IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 7 July 2023, accepted 1 August 2023, date of publication 7 August 2023, date of current version 15 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3303203

RESEARCH ARTICLE

Trust-Based Distributed Set-Membership Filtering for Target Tracking Under Network Attacks

HAIBO WU, 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 Natural Science Foundation of China under Grant 62003001, in part by the Anhui Provincial Natural Science Foundation under Grant 2008085QF298, and in part by the Open Research Grant of Joint National-Local Engineering Research Centre for Safe and Precise Coal Mining under Grant 2022KLMI01.

ABSTRACT For target tracking problems in wireless sensor networks subject to malicious network attacks, this paper proposes a distributed set-membership filtering algorithm based on trust dynamic combination strategy. The algorithm has a prediction-correction recursive updating structure similar to Kalman filtering, by introducing the clustering fusion step of received data from other nodes between the prediction step and the measurement correction update step, the clustering fusion step uses K-means to cluster and classify the data of trusted and untrusted nodes, the target state is updated by the fusion of trusted received data set, to improve the resistance to various wicked network attacks. Simulation results show that compared with the traditional distributed set-membership filtering method, the proposed method has better target tracking performance in the face of wicked network attacks such as random attacks, false data injection, replay attacks, and hybrid attacks.

INDEX TERMS Distributed set-membership filter, information fusion, network attack, target tracking, wireless sensor networks.

I. INTRODUCTION

Wireless Sensor Network (WSN) consists of a large number of sensor nodes with low power consumption and limited computing resources, these nodes use their self-organizing capabilities to form a small network for data collection, processing, and transmission [1]. Due to its free network construction mode and flexible network topology [2], wireless sensor nodes can flexibly reconstruct the network to deal with sub-network faults, which is widely used in target tracking [3], smart grid [4], automatic vehicle navigation [5], environment detection [6] and other fields. For example, target security detecting and tracking in the large-scale WSNs are challenging problems [7]. Set-membership filtering (SMF) is one of the important methods for processing the target tracking of scattered nodes in the large-scale WSN [8]. It only requires the boundary of the noise without knowing the statistical properties of the noise, and has proved advantageous in improving the robustness against the uncertainty or noise [9].

Target tracking is one of the important applications of wireless sensor networks. It is a process of estimation and prediction of target position, speed, direction and other related information by using sensor observation and data processing. Here, we are concerned with distributed set-membership filtering algorithms for target tracking, where each node only exchanges local estimates with its single-hop neighbors. In the problem of target tracking and positioning [10], some algorithms based on statistical assumptions (such as Kalman-type algorithm) can degrade the estimation performance when the prior distribution of noise is not accurate enough or unknown. Since there is no requirement for accurate noise distribution but just for boundedness of noise in distributed set-membership filtering, it is a better alternative. In [11], a new distributed set-membership filter with coding–decoding communication strategy is proposed to regulate the data transmission between the individual nodes. Before transmission, the data is converted into a

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

TABLE 1. Different distributed KF (Kalman filtering) technology under the network attack.

Algorithm	Fusion Level	Combiner	Model	Random	Replay	FDI	Hybrid
[22]	High	Static	Stochastic	×	×	×	×
[23]	High	Dynamic	Stochastic	√	×	×	×
[24]	Low and High	Dynamic	Stochastic	√	×	×	×
[25]	High	Dynamic	Stochastic	√	×	×	×
[19]	High	Dynamic	Stochastic	√	√	√	×
Proposed	High	Dynamic	Deterministic	√	√	√	√

limited set of raw data according to the corresponding coding rules to reduce the communication frequency. In [12], a new recursive distributed set-membership filter is proposed to improve the filter performance by using the precise estimation of the Lagrange remainder. In [13], a new distributed set-membership filtering algorithm with dynamic event-triggered transmission scheme (ETS) is proposed to reduce the energy consumption of WSN.

Although many distributed set-membership filter algorithms for target tracking have been proposed from the aspects of energy saving, bandwidth and communication overload [14], [15], [16], but the security of target tracking is rarely considered [17], [18]. Because the sensor network is deployed in an externally accessible environment and uses wireless communication to transmit information, the sensor nodes are vulnerable to external intrusions in the process of transmitting information, which leads to information leakage and damage. Recently, [19] proposed a method to combine multi-agent filtering algorithm with trust metrics, security is improved by establishing trust relationships between different agents. In the trust-based scheme, each agent associates trusted metrics with its neighbors, while the untrusted nodes are ignored. This scheme needs to manually determine the threshold, and as such without adequate robustification against complex or various network attacks.

To solve this problem, this paper presents a new trust-based distributed set-membership filtering method with adequate robustification against various or complex network attacks. In order to identify the attacked nodes, the K-means algorithm is introduced into the distributed set-membership filtering process. When the attacked nodes do not exceed half of all nodes, the attacked nodes can be accurately identified. In Table 1, this paper gives different distributed technology in the fusion level, combiner, and briefly compared model.

This article mainly has the following contributions:

1) This paper proposed a trust-based distributed set-membership filtering method to deal with the target tracking problem under malicious network attacks. The clustering algorithm is used to identify the attacked nodes.
2) The trust-based model can deal with a variety of network attacks, and there is no need to build different models for different attack patterns. It only needs assumption that the number of attacked nodes does not exceed half of the whole network.
3) The communication load of the proposed method is lower than that of low-level measurement fusion schemes. In addition, this method can also detect and locate damaged nodes.

The rest of the structure of this article is divided into four parts. The problem formulation is provided in Section II. In Section III, the trust-based distributed ellipsoid set-membership filtering is designed and developed. In Section IV, the numerical simulation results are given. The conclusion is given in Section V.

II. PROBLEM FORMULATION

The ellipsoid set-membership filtering is similar to the Kalman filtering in form, which is also divided into prediction step and measurement correction update step. The ellipsoid set-membership filtering model assumes that the current state x_r of the system is evolved from the state x_{r-1} at the last time according to the linear equations as follows:

$$x_r = F_{r-1}x_{r-1} + w_{r-1} \tag{1}$$

$$z_r = H_r x_r + v_r \tag{2}$$

where x_r and z_r are the state vector and measurement vector respectively. F_{r-1} is the state transition matrix, H_r is the measurement matrix; w_{r-1} and v_r are unknown but bounded (UBB) process noise and measurement noise respectively. For distributed ellipsoid set-membership filtering, the measurement model is defined similarly. For sensor node n, its measurement model is given as follows:

$$z_{n,r} = H_{n,r}x_{n,r} + v_{n,r} \tag{3}$$

where $\boldsymbol{H_{n,r}}$ is the measurement matrix. $\boldsymbol{v_{n,r}}$ is UBB measurement noise of sensor node $\boldsymbol{n}$.

Assume that the noise is UBB and belongs to the set of ellipsoids:

$$W_r = \left\{ w_r : w_r^T Q_r^{-1} w_r \le 1 \right\} \tag{4}$$

$$V_{n,r} = \left\{ v_{n,r} : v_{n,r}^T R_{n,r}^{-1} v_{n,r} \le 1 \right\} \tag{5}$$

where $\boldsymbol{Q_r}$ and $\boldsymbol{R_{n,r}}$ are given positive definite matrices. The initial state $\boldsymbol{x_0}$ and its estimate $\hat{x}_{\boldsymbol{n},\boldsymbol{0}}$ belongs to the following ellipsoid

$$E_0 = \left\{ x_0 : \left(x_0 - \hat{x}_{n,0}\right)^T P_0^{-1} \left(x_0 - \hat{x}_{n,0}\right) \le 1 \right\} \tag{6}$$

where P_0 is a positive definite matrix that describes the shape and direction of the ellipsoid. The ellipsoid set at time r-1 is given as follows:

$$E_{r-1} = \left\{ \begin{array}{l} x_{r-1} : \left(x_{r-1} - \hat{x}_{n,r-1}\right)^T P_{r-1}^{-1} \\ \times \left(x_{r-1} - \hat{x}_{n,r-1}\right) \le 1 \end{array} \right\}. \tag{7}$$

The predicted ellipsoid set $E_{r|r-1}$ is:

$$E_{r|r-1} = \left\{ \begin{array}{l} F_{r-1}x_{r-1} + w_{r-1} : \\ x_{r-1} \in E_{r-1}, w_{r-1} \in W_{r-1} \end{array} \right\} \tag{8}$$

and the measurement ellipsoid set is:

$$S_{n,r} = \left\{ \begin{array}{l} x_{n,r} : \left(z_{n,r} - H_{n,r}x_{n,r}\right)^T R_{n,r}^{-1} \\ \times \left(z_{n,r} - H_{n,r}x_{n,r}\right) \le 1 \end{array} \right\}. \tag{9}$$

Then, the posterior ellipsoid E_r is the intersection of the predicted ellipsoid set and the measurement ellipsoid set:

$$E_r = S_{n,r} \cap E_{r|r-1}. \tag{10}$$

As shown in Fig 1, this paper considers target tracking based on distributed set-membership filtering in WSN with attacked nodes. The attacked node broadcasts inaccurate or incorrect estimates. Assuming that no more than half of the nodes are attacked, this paper considers the following network attacks:

1) *Random Attack:* Attackers attack WSN nodes and can attack nodes at any time.
2) *False Data Injection Attack:* The attacker can bypass the bad data detection technique of the system and send the false data to the system without being detected.
3) *Replay Attack:* The attacker intercepts packets broadcasted by wireless sensor nodes, which contain measured values and sends them again at some later time to fool the system.
4) *Hybrid Attack:* The attacker uses the combination of the above three attacks to attack the nodes.

Remark: Formula (8) is the ellipsoid set of system model prediction for the tracking target, and formula (9) is the measurement ellipsoid set of the sensor nodes for the tracking target position. Formula (10) is the intersection of prediction ellipsoid set and measurement ellipsoid set, which is more accurate for tracking target position than prediction ellipsoid set or estimation ellipsoid set.

III. TRUST-BASED DIFFUSION ELLIPSOID SET-MEMBERSHIP FILTERING

A. MEASUREMENT-UPDATE

According to the posterior ellipsoid set (10), the center and shape of ellipsoid are as follows:

$$\hat{x}_{n,r} = \hat{x}_{r|r-1} + K_{n,r}\left(z_{n,r} - H_{n,r}\hat{x}_{r|r-1}\right) \tag{11}$$

$$K_{n,r} = \hat{P}_{r|r-1}H_{n,r}^T \left(\frac{H_{n,r}\hat{P}_{r|r-1}H_{n,r}^T}{1-\rho_{n,r}} + \frac{R_{n,r}}{\rho_{n,r}} \right)^{-1} \tag{12}$$

$$\hat{P}_{n,r} = \frac{\hat{P}_{r|r-1}}{1-\rho_{n,r}} \left(I - \frac{K_{n,r}H_{n,r}}{1-\rho_{n,r}} \right). \tag{13}$$

According to the minimum trace principle, the optimal value of $\rho_{n,r}$ is as follows:

$$\rho_{n,r} = \frac{\sqrt{r}_m}{\sqrt{\gamma}_m + \sqrt{r}_m} \tag{14}$$

where r_m and γ_m are the maximum singular values of the matrices $H_{n,r}\hat{P}_{r|r-1}H_{n,r}^T$ and $R_{n,r}$, respectively.

Let's ℓ_n be the single-hop neighbors of node n and includes itself. The center of the ellipsoid $\hat{x}_{n,r}$ and the shape $\hat{P}_{n,r}$ are exchanged in ℓ_n.

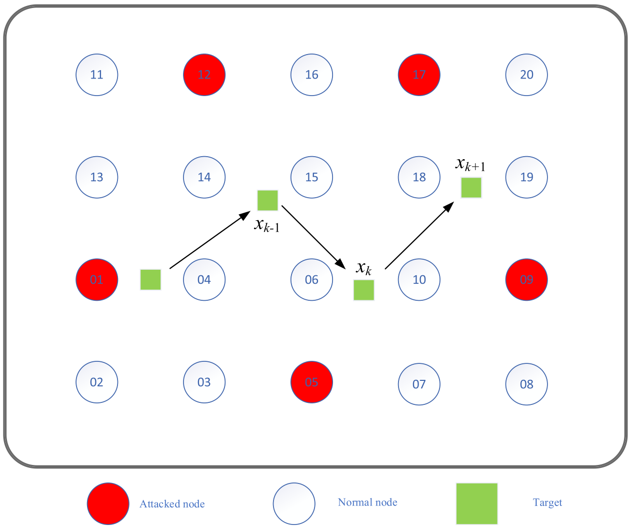


FIGURE 1. The wireless sensor network is attacked in target tracking.

B. TRUST-BASED CLUSTERING FUSION

Combinators play an important role in node data fusion, which determines the overall network performance [20]. Compared with the unified scheme, the trust-based distributed ellipsoid set-membership filter can better assign weights. For untrusted nodes, their weights will be very low and will be ignored in the fusion process, which realizes the effective discrimination of information. The algorithm only needs to be performed on the local node [21].

K-means is one of the outstanding representatives of unsupervised learning algorithm. The principle of K-means is relatively simple, the convergence speed is fast, and the clustering effect is good. In this paper, a clustering algorithm is used to classify WSN nodes, and the cluster containing the most elements is considered as the trusted cluster. The basic idea is to find K clusters through iteration to minimize the loss function corresponding to the clustering result.

For node n, our goal is to classify the ellipsoidal center data in the communication node $\{x_i, i \in \ell_n\}$, where the loss function is defined as the sum of distance error squares from the sample to the center of cluster:

$$J\left(c, \mu\right) = \sum\nolimits_{i=1}^{M} ||x_i - \mu_r||^2 \tag{15}$$

where x_i represents the i sample, μ_r represents the centroids corresponding to the cluster, and M is the total number of ellipsoidal centers or ellipsoidal shapes.

K-means assignments and updates the data to collect the data closer to the cluster center. In the assignment step, each data sample will be randomly assigned to the nearest clustering center:

Assignment step: The center x_i of the ellipsoid is randomly assigned to either μ_1 or μ_2 as follows.

$$\mathrm{c} = \arg\min\nolimits_{\mathrm{r}} ||x_i - \mu_r||^2, \quad \mathrm{r} = 1, 2. \tag{16}$$

Let τ_r^i be the index describing the ellipsoid center x_i near μ_r, if μ_r is closer to the center of the ellipsoid, let $\tau_r^i = 1$, otherwise $\tau_r^i = 0$.

Update step: For each class center μ_r, recalculate the center of the class:

$$\mu_r = \frac{\sum \tau_r^i x_i}{\tau_r^i}, \quad r = 1, 2. \tag{17}$$

Through the iteration of the assignment steps and the update step until J converges. Let $\delta_r = \sum \tau_r^i$ be the number of elements in the cluster, and

$$c_i = argmax_r \delta_r, \quad r = 1, 2. \tag{18}$$

Only the data in c_i is considered to be trusted data, where the corresponding node is $\mathbb{C}_k$. Let card$(\mathbb{C}_k)$ describes the number of elements in the set $\mathbb{C}_k$ and untrusted nodes are ignored.

The weight is calculated as follows:

$$\mathcal{L}_{k \leftarrow m,r} = \frac{1}{card(\mathbb{C}_i)}, \quad m \in \mathbb{C}_k. \tag{19}$$

Let $P_{n,r} = diag\{P_{n,r}\}$, where the operator $diag\{\cdot\}$ returns the main diagonal element of the $P_{n,r}$ matrix. At node n, its ellipsoid shape matrix is placed in two clusters like the ellipsoid center, where the set of trusted nodes is $\mathbb{D}_k$, and the untrusted nodes are ignored.

The weight is calculated as follows:

$$\mathcal{g}_{k \leftarrow l,r} = \frac{1}{card\left(\mathbb{D}_k\right)}, \quad l \in \mathbb{D}_k. \tag{20}$$

Refined center of the ellipsoid and shape are given as follows:

$$\hat{x}_r = \sum\nolimits_{m \in \mathbb{C}_k} \mathcal{L}_{\mathrm{k} \leftarrow m,r} \hat{x}_{m,r} \tag{21}$$

$$\hat{P}_r = \sum\nolimits_{l \in \mathbb{D}_k} \mathcal{g}_{k \leftarrow 1,\mathrm{r}} \hat{P}_{m,r}. \tag{22}$$

It should be noted that if the number of nodes spreading false information is greater than half of the total network nodes, negative effects will still occur in the information fusion step. Therefore, it is necessary to ensure that at least half of the network nodes are in normal working state to reduce the impact of untrusted data on the system during information fusion. Algorithm 1 shows the detailed process of trust-based distributed set-membership filtering.

C. TIME-UPDATE

According to the predicted ellipsoid set (9), the center and shape of ellipsoid are as follows:

$$\hat{x}_{r+1|r} = F_{r-1}\hat{x}_r \tag{23}$$

$$\hat{P}_{r+1|r} = F_r \frac{\hat{P}_r}{1 - p_{r+1}} F_r^T + \frac{Q_{r+1}}{p_{r+1}}. \tag{24}$$

The predicted minimum trajectory state ellipsoid obtained by optimizing the parameter p_{r+1} according to the minimum trace principle is given as follows:

$$p_{r+1} = arg \min_{p_{r+1 \in (0,1)}} tr\left(\hat{P}_{r+1|r}\right). \tag{25}$$

The optimal selection of p_{r+1} is given as follows:

$$p_{r+1} = \frac{\sqrt{tr\left(Q_{r+1}\right)}}{\sqrt{tr(F_r \hat{P}_r F_r^T) + \sqrt{tr\left(Q_{r+1}\right)}}}. \tag{26}$$

IV. NUMERICAL SIMULATION RESULTS

The numerical simulation experiments show that the scheme has lower root mean square error (RMSE) in the face of network attacks. In simulation a fully connected WSN consisting of 09 nodes, as shown in Fig 2, where nodes 02, 05 and 09 are under network attack, is considered. For simplicity, $F_{n,r}$ and $H_{n,r}$ are set to be same. The ellipsoidal initialization center $\hat{x}_{n,0|-1}$ and shape $\hat{P}_{n,0|-1}$ are given in Algorithm 1. The Kalman filter algorithm has the same initial value. And the parameters are set as follows:

$$F_r = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad H_r = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$Q = \begin{bmatrix} 10 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 10 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad R = \begin{bmatrix} 0.8 & 0 & 0 & 0 \\ 0 & 0.5 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}.$$

A. RANDOM ATTACK

Random attacks can be launched at any time or place, using random data to launch attacks on sensor nodes. The actual trajectory, trust-based fusion trajectory, attacked node trajectory and Kalman filter trajectory are given in Fig 3, and Fig 4 shows the corresponding RMSE performance. Compared with the unified fusion scheme, the trust-based fusion scheme has better performance. The reason is that the untrusted nodes are ignored and only trusted nodes participate in the fusion

Algorithm 1 Trust-Based Distributed Set-Membership Filter

```
Initial state estimate $\hat{x}_{n,0|-1} = \left[20\ \ 20\ \ 20\ \ 20\right]^T$, and
shape $\hat{P}_{n,0|-1} = 40I_4$, where $I_n$ is denoted as the identity
matrix of size $n$, for $n = 1,2\ldots N$.
For $r = 0$ to $r_{max}$
  for $n = 1$ to $N$ do
    //measurement update
    The ellipsoid center and ellipsoid shape were
    calculated:
      $\hat{x}_{n,r} = \hat{x}_{r|r-1} + K_r(z_{n,r} - H_{n,r}x_{r|r-1})$
      $\hat{P}_{n,r} = \frac{\hat{P}_{r|r-1}}{1-\rho_{n,r}}\left(I - \frac{K_{n,r}H_{n,r}}{1-\rho_{n,r}}\right).$
    Exchange $\hat{x}_{k,r}$ and $\hat{P}_{k,r}$ at node $n$, $k \in \ell_n$.
    // information fusion
    Compute $\mathcal{L}_{k,r}$ and $g_{k,r}$ by the formula:
      $\mathcal{L}_{k\leftarrow m,r} = \frac{1}{card(\mathbb{C}_k)}, m \in \mathbb{C}_k$
      $\mathcal{G}_{k\leftarrow l,r} = \frac{1}{card(\mathbb{D}_k)}, l \in \mathbb{D}_k.$
    Trust-based ellipsoid centers and shapes:
      $\hat{x}_r = \sum_{m\in\mathbb{C}_k} \mathcal{L}_{k\leftarrow m,r}\hat{x}_{m,r}$
      $\hat{P}_r = \sum_{l\in\mathbb{D}_k} g_{k\leftarrow l,r}\hat{P}_{m,r}.$
    // time update
      $\hat{x}_{r+1|r} = F_r\hat{x}_r$
      $\hat{P}_{r+1|r} = F_r\frac{\hat{P}_r}{1-p_{r+1}}F_r^T + \frac{Q_{r+1}}{p_{r+1}}.$
  end
End
```

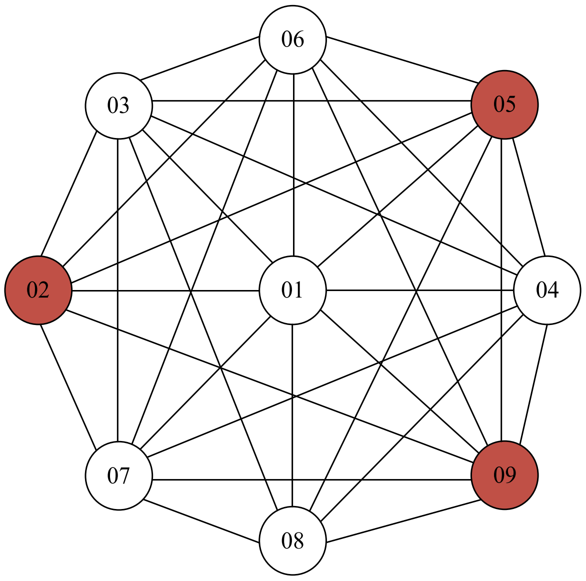


FIGURE 2. The fully connected WSN consists of 9 nodes, among which nodes 02, 05, and 09 are attacked.

step. It has good robustness to random attacks and can achieve low RMSE.

B. FALSE DATA INJECTION ATTACK

In FDI, it is considered that the attacker knows the model and parameters of the system. Attackers can evade the system's detection techniques, tamper with the real data $\hat{x}_{n,r}$

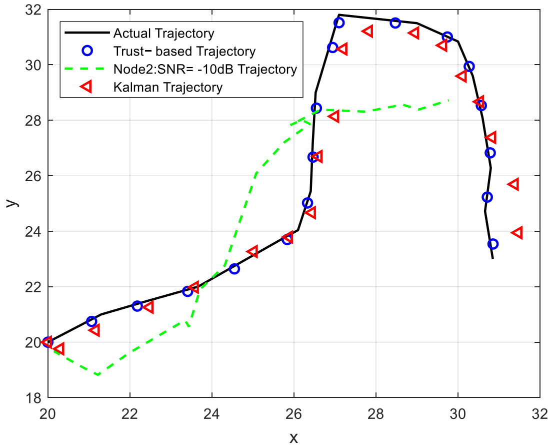


FIGURE 3. Comparison of real trajectory, fused trajectory based on trust-based schemes, and Kalman filter trajectory where 02 node is under random attack.

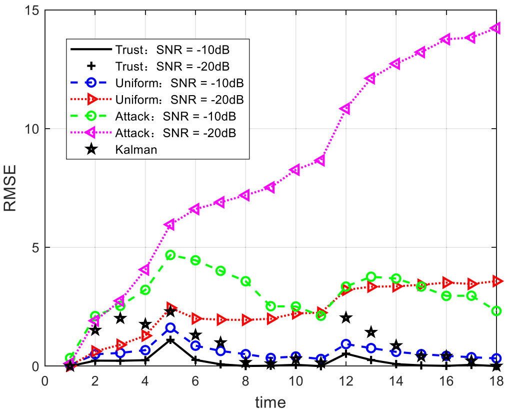


FIGURE 4. Compare RMSE of different schemes under random attack.

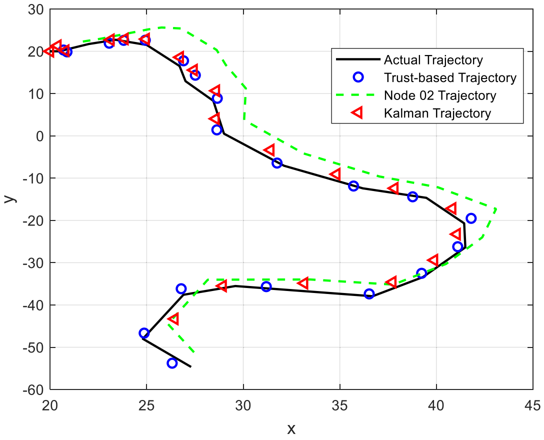


FIGURE 5. Comparison of real trajectory, fused trajectory based on trust-based schemes, and Kalman filter trajectory where 02 node is under FDI attack.

of the system. In the simulation, the actual trajectory, trust-based fusion trajectory, attacked node trajectory and Kalman filter trajectory are given in Fig 5, and its corresponding RMSE performance is shown in Fig 6. Compared with the traditional distributed set-membership filter and Kalman filter, the trust-based scheme has better performance. Because it directly ignores the fake data of the attacked node and

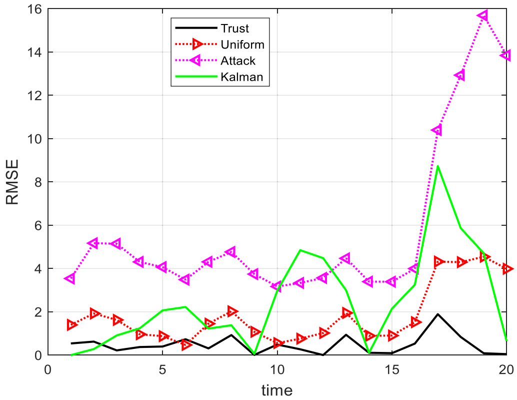


FIGURE 6. Compare RMSE of different schemes under FDI attack.

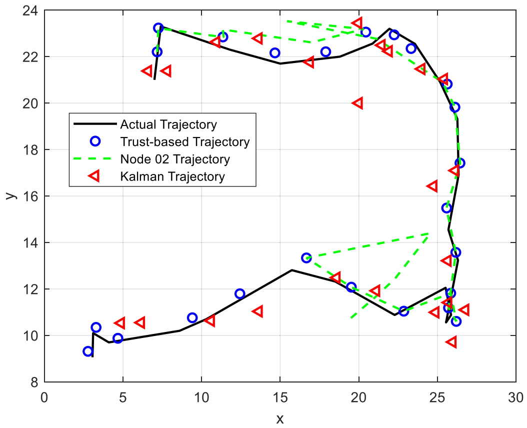


FIGURE 7. Comparison of real trajectory and fused trajectory based on trust-based schemes, and Kalman filter trajectory where three nodes are replay attack.

only integrates the data of the trusted node, it has strong robustness.

C. REPLAY ATTACK

In the simulation of this type of attack, it is considered that the attacker may grab the data transmitted by the system and use it to attack the system. Because the attacked data is the real state of the system in the past, it can bypass the widely used defect detection technology based on residual error. The attack is launched at moment t for nodes 02, 05, and 09 with $\hat{x}_{t-T}$, $T = 4, 7$, for a short attack and $T = 20$ for a long attack. The attacker propagates error messages to the neighboring nodes of the three nodes, for which the true and trust-based trajectories of the attack and the trajectory of node 02 are given in Fig 7. Its corresponding RMSE is given in Fig 8. Compared with the traditional Kalman filter, the trust-based scheme is more robust.

D. HYBRID ATTACK

In the hybrid attack, the attacker uses the above three attack methods to launch attacks on different nodes. For nodes 02, 05, and 09 replay attack at time t, $\hat{x}_{t-T}$, $T = 4, 7, 14$. The attacker propagates false information to the neighboring nodes of the three nodes under attack. Its true trajectory, trust-based trajectory and Kalman trajectory are given in Fig. 9.

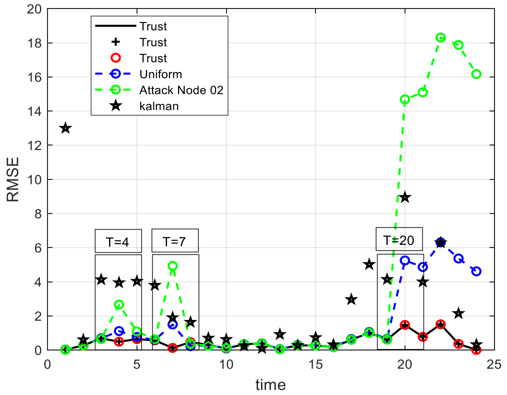


FIGURE 8. Compare RMSE of different schemes under replay attack.

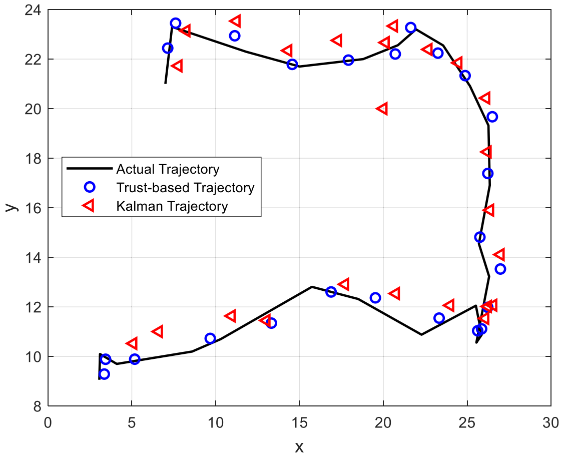


FIGURE 9. Comparison of real trajectory and fused trajectory based on trust-based schemes, and Kalman filter trajectory where three nodes are hybrid attack.

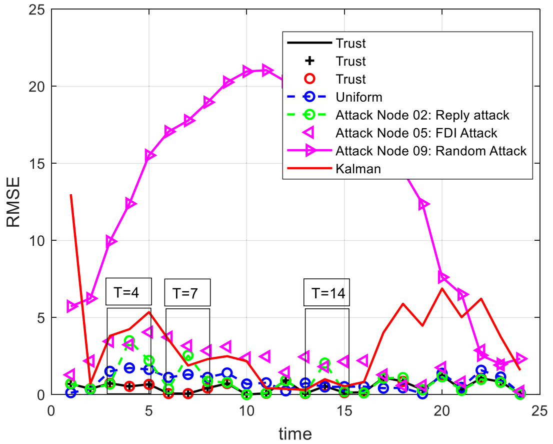


FIGURE 10. Compare RMSE of different schemes under hybrid attack.

Their corresponding RMSE are given in Fig. 10. Simulation results show that compared with the traditional Kalman filter, the trust-based scheme is still robust to the hybrid attack.

V. CONCLUSION

In this paper, a trust-based distributed ellipsoidal set-membership filtering algorithm is proposed for moving target tracking subject to various malicious network attacks.

Spatial clustering scheme is introduced to improve the distributed estimation accuracy by removing the attacks-contaminated data. In the sequel of clustering, a dynamic trusted information framework is obtained. The numerical simulation results show that it is robust against various network attacks.

REFERENCES

[1] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in *Proc. 1st IEEE Int. Workshop Sensor Netw. Protocols Appl.*, Anchorage, AK, USA, Mar. 2003, pp. 113–127.

[2] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Sparse attack construction and state estimation in the smart grid: Centralized and distributed models," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1306–1318, Jul. 2013.

[3] 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.

[4] E. Fadel, V. C. Gungor, L. Nassef, N. Akkari, M. G. A. Malik, S. Almasri, and I. F. Akyildiz, "A survey on wireless sensor networks for smart grid," *Comput. Commun.*, vol. 71, pp. 22–33, Nov. 2015.

[5] H. Chu and C.-D. Wu, "A Kalman framework based mobile node localization in rough environment using wireless sensor network," *Int. J. Distrib. Sens. Netw.*, vol. 11, no. 5, 2015, Art. no. 8414462.

[6] 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.

[7] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan, "Sparse malicious false data injection attacks and defense mechanisms in smart grids," *IEEE Trans. Ind. Informat.*, vol. 11, no. 5, pp. 1–12, Oct. 2015.

[8] S. Liu, Z. Wang, G. Wei, and M. Li, "Distributed set-membership filtering for multirate systems under the round-robin scheduling over sensor networks," *IEEE Trans. Cybern.*, vol. 50, no. 5, pp. 1910–1920, May 2020.

[9] 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.

[10] M. Vazquez-Olguin, Y. S. Shmaliy, O. Ibarra-Manzano, J. Munoz-Minjares, and C. Lastre-Dominguez, "Object tracking over distributed WSNs with consensus on estimates and missing data," *IEEE Access*, vol. 7, pp. 39448–39458, 2019.

[11] L. Liu, L. Ma, J. Guo, J. Zhang, and Y. Bo, "Distributed set-membership filtering for time-varying systems: A coding–decoding-based approach," *Automatica*, vol. 129, Jul. 2021, Art. no. 109684.

[12] D. Ding, Z. Wang, and Q.-L. Han, "A set-membership approach to event-triggered filtering for general nonlinear systems over sensor networks," *IEEE Trans. Autom. Control*, vol. 65, no. 4, pp. 1792–1799, Apr. 2020.

[13] X. Ge, Q.-L. Han, and Z. Wang, "A dynamic event-triggered transmission scheme for distributed set-membership estimation over wireless sensor networks," *IEEE Trans. Cybern.*, vol. 49, no. 1, pp. 171–183, Jan. 2019.

[14] D. Zhang, P. Shi, W.-A. Zhang, and L. Yu, "Energy-efficient distributed filtering in sensor networks: A unified switched system approach," *IEEE Trans. Cybern.*, vol. 47, no. 7, pp. 1618–1629, Jul. 2017.

[15] S. Bhatti and J. Xu, "Survey of target tracking protocols using wireless sensor network," in *Proc. 5th Int. Conf. Wireless Mobile Commun.*, 2009, pp. 110–115.

[16] M. Fayyaz, "Classification of object tracking techniques in wireless sensor networks," *Wireless Sensor Netw.*, vol. 3, no. 4, pp. 121–124, 2011.

[17] A. Oracevic, S. Akbas, and S. Ozdemir, "Secure and reliable object tracking in wireless sensor networks," *Comput. Secur.*, vol. 70, pp. 307–318, Sep. 2017.

[18] A. P. Fard and M. Nabaee, "Secure tracking in sensor networks using adaptive extended Kalman filter," 2012, *arXiv:1204.3141*.

[19] I. Matei, J. S. Baras, and V. Srinivasan, "Trust-based multi-agent filtering for increased smart grid security," in *Proc. 20th Medit. Conf. Control Autom. (MED)*, Barcelona, Spain, Jul. 2012, pp. 716–721.

[20] V. Shnayder, M. Hempstead, B.-R. Chen, G. W. Allen, and M. Welsh, "Simulating the power consumption of large-scale sensor network applications," in *Proc. 2nd Int. Conf. Embedded networked sensor Syst.*, Nov. 2004, pp. 188–200.

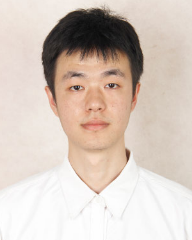
[21] H. Zhu and M. Luo, "Hybrid robust sequential fusion estimation for WSN-assisted moving-target localization with sensor-node-position uncertainty," *IEEE Trans. Instrum. Meas.*, vol. 69, no. 9, pp. 6499–6508, Sep. 2020.

[22] Y. Zhang, C. Wang, N. Li, and J. Chambers, "Diffusion Kalman filter based on local estimate exchanges," in *Proc. IEEE Int. Conf. Digit. Signal Process. (DSP)*, Singapore, Jul. 2015, pp. 828–832.

[23] G. Wang, N. Li, and Y. Zhang, "Diffusion distributed Kalman filter over sensor networks without exchanging raw measurements," *Signal Process.*, vol. 132, pp. 1–7, Mar. 2017.

[24] 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.

[25] F. Wen and W. Liu, "Diffusion least mean square algorithms with zero-attracting adaptive combiners," in *Proc. IEEE Int. Conf. Comput. Inf. Technol., Ubiquitous Comput. Commun.; Dependable, Autonomic Secure Comput.; Pervasive Intell. Comput.*, Oct. 2015, pp. 252–256.



HAIBO WU received the B.Eng. degree in electrical engineering from Anhui Xinhua University, Hefei, China, in 2021. He is currently pursuing the M.Eng. degree with the Anhui University of Science and Technology, Huainan, China. His research interests include information fusion, cyber-physical systems, and WSNs-assisted mobile robot localization.

HONGBO ZHU received the Ph.D. degree in control science and engineering from the University of Science and Technology of China, in 2017. Since 2017, he has been with the Anhui University of Science and Technology, where he is currently an Associate Professor with the School of Electrical and Information Engineering and the State Key Laboratory of Mining Response and Disaster Prevention and Control in Deep Coal Mines. His current research interests include WSNs-assisted mobile robot localization, biped robots, and information fusion.

XUEYANG LI, photograph and biography not available at the time of publication.

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 research interests include information fusion, cyber-physical systems, and WSNs-assisted mobile robot localization.