Distributed Jammer-Equipped Target Tracking with Hybrid Extended Kalman and Particle Filter in Sensor Network

Iman Maghsudlu[1], Meysam Raees Danaee[2], Hamid Arezumand[3]

1- Faculty of Electrical Engineering Department, Imam Hossein Comprehensive University, Tehran, Iran.
Email: iman.maghsudlu@gmail.com

2- Imam Hossein Comprehensive University, Tehran, Iran.
Email: mrdanaee@gmail.com, (Corresponding Author)

3- Imam Hossein Comprehensive University, Tehran, Iran.
Email: arezumand.h@ihu.ac.ir

ABSTRACT:
In this paper, we propose a distributed tracking algorithm for a jammer-equipped target that passes through the nodes of a wireless sensor network (WSN). The jammer that the target carries is of the deceptive type, which means that it can mimic the signal of the target and confuse the sensors. Unlike other existing methods, our proposed algorithm does not require any additional hardware installation on each WSN node. It only relies on signal processing and solving the average consensus problem to detect the presence of jamming effects in the observations of the contaminated nodes and exclude them from the distributed tracking problem. For the distributed tracking problem, we use the hybrid extended Kalman filter (EKF) and particle filter to reduce the number of parameters needed for solving the average consensus problem and to decrease the communication overhead. The simulation results show that our algorithm improves the tracking performance compared to the case where the nodes with jammed observations are used.

KEYWORDS: Distributed Particle Filter, Sensor Network, Multi-Sensor Target Tracking, Data Fusion, Consensus-Base Algorithms.

1. INTRODUCTION

Estimating the state vector of a target that passes through the nodes of a WSN has recently attracted attention [1]. This task can be performed either centrally (where all the sensors send their information to a central node) or distributedly (where each sensor obtains an estimate of the state vector of the target by exchanging information with its one-hop neighbors). The distributed tracking method is more preferable because the nodes do not need to know the network topology and the whole system does not fail if the central node breaks down [2]. In the nonlinear environment, particle filters have shown better results than other nonlinear filters [3]. In the following, we review different ideas that have been proposed in the field of distributed tracking. We categorize them based on the type of communication, estimation, and fusion methods used by the sensors and the fusion center.

In [4], the probability vector of particles at the location of each node is projected on a set of eigenvectors of the Laplacian matrix of the graph and then the obtained projections are averaged with the help of a consensus-based algorithm in the network to calculate the global probability vector of the network in each node. [5] proposes a method for achieving average consensus on the sufficient statistics of the target state, which are computed by using a particle filter to approximate the posterior distribution. The method is based on a distributed weighted average algorithm that allows the nodes to exchange and update their local estimates iteratively until they converge to a global estimate. In [6], a distributed particle filter for bearing-only tracking applications is proposed, based on a constrained sufficient statistic approach. The method uses local particle filters at each sensor node and computes the global sufficient statistics as a sum of the local sufficient statistics. The method reduces the communication complexity and bandwidth requirement by running average consensus algorithms only on the means of the local sufficient statistics. The method achieves near-

Paper type: Research paper
https://doi.org/10.30486/MJTD.2024./901839
Received: 29 August 2023; revised: 21 January 2024; accepted: 29 January 2024; published: 1 June 2024
How to cite this paper: I. Maghsudlu, M. Raees Danaee , H. Arezumand, **"Distributed Jammer-Equipped Target Tracking with Hybrid Extended Kalman and Particle Filter in Sensor Network"**, *Majlesi Journal of Telecommunication Devices*, Vol. 13, No. 2, pp. 87-96, 2024.

optimal performance, comparable to the centralized particle filter.

Reference [7] presents a method for distributed estimation of the target state based on a Gaussian mixture model (GMM). Each node uses a particle filter to approximate the local posterior distribution by a GMM, and then exchanges and updates the GMM parameters with its neighbors using a distributed weighted average algorithm. This results in a global GMM that represents the posterior distribution projected onto the basis functions. Each node can then compute its own estimate of the target state from the global GMM. In [8], the key idea is to use consensus algorithms to approximate the joint likelihood function of all sensors, which summarizes the measurement information. This approach is applicable if the local likelihood functions belong to the exponential family. The paper then develops distributed particle filters and distributed Gaussian particle filters based on the consensus approximation of the joint likelihood function. Each sensor runs a local (Gaussian) particle filter that computes a global state estimate. The paper also proposes a method to reduce the number of particles in the distributed Gaussian particle filter by using another consensus scheme. Despite these advances in distributed tracking, there is no suitable method for addressing and solving the problem of jamming in WSNs when the target tracking is performed in a distributed manner. Some targets have installed a hardware device on themselves that acts as a self-screening jammer to prevent WSNs from tracking them effectively [9-11].

In this paper, we aim to propose a method that can cope with such a jammer and preserve the distributed tracking performance. In [12-13] the methods of dealing with deceptive jammer in a sensor network have been investigated. This jammer can create collaborative or non-collaborative targets for network nodes. In this paper, jammer is considered a non-collaborative type. In the scenario presented by [12] to detect a collaborative jammer it is necessary to place a number of passive sensors scattered in a number of network nodes which is not always possible. In the second type of sensor network jammers, the communication links of the network nodes are disrupted and in [14-17] some algorithms are presented that can estimate the location of the jammer. To learn more about the second type of jammers, we refer the reader to the relevant literature [9-11]. Target tracking in wireless sensor networks is vulnerable to jamming attacks, which can degrade the performance of the distributed estimation algorithms and cause the target to escape detection.

In this paper, we propose a method that can identify the jammed nodes based on the disturbance in their measurements and exclude them from the consensus-based tracking algorithm. By removing the jammed nodes, we can improve the accuracy and reliability of the target tracking in the network.

In this paper, we propose an idea that if only a small portion of the sensors are contaminated by the jamming disturbances, then we can obtain the average of the observations by solving the average consensus problem. Then, since the contaminated sensors cannot change the average value, we can identify them by comparing them with the obtained average (because they are far from it). Therefore, the network can ignore their data and then solve the distributed tracking problem assuming that all the data are clean, as in the usual algorithms in this field. The advantage of this method is that, unlike the proposed methods for controlling the jamming problem in WSNs that require additional hardware installation for jamming detection, the proposed method only detects the contamination of the observations by using the solution of the average consensus problem on the received observations.

The rest of the paper is organized as follows: Section 2 formulates and states the problem. Section 3 introduces the distributed state estimation problem based on the graph theory idea. In this section, we first describe the characteristics of the jammer that the target is equipped with, and then we present the algorithm for detecting the jammed sensors by solving the average consensus problem. Section 4 presents and analyzes the simulation results. Section 5 concludes the paper.

2. PROBLEM FORMULATION

The sensor network used in this paper consists of S nodes that are scattered in an area where we want to track the jammer-equipped target. Jammer signal specifications are explained in the relevant section. This sensor network is modelled with an undirected graph G={V,E}. V is the set of all the nodes of the network and E is the set of all edges. E⊂V×V is established between these two sets. *(i,j)* is a member of this set if node *i* and *j* are connected through a communication link. $N_i = \{ j | (i, j) \in E \}$ is the set of all one-hop neighbours of node *i* where $d_i = |N|$ is called degree of node i. in each time step, each node can exchange its data with its neighbouring nodes for a specified number of iterations. $X_k = [x_k, y_k, \dot{x}_k, \dot{y}_k]^T$ is the state vector of the target that we want to track in each time step and this vector includes the position and speed of the target in two-dimensional coordinates. The target state transition model in this network is as

$$\mathbf{x}_{k+1}=\mathrm{f}(\mathbf{x}_k,\boldsymbol{\xi}_k) \qquad (1)$$

Also, the observation made of the target in node *s* and time step *k* is as

$$\mathbf{z}_k^{\mathrm{s}}=\mathrm{h}^{\mathrm{s}}(\mathbf{x}_k,\mathbf{v}_{k},,\mathbf{j}_k) \qquad (2)$$

Where $\mathbf{z}_k^s=[r_{\mathbf{z},k}^s,\theta_{\mathbf{z},k}^s]^T$ is an observation made in node s. ξ_k, $\mathbf{v}_k$ and $\mathbf{j}_k$ are noise vectors of state, observation and jamming whose covariance matrices are equal to $\mathbf{Q}_k$, $\mathbf{R}_k$ and $\mathbf{J}_k$ respectively. Observation vector $\mathbf{z}_k^s$ is as

$$\mathbf{z}_k^s=[r_{\mathbf{z},k}^s,\theta_{\mathbf{z},k}^s]^T=[r_k^s,\theta_k^s]^T+\mathbf{z}_k^n=[r_k^s,\theta_k^s]^T+[r_k^n,\theta_k^n]^T \tag{3}$$

Where r_k^s and θ_k^s are the range and angle of the target relative to the node s as (4) and (5) respectively. $\mathbf{z}_k^n$ is zero mean Gaussian noise with covariance matrix $\begin{bmatrix}\sigma_r^2 & 0\\ 0 & \sigma_\theta^2\end{bmatrix}$.

$$\mathrm{r}_\mathrm{k}^\mathrm{s}=\sqrt{(x_k\text{-}x_s)^2+(y_k\text{-}y_s)^2} \tag{4}$$

$$\theta_k^s=\mathrm{Arctan}(\frac{y_k\text{-}y_s}{x_k\text{-}x_s}) \tag{5}$$

$[x_s,y_s]^T$ and $[x_k,y_k]^T$ are coordinates of node s and target in the reference coordination system. If in (1) and (2) the functions f and h^s have a lot of nonlinear properties or if the target manoeuvre is very high, distributed particle filter will be a good choice for target tracking.

3. GRAPH-BASED DISTRIBUTED HEPF

In this paper, jammer-equipped target tracking in WSN is presented. This jammer can be a type of noise or a type of deception as what is considered here.

We consider the problem of distributed estimation of a target that is equipped with a jammer. We assume that the target can be tracked by a network of sensors, which communicate with each other using consensus-based algorithms. We propose a method to identify and exclude the sensors that are affected by the jamming signals, and thus reduce the impact of the jamming on the estimation accuracy. Moreover, we propose a hybrid approach that switches between different filters depending on the target's motion dynamics. When the target's motion is high, we use a particle filter, which can handle the nonlinearity and uncertainty of the target's state. When the target's motion is low, we use an extended Kalman filter, which is faster but less accurate than the particle filter.

Hybrid Extended Kalman Filter (HEPF) consists of a combination of particle and extended Kalman filters and can be used in distributed target tracking in a sensor network. By doing so, we can balance the trade-off between the communication overhead and the tracking speed. We compare our proposed method with the conventional methods that use only one sensor or all the sensors for tracking, and show that our method can significantly improve the performance in terms of the root mean square error (RMSE) of the target state estimation.

In the first case when the combination of these two filters is used for tracking the tracking speed will be low due to the complex calculations of the particle filter and in the second case due to the removal of the particle filters the calculation volume will be low and as a result the tracking speed will be higher. One can refer to [18] to study more details of HEPF and its related relationships. Also, the particle filter used here is a graph-based distributed particle filter the details of which are described in [4]. As can be seen in Fig. 1 a switch is considered that compares the dynamic value of the target movement with the threshold level and selects the appropriate filter. Threshold level and target dynamic value can be defined at the discretion of the designer.

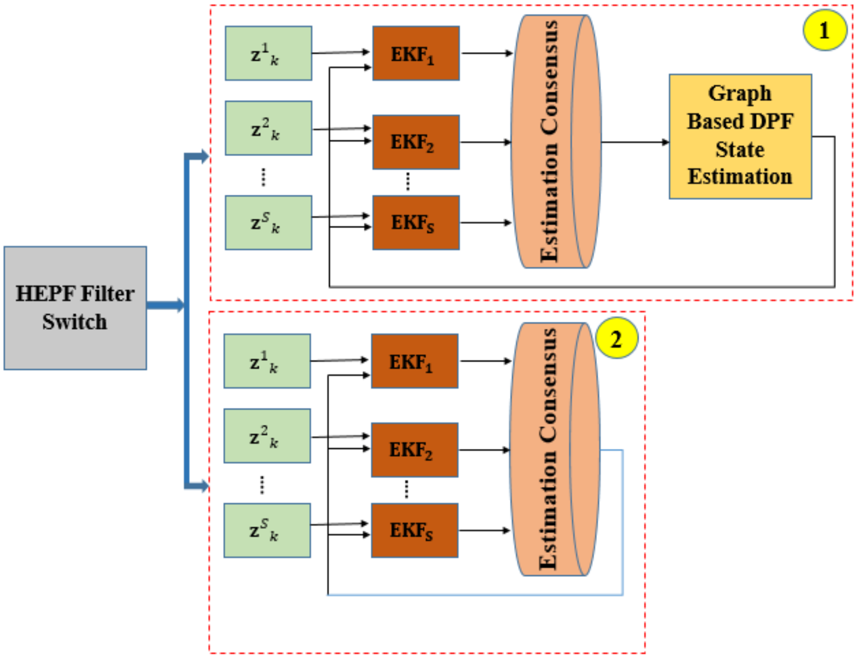

Fig. 1. Distributed HEPF in sensor network.

3.1. Target self-screening jammer

In general, jammer can be of the type of suppression or deception [19]. The target that we want to track in the sensor network is equipped with a deceptive jammer which can send the deception targets to the sensors of the network with the help of DRFM[1] technology [20]. Deception targets are of collaborative type and it means that the deception targets created for all network sensors are produced at the same location in the reference coordinates even though the location coordinates of the network nodes are different [12]. The point that seems important here is that the number of signals received by DRFM is limited, therefore after saturation of this system the deception signal does not affect the sensors located at a further distance.

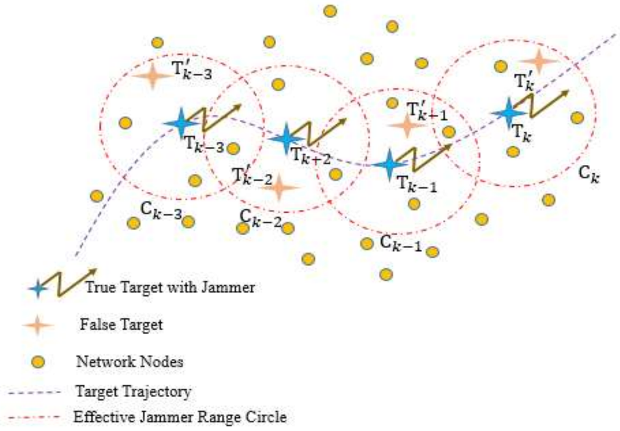

Fig. 2. Jammer effect on observation model of in-range nodes.

As can be seen in figure 2, the real target that carries a jammer and is marked with a blue star, is at the point T_k of its true path at the time step k. Jammer that is installed on the target jams all the sensors inside the hypothetical circle C_k at the time step k so all the sensors inside C_k do not see the real location of the target as can be seen in figure 4. T'_k indicates the deception target in the hypothetical circle. the nodes that are outside of C_k are not jammed and the correctness of their operation is preserved. Therefore, it can be said that at any time step k a limited number of nodes

[1] Digital Radio Frequency Memory

are jammed and their state estimations are incorrect and instead there are a much larger number of nodes that are not jammed and their state estimations are completely correct. Here we presented a method by which the network detects the jammed nodes with the help of the consensus algorithm and makes a correct distributed estimation of the target state and prevents the target tracking from diverging.

3.2. Distributed jammer detection algorithm in network sensor

Consider a situation where we have only one node to track the jammer-equipped target. This issue is shown in figure 3.

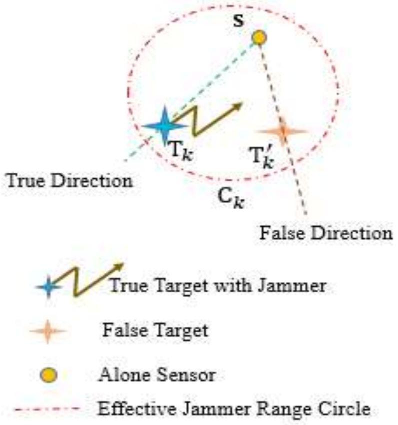

Fig. 3. Jammer-equipped target tracking with only one node.

This node determines the state of the target independently by processing the observation received from the target. Since there is no other node, it is impossible to compare the received observations with other nodes to reveal the presence of a jammer effect in the received observation signal. The main idea of this paper is to use a sensor network and define a consensus-based criterion for evaluating the presence of jamming in the observations nodes have been received by comparing the observations obtained in the nodes of the network. The presented distributed consensus-based algorithm can identify the observations containing the jammer signal and then remove the jamming effect from the target tracking. Therefore, the method presented here generally has two steps and is shown in figure 6. As can be seen in figure 6, before the target tracking is done with a distributed particle filter (DPF), local observations are entered into two blocks that implement jamming detection in stage 1 and jamming cancellation in stage 2. These two stages are explained below.

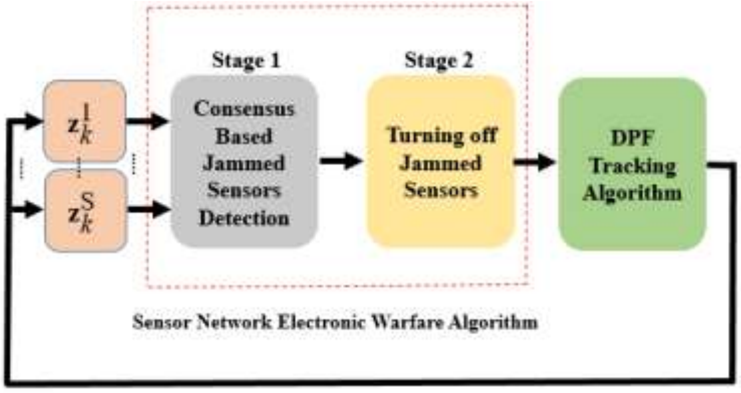
z_k^1
z_k^S
Stage 1
Consensus Based Jammed Sensors Detection
Stage 2
Turning off Jammed Sensors
DPF Tracking Algorithm
Sensor Network Electronic Warfare Algorithm

Fig. 4. Distributed target tracking algorithm with ability to detect and remove jamming effect .

Stage 1: in stage 1, after receiving the observations in the network nodes, the observations are first converted into the reference coordinate system through the following relationships.

$$x^s_{o,\,k}{=}x_s{+}r^s_{\mathbf{z},k}\cos(,\theta^s_{\mathbf{z},k}) \quad (16)$$

$$y^s_{o,\,k}{=}y_s{+}r^s_{\mathbf{z},k}\sin(,\theta^s_{\mathbf{z},k}) \quad (17)$$

Where $\mathbf{z}^s_{o,k}$=[$x^s_{o,k}$,$y^s_{o,k}$]$^{\mathrm{T}}$ is the coordinate of the observation of the node s in the reference coordinate system. reference coordination system concept is shown in figure 7. converting local coordinates to reference one is because the consensus algorithm can only be applied to observations in the same coordinate system.

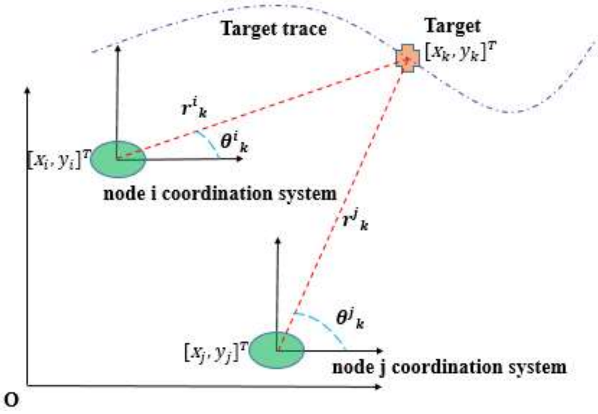

Fig. 5. Reference coordination system.

After transferring the observation coordinates of the network nodes to the reference coordinate system, the consensus algorithm is executed in the form of (18) in each node

$$\mathbf{z}^i_{o,k}(t+1)=w_{ii}\,\mathbf{z}^i_{o,k}(t)+\textstyle\sum_{j\in \mathrm{N_i}} w_{ij}\,\mathbf{z}^j_{o,k}(t) \qquad (18)$$

According to (18), each node exchanges information only with its neighboring nodes for a certain number of iterations. $\bar{\mathbf{z}}^i_{o,k}$ is the observation resulting from the average consensus at node i and time step k. According to (19) the difference in the observation of each node in the reference coordinate system $\mathbf{z}^i_{o,k}$ with the observation resulting from the average consensus algorithm $\bar{\mathbf{z}}^i_{o,k}$ is calculated at the location of each node.

$$\Delta\bar{\mathbf{z}}^i_{o,k} = \bar{\mathbf{z}}^i_{o,k} - \mathbf{z}^i_{o,k} \qquad (20)$$

In the nodes where the jamming signal is added to their observation, it is expected that the jamming infected observation will have more difference than the average observation of the network. The amount of this difference can be determined in (21)

$$|\frac{\Delta\bar{\mathbf{z}}^i_k}{\bar{\mathbf{z}}^i_k}| > \alpha \qquad (21)$$

α is called Relative Difference Threshold (RDT). In the jammed nodes, the left side of the inequity (21) is larger than the nodes on which jamming had no effect, and the greater the power of jamming RDT should be chosen larger to detect the jammed nodes more effectively.

Algorithm1: Distributed Jammer-Equipped Target Tracking with Hybrid Extended Kalman and Particle Filter

HEPF filter (according to Fig 1):
Depending on the maneuverability of the target, different filters are selected for the estimation process. For high maneuver targets, the first filter is chosen, while for low maneuver targets, the second filter is applied.
First filter (EKF+DPF):

```
1.  for i=1, …, S
        • Observations of all sensors will be averaged using EKFs and then local estimates are obtained in each node.
        • If $|\frac{\Delta \bar{z}_k^i}{\bar{z}_k^i}| > \alpha$, then the node is considered to be contaminated by jammer and its estimate is excluded from the fusion process.
    end
2.  for i=1, …, S
        • After purifying the observations from jamming signals, we apply the graph-based algorithm proposed in [4] for distributed estimation of the target state.
    end
second filter (EKF):
1.  for i=1, …, S
        • Observations of all sensors will be averaged using EKFs and then local estimates are obtained in each node.
        • If $|\frac{\Delta \bar{z}_k^i}{\bar{z}_k^i}| > \alpha$, then the node is considered to be contaminated by jammer and its estimate is excluded from the fusion process.
        •
    end
2.  for i=1, …, S
        • local state estimations are calculated by using EKF in a distributed manner.
    end
```

Stage 2: by identifying the jammed nodes in the first stage, observations of these nodes can be removed from entering the distributed tracking filters. The jammed nodes that are detected in the previous stage, remain in the network only for the distributed processing of the information of other nodes as well as telecommunication relay, but they don’t inject the information obtained from the observation into the network. When the distributed particle filter runs average consensus on the local state estimations as shown in figure 1 the jammed nodes copy the estimation of the first node from their neighbouring nodes and discard estimation of their own due to jamming effects and the rest of the DPF steps will be done same as the normal case.

The pseudocode of distributed Jammer-Equipped Target Tracking with Hybrid Extended Kalman and Particle Filter is shown in Table 1.

4. MONTE CARLO SIMULATIONS

In this section, we simulate the distributed jammer-equipped target tracking algorithm in a sensor network and compare its performance with the results of tracking the same target by a single node. In the second case, we compare the results of the proposed algorithm with the results of tracking the mentioned target in the conventional sensor network, which does not use jamming detection and cancellation blocks in its distributed tracking filters. As seen in figure 6, the network graph used in this simulation includes 16 vertices, and the connections of each node with neighboring ones are also specified with dashed line in the figure. As explained, each node communicates information only with its one-hope neighbors in each repetition of consensus. The state transition model in this simulation is in the form of

$$\mathbf{x}_{k+1}=\mathrm{f}(\mathbf{x}_k,\xi_k)=\mathbf{A}\mathbf{x}_k+\xi_k \tag{22}$$

Which is a motion with a constant turn in the clockwise direction. **A** is constant turn matrix which is as

$$\mathbf{A}=\begin{bmatrix} 1 & 0 & \frac{\sin(\mathrm{C}(k)\mathrm{T})}{\mathrm{C(k)}} & -\frac{1-\cos(\mathrm{C}(k)\mathrm{T})}{\mathrm{C}(k)} \\ 0 & 1 & \frac{1-\cos(\mathrm{C}(k)\mathrm{T})}{\mathrm{C}(k)} & \frac{\sin(\mathrm{C}(k)\mathrm{T})}{\mathrm{C}(k)} \\ 0 & 0 & \cos(\mathrm{C}(k)\mathrm{T}) & -\sin(\mathrm{C}(k)\mathrm{T}) \\ 0 & 0 & \sin(\mathrm{C}(k)\mathrm{T}) & \cos(\mathrm{C}(k)\mathrm{T}) \end{bmatrix} \tag{23}$$

We make a simplifying assumption that the communication links between the one-hop sensors are ideal, i.e., there is no AWGN noise or packet loss in the data transmission To compare the performance of the used algorithms here, we have used Root Mean Square Error (RMSE) as

$$\mathrm{RMSE(k)}=\sqrt{\frac{1}{n_{\mathrm{MC}}}\frac{1}{S}\sum_{j=1}^{n_{\mathrm{MC}}}\sum_{l=1}^{S}(x_k^j\text{-}\hat{x}_k^l)^2+(y_k^i\text{-}\hat{y}_k^l)^2} \tag{24}$$

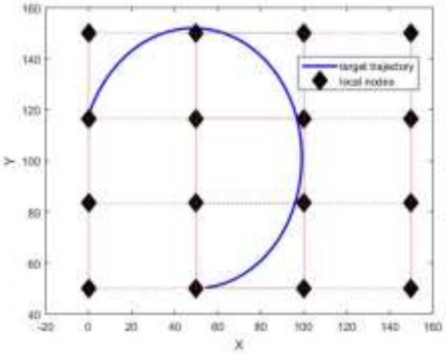

Fig. 6. target trajectory in the sensor network.

Where n_{MC} is number of Monte Carlo simulations, $\hat{x}_k^l$ and $\hat{y}_k^l$ are longitudinal and transverse components of target state estimation in node l respectively. We consider a scenario where 16 active radar sensors are deployed in a cluttered environment to track a moving target. Fig. 6 shows the sensor network topology and the target trajectory. Two sensors are considered to be single-hop neighbors if they can communicate directly with each other. The red dotted lines in Fig. 6 indicate the single-hop communication links between the sensors. If there is no dotted line between two sensors, it means that they are out of each other's communication range. The observation variance in distance measurement is equal to $\sigma_r^2 = 0.3m$ and simulation is repeated for 500 Monte Carlo simulations. In the nodes that are subject to jamming, the covariance value of the jamming noise is 30 dB higher than the observation noise, which makes the observation of these nodes completely incomprehensible. In this simulation ten percent of the network nodes that have a smaller distance from the target are jammed at each time step. We assume that all the nodes are identical, but since the target is equipped with a digital radio frequency memory (DRFM) jammer, only a limited number of WSN nodes are affected by this jammer due to the following two reasons:

1. The jammer has a limited memory for generating false targets, so it can only deceive a fraction of the nodes.
2. The antenna pattern for the DRFM is not omnidirectional, and only a few nodes are in its main lobe. In the simulations, we denote this fraction by α, which is set to 0.1, meaning that we assume that 10% of the nodes are jammed.

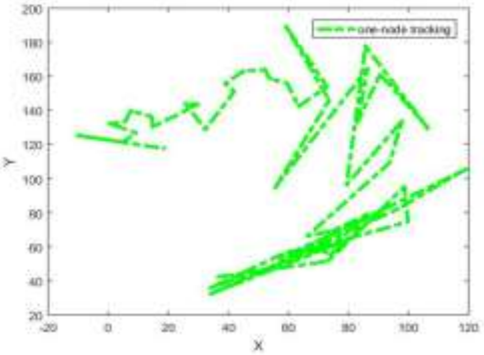

Fig. 7. Estimated target trajectory for single node.

In the figure 8 the performance of distributed target tracking in the sensor network using jamming detection and cancellation blocks is compared with single node target tracking.

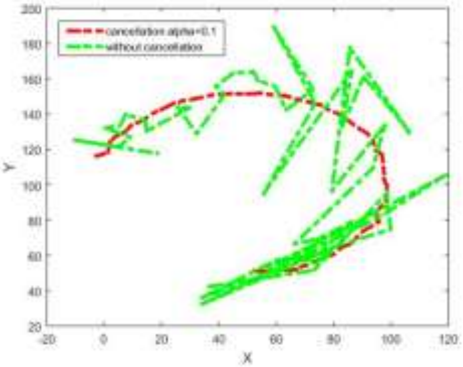

Fig. 8. Estimated target trajectory for sensor network with jamming cancellation and tracking by single node.

The tracking performance for single node is shown in Table 1. We adopt the root mean square error (RMSE) as the performance metric to assess the accuracy of the proposed algorithm for distributed estimation of the target state. As can be seen in table 1, with the defined criterion, tracking RMSE of a single node is high and as a result the tracking performed is not acceptable. The estimated trajectory of the target for single node is drawn in the figure 7. RMSE results of distributed target tracking using the jamming cancellation algorithm is shown in Table 1 at different time steps

Table 1. RMSE (m) for different scenarios.

Time-step number	10	20	30	40	50
RMSE (m) (using only single node)	51	38	68	48	62
RMSE (m) (excluding contaminated sensors)	1.96	1.46	1.2	1.35	2.01
RMSE (m) (using all contaminated sensors)	10.52	12.24	13.35	11.5	14.35

5. CONCLUSION

This paper presented jammer-equipped target tracking in a sensor network using distributed particle filters. A robust distributed method based on the consensus algorithm was presented here which can discover the nodes of the network that are subject to jamming and remove them from the distributed target tracking algorithm. To illustrate the effectiveness of the proposed method, we compare the RMSE values of the target state estimation at the 30th time step under different scenarios. When only one sensor is used for tracking, the RMSE value is 68 meters. When all the sensors in the network, including the ones affected by jamming, are used, the RMSE value drops to 13.35 meters. When the proposed method is applied to identify and exclude the jammed sensors, the RMSE value reduces to 1.2 meters. This shows that using all the sensors improves the performance by a factor of 5, and using the proposed method further improves the performance by a factor of 56.6. Therefore, the proposed method can significantly enhance the accuracy of the distributed estimation in the presence of jamming signals.

REFERENCES

[1] W. Xia, S. Meiqiu, W, Qian, "**Direct Target Tracking by Distributed Gaussian Particle Filtering Based on Delay and Doppler**" IEEE Transactions on Signal Processing, 2020, vol. 68, pp. 1361-1373.

[2] J. Fan, Y. Guo, K. Wang. "**Communication-efficient accurate statistical estimation**" Journal of the American Statistical Association, vol. 118 (542), 2023, pp. 1000-1010.

[3] M. Coates, "**Distributed particle filters for sensor networks**" 3rd international symposium on Information processing in sensor networks, 2004.

[4] I J. Y. Yu, M. J. Coates, M. G. Rabbat, "**Graph-Based Compression for Distributed Particle Filters**" IEEE Transactions on Signal and Information Processing over Networks. vol 5(3), 2019, pp. 404-417.

[5] A. Mohammadi, and A. Asif, "**Distributed Consensus + Innovation Particle Filtering for Bearing/Range, Tracking with Communication Constraints**" IEEE transactions on Signal Processing, 2014, vol. 63, no. 3, pp. 620–635.

[6] A. Mohammadi, and A. Asif, "**A constraint sufficient statistics based distributed particle filter for bearing only tracking**" IEEE International Conference on Communications (ICC), 2012.

[7] X. Sheng, Y.H. Hu, P. Ramanathan, "**Distributed particle filter with GMM approximation for multiple targets localization and tracking in wireless sensor network**" Fourth International Symposium on Information Processing in Sensor Networks, Los Angeles, California, USA, 2005, pp. 181-188.

[8] O. Hlinka, O. Sluciak, F. Hlawatsch, P. Djuric, and M. Rupp, "**Likelihood consensus and its application to distributed particle filtering**" IEEE Transactions on Signal Processing, 2012, vol. 60, no. 8, pp. 4334–4349.

[9] S.A.Vakin,"**Fundamentals of Electronic Warfare**" Artech House, 2001.

[10] A,Graham,"**Communications, Radar and Electronic Warfare**" John Wiley & Sons, 2011.

[11] D, Adamy, "**Introduction to Electronic Warfare Modeling and Simulation**" Artech House, 2003.

[12] Y. Ye, D. Kai, Z. Yongfeng, X. Shengwen and F. Qiang, "**Consensus based target tracking against deception jamming in distributed radar networks**" IET Radar, Sonar & Navigation, 2023.

[13] Y. Ye, D. Kai, Z. Yongfeng and F. Qiang, "**Consensus-based distributed target tracking in the presence of active false targets**" 2021 IEEE 2nd International Conference in Big Data, Artificial Intelligence and Internet of Things Enfinneering (ICBAIE). IEEE, 2021, pp. 753-757.

[14] J. Thangapoo Nancy, K.P. Vijaya Kumar and P. Ganesh Kumar, "**Detection of Jammer in Wireless Sensor**" 2014 Internatonal Conference on Communication and Signal Processing. IEEE, 2014, pp. 1435-1439.

[15] C. Tianzhen, L. Ping and Z. Sencun, "**An Algorithm for Jammer Localization in Wireless Sensor Networks**" 2012 IEEE 26th international conference on advanced information networking and applications. IEEE, 2012, pp. 724-731.

[16] X. Wenyuan, T. Wade and Z. Yanyong, "**Jamming Sensor Networks: Attack and Defense Strategies**" IEEE network. vol. 20, no. 3, 2006, pp. 41-47.

[17] K.P. Porkodi, I. Kartika and H.K. Gianey, "**Localization and Tracking of Mobile Jammer Sensor Node Detection in Multi-Hop Wireless Sensor Network**" Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science). vol. 14, no. 1, 2021, pp. 54-61.

[18] P. Aggarwal, Z. Syed and N. El-Sheimy, "**Hybrid Extended Particle Filter (HEPF) for Integrated Civilian Navigation System**" 2008 IEEE/ION Position, Location and Navigation Symposium. IEEE, 2008.

[19] A. Farnia, M. Skolnik, "**Electronic counter-countermeasures**" Radar Handbook, vol. 2. McGraw-Hill, New York, 2008. pp. 0964-0969.

[20] S .D Berger, "**Digital radio frequency memory linear range gate stealer spectrum**" IEEE Transactions on Aerospace and Electronic Systems, vol. 39, no. 2, 2003, pp. 725-735.