some typical distributed filtering methods in WSN include distributed Kalman filtering [12], distributed particle filtering [13], and distributed $H\infty$ filtering [14], [15]. Among them, the distributed particle filtering boasts higher estimation accuracy than the

The associate editor coordinating the review of this manuscript and approving it for publication was Min Wang.

TABLE 1. A list of solutions to cyber attacks.

Methods		Fusion strategy	Dos attacks	Deception attacks		
				Random	Replay	FDI
Attack detection	Distributed attack detection estimations[10]	\	\	√	√	√
	A Kullback-Leibler divergence-based detector[23]	\	√	√	√	√
Attack mitigation	Event-triggered distributed Kalman filters[23]	\	\	√	√	√
	A specific system protection scheme[24]	\	\	\	\	√
	A variation of the receding-horizon control method[25]	\	\	\	√	\
	Trust-based distributed Kalman filtering[26]	√	\	√	√	√
	Distributed sampled-data $H\infty$ consensus filtering[28]	√	√	\	\	\
	Distributed $H\infty$ fusion filtering [29]	√	√	\	\	\
	Distributed finite-time $H\infty$ filtering[30]	\	\	√	√	√
	Presented method	√	√	√	√	√

distributed Kalman filtering, but at the expense of increased calculation amount. Previous studies [16], [17] demonstrate that $H\infty$ filtering is superior to Kalman filtering in handling arbitrary noise with bounded energy, without requiring any assumptions about the statistical characteristics of the system and observation noise. Additionally, it exhibits stronger robustness to parameter uncertainty and lower computational complexity for large-scale sensor networks. Reference [14] investigates how to perform distributed $H\infty$ filtering for polynomial nonlinear stochastic systems in sensor networks. Reference [15] addresses the issue of randomly occurring missing measurements and communication link failures in sensor networks through the development of a distributed $H\infty$ filtering algorithm. To propose a more robust distributed state estimation solution, [18] shows that the piecewise linear discrete system effectively incorporates the consensus strategy based on distributed $H\infty$ filtering. Furthermore, distributed $H\infty$ consensus filtering is applied to sensor networks with missing measurement data [19], specifically in a finite-horizon context. Nevertheless, distributed consensus filtering schemes require estimators to complete consensus steps faster than local filtering time steps, imposing a time-bound burden on the network. To this end, the author of [20] first proposed a class of fully distributed $H\infty$ filtering technology that uses diffusion structure to coordinate the information flow in the network and complete the fusion of local filtering, and thus have better real-time performance. Regrettably, the selection of its fusion weights has not been carefully considered.

Although significant progress has been made in the research of distributed $H\infty$ filtering in sensor networks, its security in WSN has not been thoroughly explored. WSN is susceptible to a variety of security challenges owing to its uncertain structure, adverse deployment locations, and insecure network protocols [21]. Specifically, (1) the application environment is complex and uncertain, and the sensor nodes have limited resources such as demanding energy, broadband, and storage capacity. (2) Compared with traditional networks, the WSN has a broader and more scalable attack surface because it collects and exchanges data wirelessly, and its multi-layer network is vulnerable to threats. (3) As WSN closely interacts with other systems, it also introduces new security issues, such as threats to the integrity and confidentiality of data exchange, interception and analysis of network traffic, and unexpected access to network resources. Security threats to WSN broadly fall into two main categories: Denial of serve (Dos) attacks and deception attacks. Dos attacks primarily block or interfere with the channels of the communication network. On the other hand, Deception attacks, by maintaining the concealment of detectors, manipulate data packets on communication networks, thereby compromising the integrity and trustworthiness of data [22]. Common deception attacks include random, false data injection (FDI), replay attacks, etc. Once the WSN is maliciously attacked by the attacker, it will adversely affect the operation of the WSN, and even more serious losses. Therefore, effective protection against cyber attacks is essential. In [10], a distributed attack detection mechanism is devised for deception attacks on communication links in sensor networks. In [23], meta-Bayes combined with an attack detection mechanism are used to reduce the impact of attacks. A protection scheme is proposed in [24], to keep the information communication channel of the system from FDI attacks. Reference [25] analyzes the replay attack and presents a specific approach to grapple with it. To resist multiple deception attacks, trust-based distributed Kalman filtering [26] and trust-based distributed set-membership filtering [27] are presented as superior to uniform and relative degree-variance combination rules. However, there are few pieces of research on distributed $H\infty$ filtering in WSN under cyber attacks. Recently, two different distributed $H\infty$ filters have been designed to effectively resist Dos attacks in the network, both employing a fusion strategy, with [28] combining common consensus fusion, and [29] constructing a weighted fuser but being constrained by local $H\infty$ filtering performance. A new asynchronous distributed $H\infty$ filter is given in [30] to protect against deception attacks. These distributed $H\infty$ filters, however, are only shown to be resilient to specific cyber attacks. Reference [31] designs a distributed event-triggered $H\infty$ filter by modeling unclassified cyber attacks as a nonlinear function. However, this will increase computational complexity, especially in real-time systems, which may lead to real-time performance degradation. TABLE 1 lists the proposed effective solutions to cyber attacks. To the best of our knowledge, there is no literature considering resilient state estimation of the WSN under cyber attacks based on distributed $H\infty$ filtering with a diffusion strategy. Inspired by the above discussion, we present a trust-based distributed $H\infty$ diffusion filtering for dynamic target tracking under cyber attacks. The main contributions are summarized as follows:

1) We propose a trust-based distributed $H\infty$ diffusion filtering approach, designed to address the challenges posed by cyber attacks, including Dos attacks and three types of deception attacks (random attacks, replay attacks, and FDI attacks).
2) Compared to existing distributed $H\infty$ filtering approaches under cyber attacks, we consider the types of cyber attacks more comprehensively and eliminate the need to construct distinct models for various types of attacks.
3) Diffusion-based fusion is the byproduct of the proposed method that computes the optimal fusion weights and achieves a significantly enhanced level of information fusion.
4) The main advantages of this scheme are intuitive understanding, simple structure, low communication burden, excellent real-time performance, and high adaptability. Beyond target tracking applications, it has potential applicability in other fields, such as navigation and positioning, as well as distributed security state estimation in power systems.

The remainder of this work continues below. Section II expounds on the distributed $H\infty$ filtering issues and makes some preliminary explanations. Section III proposes trust-based distributed $H\infty$ diffusion filtering for target tracking in WSN. Section IV provides simulation and numerical results with examples. Lastly, the article is summarized in section V.

II. PROBLEM DESCRIPTION

For convenience and simplicity, the dynamic state of a physical target is assumed as the following linear equation

$$\begin{cases} x_{k+1} = F_k x_k + \omega_k \\ z_k = L_k x_k \end{cases} \tag{1}$$

where $x_k \in \mathbb{R}^n$ is the state vector, ω_k is the zero mean of the process noise with covariance Q_k, F_k is the system state matrix with appropriate dimensions, L_k is a custom given matrix, and z_k is a linear combination of state x_k. The measurement equation of this dynamic system is expressed as

$$y_k = H_k x_k + v_k \tag{2}$$

where $y_k \in \mathbb{R}^m$ is the measurement output, v_k is the zero mean of the measured noise with covariance R_k, and H_k is the system output matrix with appropriate dimensions.

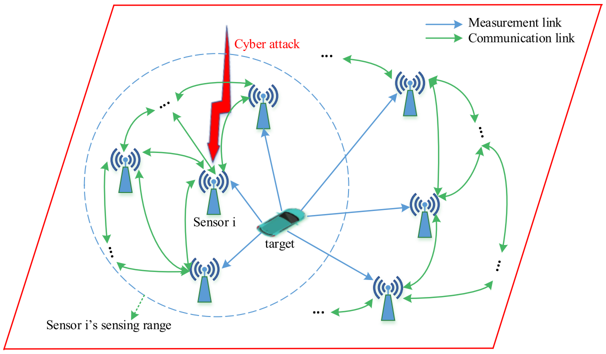

FIGURE 1. Distributed target tracking over WSN under cyber attacks.

For distributed $H\infty$ filtering, the measured value of the sensor node i at time k is expressed as follows, referring to the given measurement equation (2).

$$y_{i,k} = H_{i,k} x_k + v_{i,k} \tag{3}$$

where $v_{i,k}$ is the observed noise of the sensor node i and $R_{i,k}$ is the covariance matrix of the observed noise $v_{i,k}$.

In the presence of malicious cyber attacks, the distributed target tracking diagram over WSN is shown in FIGURE 1. The sensor node i in the network collects local dynamic information about the target from its neighbors and itself, which is processed in a distributed fusion architecture that does not require all connections to the network. This reduces the communication burden of the WSN, enhances the built-in redundancy of the network, and improves the robustness of the network. The various malicious cyber attacks stated below are taken into account and reasonable assumptions are applied. Suppose the attacker has the ability to launch different cyber attacks on this network. And suppose that the quantity of sensor nodes in the sensor network under malicious attack is less than half of the number of all sensor nodes.

- **Dos attacks:** Maliciously interfere or block the channel of the communication network, the receiver cannot access the required data. Measurement links between the physical target to sensor nodes and communication links between adjacent sensor nodes are vulnerable to Dos attacks.
- **Deception attacks:** Compromising the accuracy or credibility of data by manipulating the sequence of data packets on the WSN communication link without detection by system detectors.

1) **Random attacks:** Attackers launch random attacks on the system by manipulating sensor observation results. The attack can be carried out at any time, and the intensity of the attack varies.
2) **Replay attacks:** The data recorded by the sensor's previous measurements is replayed into the filtering for a certain period.
3) **FDI attacks:** Attackers mislead the system filtering by designing well-structured attack sequences to introduce into the system state.

III. TRUST-BASED DISTRIBUTED H∞ DIFFUSION FILTERING

A. DISTRIBUTED H∞ FILTERING

Based on game theory $H\infty$ filtering [32], the distributed $H\infty$ filtering of the system (1) needs to meet the performance constraint

$$\frac{\sum_{k=0}^{N-1} \| z_{i,k} - \tilde{z}_{i,k} \|^2_{S_{i,k}}}{\| x_0 - \tilde{x}_0 \|^2_{P_0^{-1}} + \sum_{k=0}^{N-1} (\| \omega_{i,k} \|^2_{Q_{i,k}^{-1}} + \| v_{i,k} \|^2_{R_{i,k}^{-1}})} < \frac{1}{\gamma} \tag{4}$$

where $z_{i,k}$ represents a linear combination of the states of sensor node i, $\tilde{z}_{i,k}$ represents the estimate of $z_{i,k}$, x_0 represents the estimate of the initial state, and γ is our defined performance boundary. P_0, Q_k, R_k, S_k are known selectable symmetric positive definite matrices. The goal is to find the estimate of $z_{i,k}$ and thus minimize $z_{i,k} - \tilde{z}_{i,k}$. Firstly, the distributed equation defines

$$\bar{S}_{i,k} = L_{i,k}^T S_{i,k} L_{i,k}. \tag{5}$$

And the distributed $H\infty$ filtering gain is

$$K_{i,k} = P_{i,k}\left[I - \gamma \bar{S}_{i,k} P_{i,k} + H_{i,k}^T R_{i,k}^{-1} H_{i,k} P_{i,k}\right]^{-1} H_{i,k}^T R_{i,k}^{-1}. \tag{6}$$

Then the estimated value $\tilde{x}_{i,k+1}$ and the estimated error covariance $\tilde{P}_{i,k+1}$ of the system state are updated on the basis of the following equation

$$\tilde{x}_{i,k+1} = F_{i,k}\tilde{x}_{i,k} + F_{i,k}K_{i,k}(y_{i,k} - H_{i,k}\tilde{x}_{i,k}) \tag{7}$$

$$\begin{aligned}\tilde{P}_{i,k+1} &= E\left[\left(x_{i,k+1} - \tilde{x}_{i,k+1}\right)\left(x_{i,k+1} - \tilde{x}_{i,k+1}\right)^T\right] \\ &= F_{i,k}P_{i,k}\left[I - \gamma \bar{S}_{i,k} P_{i,k} + H_{i,k}^T R_{i,k}^{-1} H_{i,k} P_{i,k}\right]^{-1} F_{i,k}^T \\ &\quad + Q_{i,k}.\end{aligned} \tag{8}$$

State estimation $\tilde{x}_{i,k+1}$ and covariance $\tilde{P}_{i,k+1}$ are exchanged between adjacent sensor nodes. In addition, for the above problems to be solved, the following conditions must be met at every instantaneousness.

$$P_{i,k}^{-1} - \gamma \bar{S}_{i,k} + H_{i,k}^T R_{i,k}^{-1} H_{i,k} > 0 \tag{9}$$

B. K-MEANS-BASED EXTRACTING ALGORITHM

To alleviate the impact of malicious cyber attacks on distributed filtering, the attacked nodes and unattacked nodes in the network need to be distinguished. The K-means algorithm is the most commonly applied and well-known clustering algorithm [33]. The measured state estimation $\tilde{x}_{i,k+1}$ and covariance matrix $\tilde{P}_{i,k+1}$ are clustered by the K-means-based trust set extracting algorithm, so the trusted clusters are obtained for further information fusion and the untrusted clusters are discarded. Firstly, the objective function of the K-means extracting algorithm is defined.

$$J = \sum_{j\in S_N^i} \sum_{c\in\{1,2\}} r_{jc} \left\|\tilde{x}_{j,k+1} - \mu_c\right\|^2 \tag{10}$$

where $r_{jc} = 1$ when the data point $\tilde{x}_{j,k+1}$ is classified to μ_c, otherwise $r_{jc} = 0$. Let S_N^i denote the group of the sensor node i and its single-hop neighbors. The detail steps of the K-means-based trust nodes set extraction are as follows.

Step 1: Two clustering center points μ_1 and μ_2 are randomly selected.

Step 2: The following process is repeated until convergence. (a) For each example $\tilde{x}_{i,k+1} \in S_N^i$, computationally cluster it into the cluster it belongs to.

$$c^{(i)} = \arg\min_c \left\|\tilde{x}_{j,k+1} - \mu_c\right\|^2, \quad c = 1, 2 \tag{11}$$

where $c^{(i)}$ represents the class closets to the node i to the two cluster centers, $c^{(i)} \in \{1, 2\}$. (b) For each class c, the center of that class is recalculated as follows.

$$\mu_c = \frac{\sum_{j\in S_N^i} r_{jc} x_{j,k+1}}{\sum_{j\in S_N^i} r_{jc}} \tag{12}$$

(c) The number of state estimates in the trusted clusters is calculated.

$$\phi = \max \sum_{j\in S_N^i} r_{jc}, \quad c = 1, 2 \tag{13}$$

Through the above steps, the cluster of trusted state estimate is obtained, and the corresponding cluster of trusted sensor nodes is denoted as ψ.

C. DIFFUSION-BASED ALGORITHM

Distributed Kalman filtering using a diffusion strategy in sensor networks was first proposed in [34], where the diffusion scheme has network adaptability and robustness to link failure nodes in distributed estimation problems. Unlike distributed $H\infty$ consensus filtering, distributed $H\infty$ diffusion filtering utilizes convex combinations of local information, in which each sensor node communicates only once with the neighbor nodes. Its general expression is as follows.

$$\tilde{x}_{i,k+1} = \sum_{j\in S_N^i} \alpha_{ij,k+1}\tilde{x}_{j,k+1} \tag{14}$$

where $\alpha_{ij,k+1}$ is the weight of the linear combination of fusion estimation of the diffusion strategy, which plays an important role in the fusion estimation performance. Usually, reliable and accurate local estimated nodes are assigned larger weights, while unreliable nodes take smaller weights. Therefore, the optimal fusion weights are calculated by the following formula:

$$\alpha_{ij,k+1} = \begin{cases} 0, & if\ j \notin \psi \\ \dfrac{\left(p_{j,k+1}^*\right)^{-1}}{\sum_{j\in\psi}\left(p_{j,k+1}^*\right)^{-1}}, & if\ j \in \psi \end{cases} \tag{15}$$

Algorithm 1 Procedure of Trust-Based Distributed $H\infty$ Diffusion Filtering

```
1: Initialize the state matrix $x_0$ and covariance matrix $P_0$.
2: Distributed $H\infty$ filtering updates state estimation
   $\tilde{x}_{i,k+1}$ (7) and covariance $\tilde{P}_{i,k+1}$ (8).
3: Two clustering center points $\mu_1$, $\mu_2$ are randomly selected.
4: Calculate the distance from the data obtained in Step 2
   to the cluster center separately and divide it into the nearest
   cluster (11).
5: Update the cluster center (12).
6: Repeat 4 and 5 until convergence.
7: The diffusion-based strategy is adopted, and its optimal
weight is calculated by (15)(16) after meeting the clustering
termination condition.
8: Recalculate state estimation $\tilde{x}_{i,k+1}$ (18) and covariance
$\tilde{P}_{i,k+1}$ (19).
```

where

$$p^{*}_{j,k+1} = \max_{t=1,\cdots,n} \tilde{P}^{tt}_{j,k+1}, \tag{16}$$

$$\sum_{j\in\psi} \alpha_{ij,k+1} = 1 \tag{17}$$

and $\tilde{P}^{tt}_{j,k+1}$ represents each element on the diagonal of matrix $\tilde{P}_{j,k+1}$. Thus, the state estimation $\tilde{x}_{i,k+1}$ and covariance $\tilde{P}_{i,k+1}$ are recalculated and expressed as

$$\tilde{x}_{i,k+1} = \sum_{j\in\psi} \alpha_{ij,k+1}\tilde{x}_{j,k+1}, \tag{18}$$

$$\tilde{P}_{i,k+1} = \sum_{j\in\psi} \alpha_{ij,k+1}\tilde{P}_{j,k+1}. \tag{19}$$

So far, a new trust-based distributed $H\infty$ diffusion filtering method against cyber attacks is presented and summarized in Algorithm 1.

IV. SIMULATION RESULTS

In this part, the above-presented technique is applied to an example to evaluate its performance against Dos attacks and three common deception attacks, random attacks, replay attacks, and FDI attacks. Based on the assumptions in this paper and the fully distributed diffusion strategy for fusion estimation, we consider a demonstration scenario involving WSN. The network consists of 9 sensor nodes, as depicted in FIGURE 2, with 4 nodes subjected to attacks and 5 nodes remaining unattacked. The target is detected and tracked within this network coverage. The corresponding parameters are set as follows:

$$F=\begin{bmatrix}1&1&0&0\\0&1&0&0\\0&0&1&1\\0&0&0&1\end{bmatrix},\quad H=\begin{bmatrix}1&0&0&0\\0&0&1&0\end{bmatrix},\ L=I_4.$$

The initial state is $x_0 = \begin{bmatrix}0 & 2 & 0 & 4\end{bmatrix}^T$, and its error covariance is $P_0 = I_4$. The error covariance matrix of system noise is $Q = diag\left\{\begin{bmatrix}0.5 & 1 & 0.5 & 1\end{bmatrix}\right\}$, and the error covariance matrix of observed noise is $R = I_2$. To comply with the condition specified by equation (9), let $S = diag\left\{\begin{bmatrix}40 & 40 & 40 & 40\end{bmatrix}\right\}$ and $\gamma = 1.1$, where $diag\{\cdot\}$ denotes the diagonal matrix, whose diagonal elements are the entries in $(\cdot)$. I_n is the identity matrix of order n. For the sake of simplicity, in this example, the diffusion fusion step computes the average estimate of the neighboring nodes.

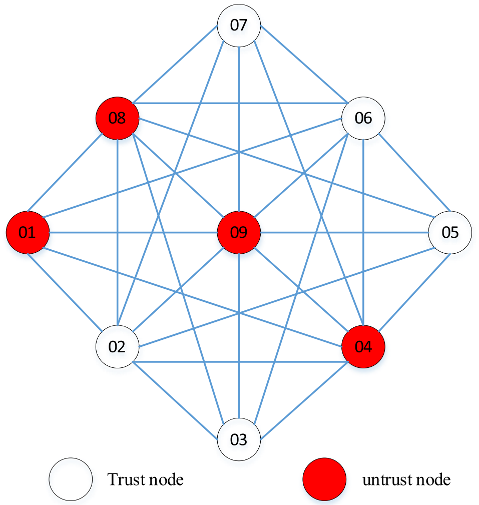

FIGURE 2. A WSN under malicious cyber attacks.

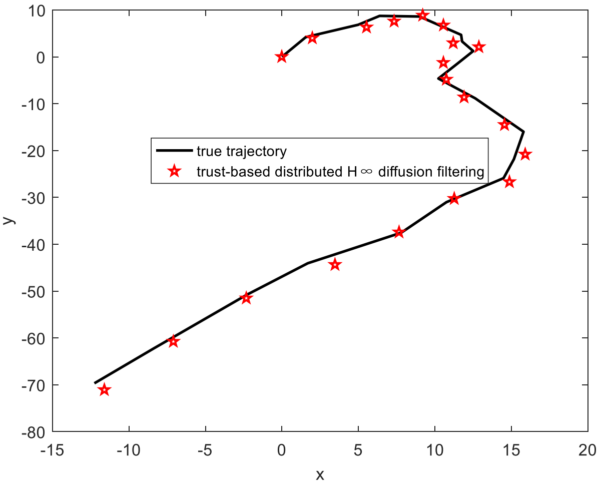

FIGURE 3. The true trajectory, and the trajectory estimated by the proposed method under Dos attacks.

A. Dos ATTACKS

The primary purpose of Dos attacks is to disrupt or block the channel of the WSN, preventing data from being successfully or completely transmitted to the intended destination. After the Dos attacks on node 01, both its communication and measurement links were blocked. Consequently, the attacked sensor node cannot obtain dynamic information of the target, and its adjacent nodes cannot send data to it or receive its data. As illustrated in FIGURE 3, the proposed trust-based

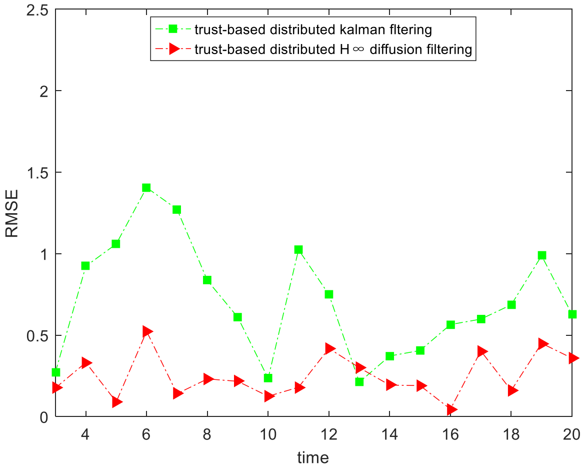

FIGURE 4. The RMSE for trust-based distributed Kalman filtering and the proposed method under Dos attacks.

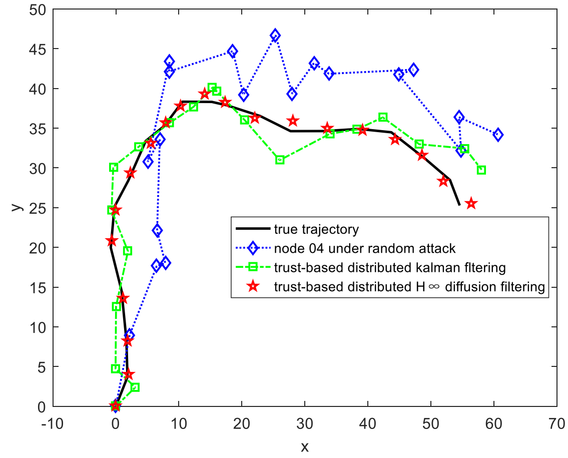

FIGURE 5. The true trajectory, the trajectory estimated by node 04, and the trajectory estimated by the trust-based distributed Kalman filtering and the proposed method under random attacks.

distributed $H\infty$ diffusion filtering method can effectively deal with the interference of Dos attacks and exhibits positive results in target tracking. This is achieved by relying on state estimates provided exclusively by trusted nodes, while disregarding inputs from untrusted nodes. FIGURE 4 shows the root mean square error (RMSE) of target tracking by the proposed method and the trust-based distributed Kalman filtering under Dos attacks. In contrast, the proposed method offers tracking results that closely match the real target state and displays higher resilience against Dos attacks.

B. DECEPTION ATTACKS

Three common deception attacks, such as random, replay, and FDI attacks, are considered to reflect the feasibility and superiority of the presented method.

1) RANDOM ATTACKS

Attackers launch random attacks on sensor networks by manipulating sensor-measuring results. In FIGURE 5, the random attack occurs at any time, and under the attack, the state estimation of the sensor node deviates significantly from the true trajectory of the target. Moreover, it is noted that the proposed method and the trust-based distributed Kalman filtering have certain resilience for this attack. FIGURE 6 makes use of RMSE as a metric to contrast the resilience of both method in the face of random attacks. Due to its enhanced ability to handle noise and errors, the proposed trust-based distributed $H\infty$ diffusion filtering exhibits a relatively smaller and smoother RMSE. This indicates that it is more robust when confronted with random attacks, enabling it to track the target with greater accuracy and consistency.

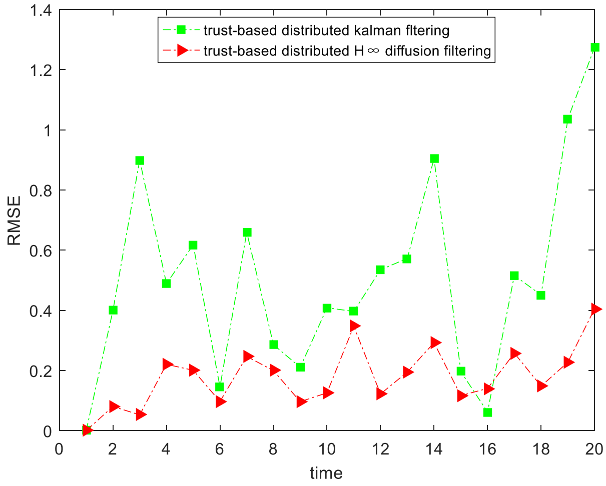

FIGURE 6. The RMSE for trust-based distributed Kalman filtering and the proposed method under random attacks.

2) REPLAY ATTACKS

During a certain period, the sequence of data previously communicated by the sensor node is replayed. The stability and performance of filtering are compromised due to outdated sequences of replayed packets. The state estimate $x_{k-\ell}(\ell < k)$ as an attack vector is replayed into the data sequence of the communication channel of the untrusted nodes. It is not difficult to perceive from FIGURE 7 that both the proposed method and the trust-based distributed Kalman filtering achieve the expected effect in tracking the target trajectory under replay attacks, but the former is relatively more accurate. This result is further reflected in the RMSE of the two methods in FIGURE 8. Consequently, the proposed scheme for target tracking exhibits greater resilience against replay attacks.

3) FDI ATTACKS

Attackers design well-structured attack sequences to change the estimated state while skillfully maintaining concealment from detectors. In this case, false data a_k is injected into the state estimate $\tilde{x}_{i,k+1}$ as an attack vector. It is observed from FIGURE 9 that the infected sensor node was severely affected due to the injection of erroneous data. However, amid this digital battleground, the trust-based distributed

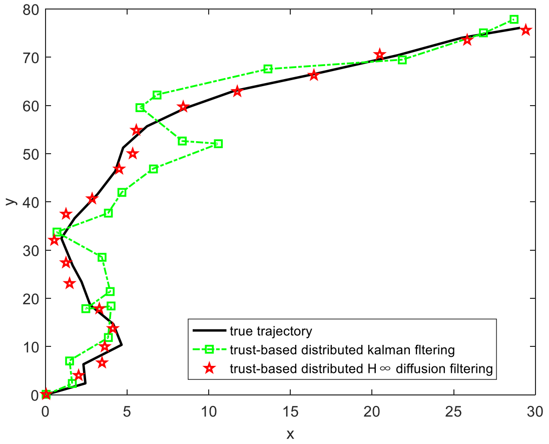

FIGURE 7. The true trajectory, the trajectory estimated by the trust-based distributed Kalman filtering, and the proposed method under replay attacks.

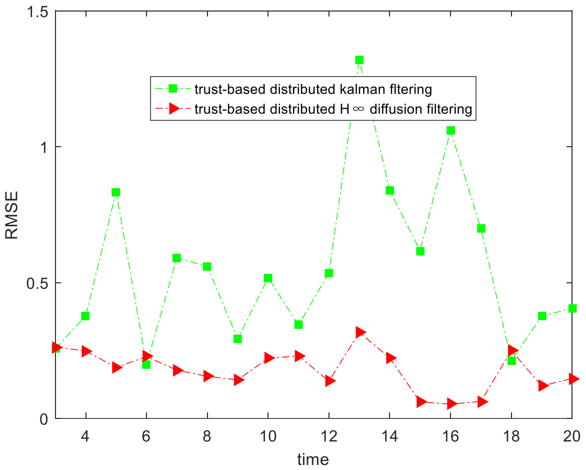

FIGURE 8. The RMSE for trust-based distributed Kalman filtering and the proposed method under replay attacks.

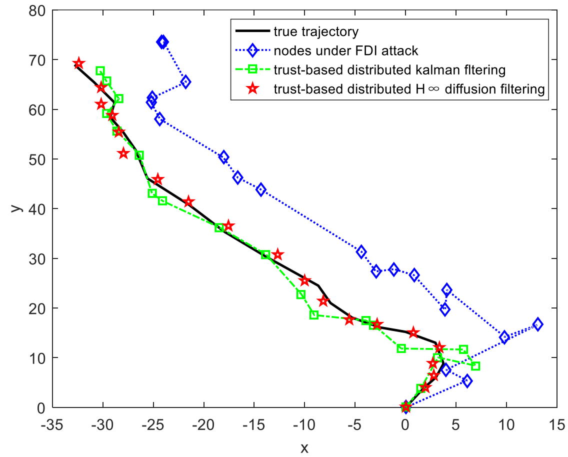

FIGURE 9. The true trajectory, the trajectory estimated by untrusted nodes, the trajectory estimated by the trust-based distributed Kalman filtering and the proposed method under FDI attacks.

filtering scheme demonstrates its effectiveness in resisting FDI attacks. FIGURE 10 provides further insights by comparing the RMSE of the proposed method with that of trust-based distributed Kalman filtering. Notably, the overall RMSE of the proposed method is smaller across the entire spectrum of analysis. As a result, the resiliency of the proposed method for target tracking against FDI attacks has a superior effect.

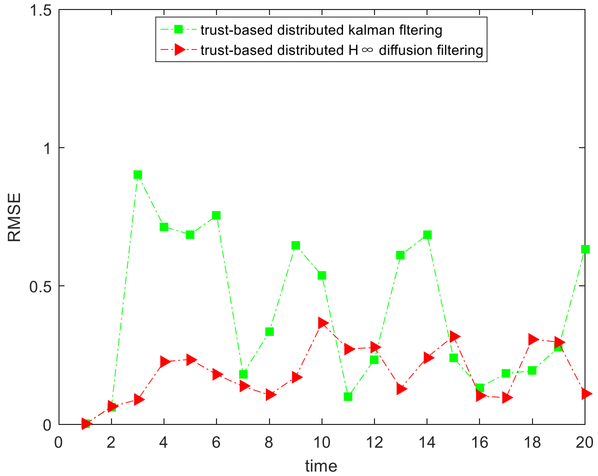

FIGURE 10. The RMSE for trust-based distributed Kalman filtering and the proposed method under FDI attacks.

V. CONCLUSION

This paper presents a trust-based distributed $H\infty$ diffusion filtering method for target tracking in the WSN under cyber attacks. Robust distributed $H\infty$ filtering equations are given for state estimation. The K-means-based trust set extracting algorithm can cluster and determine the unattacked nodes' state data. Furthermore, local data of trust is fused by the diffusion-based strategy that computes the optimal fusion weights. Finally, under Dos attacks and three deception attacks, including random, replay, and FDI attacks, the tracking performance of the proposed method is in comparison with that of trust-based distributed Kalman filtering through simulation experiments. The results show that the proposed trust-based distributed $H\infty$ diffusion filtering is more resilient to cyber attacks than trust-based distributed Kalman filtering. In the future, more perfect and intelligent clustering algorithms and distributed fusion strategies will be further considered and introduced to tackle similar challenges.

REFERENCES

[1] H. Chen, Q. Shi, R. Tan, H. V. Poor, and K. Sezaki, "Mobile element assisted cooperative localization for wireless sensor networks with obstacles," *IEEE Trans. Wireless Commun.*, vol. 9, no. 3, pp. 956–963, Mar. 2010.

[2] J. Yuan, J. Zhang, S. Ding, and X. Dong, "Cooperative localization for disconnected sensor networks and a mobile robot in friendly environments," *Inf. Fusion*, vol. 37, pp. 22–36, Sep. 2017.

[3] H. Hur and H. S. Ahn, "Discrete-time H_∞ filtering for mobile robot localization using wireless sensor network," *IEEE Sensors J.*, vol. 13, no. 1, pp. 245–252, Jan. 2013.

[4] H. Zhu, H. Wu, and M. Luo, "Environmentally adaptive event-driven robust cubature Kalman filter for RSS-based targets tracking in mobile wireless sensor network," *IEEE Internet Things J.*, vol. 10, no. 6, pp. 5530–5542, Mar. 2023.

[5] C. Zhang, J. Qin, H. Li, Y. Wang, S. Wang, and W. X. Zheng, "Consensus-based distributed two-target tracking over wireless sensor networks," *Automatica*, vol. 146, Dec. 2022, Art. no. 110593.

[6] H. Zhu, J. Luo, M. Luo, and J. Minane, "A recursive robust set-membership estimator for WSN-assisted moving targets tracking with UBB anchor location uncertainty," *IEEE Trans. Veh. Technol.*, vol. 72, no. 5, pp. 6547–6557, May 2023.

[7] H. Zhu and M. Luo, "Hybrid robust sequential fusion estimation for WSN-assisted moving-target localization with sensor-node-position uncertainty," *IEEE Trans. Instrum. Meas.*, vol. 69, no. 9, pp. 6499–6508, Sep. 2020.

[8] H. Zhu, H. Chen, and M. Luo, "Adaptive event-driven robust set-membership estimation for received-signal-strength-based moving targets localization," *IEEE Internet Things J.*, vol. 9, no. 14, pp. 12825–12835, Jul. 2022.

[9] S. Feng, H. Shi, L. Huang, S. Shen, S. Yu, H. Peng, and C. Wu, "Unknown hostile environment-oriented autonomous WSN deployment using a mobile robot," *J. Netw. Comput. Appl.*, vol. 182, May 2021, Art. no. 103053.

[10] X. Ge, Q.-L. Han, M. Zhong, and X.-M. Zhang, "Distributed Krein space-based attack detection over sensor networks under deception attacks," *Automatica*, vol. 109, Nov. 2019, Art. no. 108557.

[11] S. He, H.-S. Shin, S. Xu, and A. Tsourdos, "Distributed estimation over a low-cost sensor network: A review of state-of-the-art," *Inf. Fusion*, vol. 54, pp. 21–43, Feb. 2020.

[12] R. Olfati-Saber, "Distributed Kalman filtering for sensor networks," in *Proc. 46th IEEE Conf. Decis. Control*, Dec. 2007, pp. 5492–5498, doi: 10.1109/CDC.2007.4434303.

[13] M. Coates, "Distributed particle filters for sensor networks," in *Proc. 3rd Int. Symp. Inf. Process. Sensor Netw.*, Berkeley, CA, USA, Apr. 2004, pp. 99–107, doi: 10.1145/984622.984637.

[14] B. Shen, Z. Wang, and G. Chesi, "Distributed H_∞ filtering for polynomial nonlinear stochastic systems in sensor networks," *IEEE Trans. Ind. Electron.*, vol. 58, no. 5, pp. 1971–1979, May 2011.

[15] H. Yu, Y. Zhuang, and W. Wang, "Distributed H_∞ filtering in sensor networks with randomly occurred missing measurements and communication link failures," *Inf. Sci.*, vol. 222, pp. 424–438, Feb. 2013.

[16] T. Zhang, F. Deng, and W. Zhang, "Robust H_∞ filtering for nonlinear discrete-time stochastic systems," *Automatica*, vol. 123, Jan. 2021, Art. no. 109343.

[17] H. Yan, F. Qian, F. Yang, and H. Shi, "H_∞ filtering for nonlinear networked systems with randomly occurring distributed delays, missing measurements and sensor saturation," *Inf. Sci.*, vols. 370–371, pp. 772–782, Nov. 2016.

[18] F. Han, G. Wei, Y. Song, and W. Li, "Distributed H_∞-consensus filtering for piecewise discrete-time linear systems," *J. Franklin Inst.*, vol. 352, no. 5, pp. 2029–2046, May 2015.

[19] B. Shen, Z. Wang, and Y. S. Hung, "Distributed H_∞-consensus filtering in sensor networks with multiple missing measurements: The finite-horizon case," *Automatica*, vol. 46, no. 10, pp. 1682–1688, Oct. 2010.

[20] M. A. Abooshahab and M. Hovd, "Distributed H_∞ filtering for linear and nonlinear systems," in *Proc. IEEE Conf. Control Technol. Appl. (CCTA)*, San Diego, CA, USA, Aug. 2021, pp. 685–692.

[21] O. A. Osanaiye, A. S. Alfa, and G. P. Hancke, "Denial of service defence for resource availability in wireless sensor networks," *IEEE Access*, vol. 6, pp. 6975–7004, 2018.

[22] D. Ding, Q.-L. Han, X. Ge, and J. Wang, "Secure state estimation and control of cyber-physical systems: A survey," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 1, pp. 176–190, Jan. 2021.

[23] A. Mustafa, M. Mazouchi, and H. Modares, "Secure event-triggered distributed Kalman filters for state estimation over wireless sensor networks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 53, no. 2, pp. 1268–1283, Feb. 2023.

[24] L. Hu, Z. Wang, Q.-L. Han, and X. Liu, "State estimation under false data injection attacks: Security analysis and system protection," *Automatica*, vol. 87, pp. 176–183, Jan. 2018.

[25] M. Zhu and S. Martínez, "On the performance analysis of resilient networked control systems under replay attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 3, pp. 804–808, Mar. 2014.

[26] C. Liang, F. Wen, and Z. Wang, "Trust-based distributed Kalman filtering for target tracking under malicious cyber attacks," *Inf. Fusion*, vol. 46, pp. 44–50, Mar. 2019.

[27] H. Wu, H. Zhu, X. Li, and M. Joel Villier Amuri, "Trust-based distributed set-membership filtering for target tracking under network attacks," *IEEE Access*, vol. 11, pp. 84468–84474, 2023.

[28] R. Gao and G.-H. Yang, "Distributed multi-rate sampled-data H_∞ consensus filtering for cyber-physical systems under denial-of-service attacks," *Inf. Sci.*, vol. 587, pp. 607–625, Mar. 2022.

[29] L. Zhang and S. Sun, "Distributed H_∞ fusion filtering for multi-sensor networked systems with DoS attacks and sensor saturations," *Digit. Signal Process.*, vol. 134, Apr. 2023, Art. no. 103908.

[30] C. Gong, G. Zhu, P. Shi, and R. K. Agarwal, "Asynchronous distributed finite-time H_∞ filtering in sensor networks with hidden Markovian switching and two-channel stochastic attack," *IEEE Trans. Cybern.*, vol. 52, no. 3, pp. 1502–1514, Mar. 2022.

[31] J. Liu, Y. Gu, J. Cao, and S. Fei, "Distributed event-triggered H_∞ filtering over sensor networks with sensor saturations and cyber-attacks," *ISA Trans.*, vol. 81, pp. 63–75, Oct. 2018.

[32] X.-M. Shen and L. Deng, "Game theory approach to discrete H_∞ filter design," *IEEE Trans. Signal Process.*, vol. 45, no. 4, pp. 1092–1095, Apr. 1997.

[33] K. P. Sinaga and M.-S. Yang, "Unsupervised k-means clustering algorithm," *IEEE Access*, vol. 8, pp. 80716–80727, 2020.

[34] F. S. Cattivelli and A. H. Sayed, "Diffusion strategies for distributed Kalman filtering and smoothing," *IEEE Trans. Autom. Control*, vol. 55, no. 9, pp. 2069–2084, Sep. 2010.

YANSHEN GAO received the B.Eng. degree in automation from the Anhui University of Science and Technology, in 2022, where he is currently pursuing the M.Eng. degree with the School of Electrical and Information Engineering. His current research interests include intelligent robotics and information fusion.

HONGBO ZHU received the Ph.D. degree in control science and engineering from the University of Science and Technology of China, in 2017. He has been with the Anhui University of Science and Technology, since 2017, where he is currently an Associate Professor with the School of Electrical and Information Engineering. His current research interests include WSNs-assisted mobile robot localization, biped robots, and information fusion.

XUEYANG LI received the M.S. degree from Liaoning Shihua University, in 2012, and the Ph.D. degree from the Institute of Cyber-Systems and Control, Zhejiang University, Hangzhou, China. He is currently a Lecturer with the School of Electrical and Information Engineering, Anhui University of Science and Technology, Huainan, China. His current research interests include finite-time stability and stabilization, input-output finite-time stability and stabilization, switched systems, time-delay systems, and distributed parameter systems.

MINANE JOEL VILLIER AMURI received the B.Eng. degree in electrical engineering from Shijiazhuang Tiedao University, Shijiazhuang, China, in 2021. He is currently pursuing the M.Eng. degree with the Anhui University of Science and Technology, Huainan, China. His current research interests include information fusion, cyber-physical systems, and WSNs-assisted mobile robot localization.