Received: 28 April 2021 | Revised: 10 July 2021 | Accepted: 21 July 2021
DOI: 10.1049/cth2.12173

IET Control Theory & Applications

ORIGINAL RESEARCH PAPER

Distributed trust-based unscented Kalman filter for non-linear state estimation under cyber-attacks: The application of manoeuvring target tracking over wireless sensor networks

Mahdieh Adeli[1] | **Majid Hajatipour**[1] | **Mohammad Javad Yazdanpanah**[2] | **Mohsen Shafieirad**[1] | **Hamed Hashemi-Dezaki**[1,3]

[1] Department of Electrical and Computer Engineering, University of Kashan, Kashan, Iran

[2] School of Electrical and Computer Engineering and Control and Intelligent Processing Center of Excellence, University of Tehran, Tehran, Iran

[3] Regional Innovational Center for Electrical Engineering, Faculty of Electrical Engineering, University of West Bohemia, Pilsen, Czech

Correspondence
Majid Hajatipour, Department of Electrical and Computer Engineering, University of Kashan, 6 km Ghotbravandi Blvd, Kashan, Iran.
Email: hajatipour@kashanu.ac.ir

Abstract

This paper is concerned with secure state estimation of non-linear systems under malicious cyber-attacks. The application of target tracking over a wireless sensor network is investigated. The existence of rotational manoeuvre in the target movement introduces non-linear behaviour in the dynamic model of the system. Moreover, in wireless sensor networks under cyber-attacks, erroneous information is spread in the whole network by imperilling some nodes and consequently their neighbours. Thus, they can deteriorate the performance of tracking. Despite the development of target tracking techniques in wireless sensor networks, the problem of rotational manoeuvring target tracking under cyber-attacks is still challenging. To deal with the model non-linearity due to target rotational manoeuvres, an unscented Kalman filter is employed to estimate the target state variables consisting of the position and velocity. A diffusion-based distributed unscented Kalman filtering combined with a trust-based scheme is applied to ensure robustness against the cyber-attacks in manoeuvring target tracking applications over a wireless sensor network with secured nodes. Simulation results demonstrate the effectiveness of the proposed strategy in terms of tracking accuracy, while random attacks, false data injection attacks, and replay attacks are considered.

1 | INTRODUCTION

Recently, cyber-physical systems (CPSs) have received widespread attention in different fields of studies, such as industrial automation systems, transportation networks, smart grids, and wireless sensor networks (WSNs) [1, 2]. WSNs have a wide range of applications, among which, target tracking is one of the most practical applications. Other applications include environmental monitoring, information collection, and control of unmanned aerial vehicles [3, 4]. A typical distributed WSN consists of several sensors that communicate with the rest of the network. In a distributed WSN, a sensor node collaborates with its neighbouring sensors to estimate the states of the target based on a given graph topology. Thus, the problem of target tracking over a WSN is considered as a distributed state estimation (DSE) problem. Due to the properties such as structural flexibility, higher scalability, and robustness to a node or link failures, distributed state estimation techniques are preferred compared to the centralised ones [5].

Generally, there are two strategies to deal with DSE: consensus strategy and diffusion strategy. To fuse estimations in a distributed manner, in consensus-based DSE, a consensus gain is multiplied by the differences of the estimation of one node and its neighbouring estimations, while in diffusion-based DSE, a weighted average of all the neighbouring estimates of a node (including itself) is calculated [6]. In distributed state estimation applications, diffusion strategy has a better estimation performance with respect to consensus strategy [6].

Among information fusion approaches, the Kalman filter (KF) is one of the most widely used techniques. Consequently, distributed Kalman filtering has received widespread attention from researchers in distributed state estimation problems [7, 8]. Consensus and diffusion Kalman filters are applied to estimate the states of linear systems in [9, 10]. Due to the applications such as power systems monitoring and rotational manoeuvring target tracking in WSNs, a huge amount of research has been devoted to distributed state estimation of non-linear dynamical systems [11–13]. Extended Kalman filter (EKF) is a non-linear filter that estimates the state variables using the linearization technique. The use of the first-order Taylor series expansion makes EKF inappropriate for highly non-linear systems, because the linearization step may lead to large errors [14]. Unscented Kalman filter (UKF) is another tool for non-linear state estimation. In comparison with EKF, UKF provides higher accuracy, because it does not require linearization computations. Thus, UKF is much applicable to the models with high non-linearities. However, UKF has a higher computational burden to obtain unscented transformation. In [12], the problem of distributed non-linear filtering has been investigated using a cooperative unscented Kalman filter. The issue of the stability of consensus EKF has been considered in [15]. Besides, the diffusion-based non-linear filtering using EKF and UKF is applied in [16].

CPSs are vulnerable to cyber-attacks. Thus, security is an important issue in the filtering problem of CPSs to avoid deterioration of system performance. Three common types of attacks are denial-of-service (DoS) attacks [17], false data injection (FDI) attacks [18], and replay attacks [19]. DoS attacks can interrupt data transfer by injecting ineffective data to waste resources [20]. In an FDI attack, the attackers manipulate the nodes data by injecting malicious information into the measurements or estimations [21]. To launch a replay attack, the attacker records valid data (sensor measurement or local estimation) in a period of time. Then, the recorded data is repeated to modify the true data [20]. The attacker can compromise sensor measurements, estimated state variables, or even the fusion centre. Therefore, the compromised data is broadcasted between the system components. Despite the importance of distributed filtering under cyber-attacks, only a few studies have addressed this issue.

In [3] and [22], a distributed Kalman filter has been applied for target tracking in a WSN. The trusted nodes have been selected using the K-means clustering approach, and their information has been used for data fusion. The robustness of the proposed method against different cyber-attacks has been illustrated. The problem of secure fusion filtering in the presence of cyber-attacks has been investigated in [23] where local measurements and local estimates have been transmitted in a sensor network. To deal with the effects of attacks, both transmitted measurements and estimates have been classified into normal and compromised classes. In [4], distributed l_2-l_∞ state estimator has been developed in the presence of deception attacks over WSNs. Moreover, improved data fusion algorithms could tackle cyber-attacks as proposed in [24]. Despite the improvement in secure fusion filtering strategies in the presence of cyber-attacks, erroneous information can be spread in the network, thus, the estimation performance might deteriorate. For example, in the secure fusion filtering as presented in [22], if a large number of neighbours of a secure node are under attack, the secured node strategy cannot avoid spreading erroneous information in the network.

Generally, the target movement is classified into manoeuvring and non-manoeuvring. The non-manoeuvring movement is described by the constant velocity (CV) and nearly constant velocity (NCV) models. Based on the target manoeuvres, and the knowledge of tuning rate, the dynamic models of manoeuvring movement are divided into three classes: constant acceleration (CA), abrupt acceleration (AA), and nearly coordination turn (NCT) models. Among different dynamic models, CV, NCV, CA, and AA models are linear. If the target moves with rotational manoeuvres with unknown turning rates, the dynamic NCT model is non-linear. In some practical applications such as military applications, the targets use manoeuvres to escape from a tracker. Manoeuvring target tracking is more complicated than non-manoeuvring target tracking. Besides, manoeuvring target tracking under cyber-attacks is more challenging. In most previous work in the field of secure state estimation in the presence of cyber-attacks for a moving target over a WSN, the target dynamic has been described by a linear model. Nevertheless, if the target has some rotational manoeuvres, the dynamic model of the target movement should possess some non-linearity. Thereafter, non-linear filtering approaches are utilised to estimate the state vector.

Due to cyber-attacks, the information of some sensor nodes becomes compromised. Thus, the polluted information may spread in the whole network, and consequently, deteriorate the estimation results. To prevent spreading polluted information in the network, some approaches have been proposed in the literature. For example, trusted-based Kalman filtering based on K-means clustering using majority voting and a secure node is presented in [3] and [22]. But the clustering approaches are not efficient enough to prevent spreading polluted information in the network.

Motivated by the above discussion, the distributed secure estimation problem of a non-linear system under cyber-attacks is investigated. To be more specific, in this article, the problem of rotational manoeuvring target tracking over a WSN under cyber-attacks is considered. Despite the importance of the problem of distributed non-linear state estimation in presence of cyber-attacks, this issue has been less addressed in the literature. This issue is investigated in this article with application to the problem of tracking a manoeuvring target in a WSN. Besides the non-linearity of the process model, which is caused by target rotational manoeuvres, the observation model is also assumed to be non-linear. As mentioned before, the existence of rotational manoeuvres in the target movement introduces non-linear behaviour in the dynamic model of the system. Further, linearization-based estimators might not be applicable to the models with high non-linearities. A distributed UKF is utilised to solve the problem. Due to cyber-attacks, the information of some sensor nodes becomes compromised. Thus, the polluted information may spread in the whole network and consequently deteriorate the estimation results. To prevent spreading polluted information in the network, some approaches have been

TABLE 1 Comparison of distributed filtering under cyber-attacks

Reference no.	Process model: Linear	Process model: Nonlinear	Measurement model: Linear	Measurement model: Nonlinear	Distributed filter: KF/EKF	Distributed filter: UKF	Distributed filter: Others	Fusion strategy: Majority voting	Fusion strategy: Secure node	Fusion strategy: Modified secure node	Fusion strategy: Others
[3]	√		√		√			√			
[4]	√		√				√				√
[22]	√			√	√			√	√		
[25]	√			√			√				√
[26]	√		√		√						√
[27]	√		√		√		√				√
[28]	√		√		√						√
[29]	√		√		√		√				√
[30]		√		√	√						√
Proposed method		√		√		√		√	√	√	

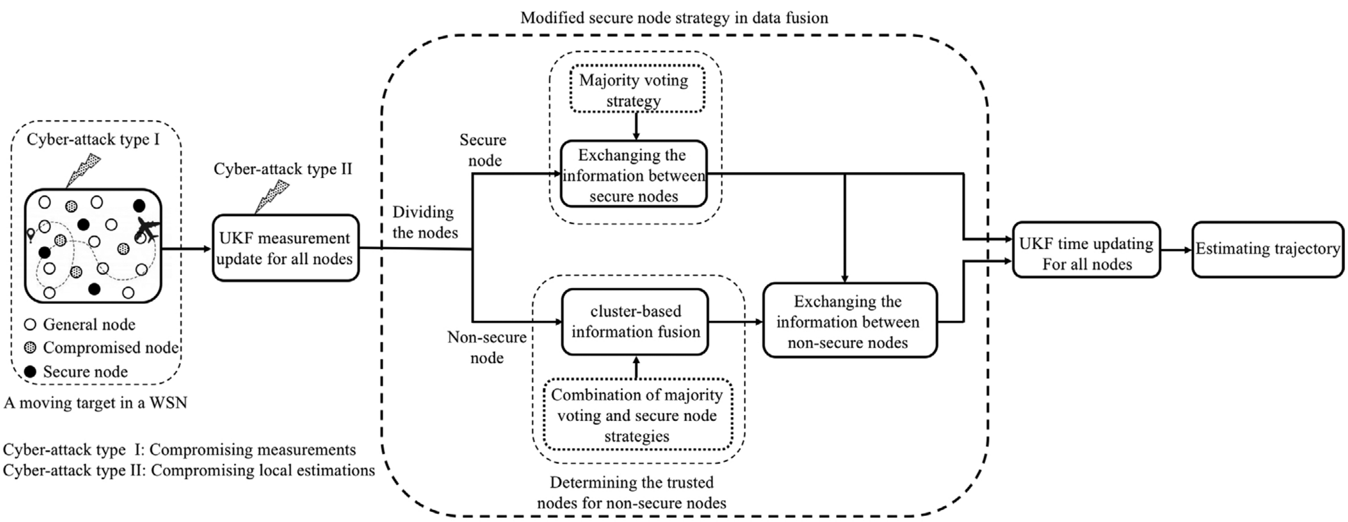

FIGURE 1 The method overview

proposed in the literature. For example, trusted-based Kalman filtering based on K-means clustering using majority voting and a secure node is presented in [3] and [22]. But the clustering approaches are not efficient enough to prevent spreading polluted information in the network. As shown in the comparative literature review, there is a research gap about considering the distributed non-linear state estimation in presence of cyber-attacks. This paper tries to fill such a research gap by proposing a trust-based UKF, which modifies the clustering approach based on the modified secure node strategy and avoids spreading the manipulated information in the network. To clarify the research gap, Table 1 compares the distributed filtering algorithms under cyber-attacks.

The method overview is shown in Figure 1. The problem of rotational manoeuvring target tracking over a WSN is considered. The WSN is composed of secure and non-secure nodes, where the non-secure nodes depending on being under cyber-attack are divided into general and compromised nodes. Each sensor node measures the position and bearing of the target. However, the sensors' measurements might be manipulated under cyber-attacks. To estimate the trajectory of the target, a trust-based UKF based on a modified secure node strategy is applied. In each node, a local estimation is obtained using UKF and the node measurement (UKF measurement update). The attackers might compromise the local estimations of non-secure nodes. To avoid spreading polluted information in the network and achieve an accurate estimated trajectory, data fusion is performed based on the proposed modified secure node strategy. First, each secure node exchanges its information between its secure node neighbours based on the majority voting strategy. Other non-secure neighbours of a secure node do not participate in exchanging information to avoid deteriorating the estimation of secure nodes. Then, each non-secure node exchanges its information between its all neighbours based on the combination of majority voting and secure node strategies. The information fusion results in secure nodes from the previous stage are applied in this stage to mitigating the effect of cyber-attack in compromised nodes. After the information fusion step, UKF time updating is performed for all nodes. Hence, the estimated trajectory is achieved in each node.

A new secure fusion non-linear filter inspired by the K-means clustering approach proposed in [3] and [22] is employed to track the target trajectory. In [3], the cluster-based information fusion has been using a majority voting strategy to classify trusted and non-trusted neighbour nodes. Besides, the majority voting strategy and secure node strategy have been applied to cluster the neighbour nodes in the information fusion step in [22]. The simulation results in [22] illustrated that using a secure node strategy provided more accurate estimates. A drawback of the secure node strategy presented in [22] is that the compromised nodes could destroy the estimates of secure nodes based on the proposed fusion algorithm. A modified secure node strategy combined with the majority voting strategy is utilised in the clustering stage of information fusion to improve the performance of the fusion filter. The robustness of the proposed method against three types of cyber-attacks (random attack, FDI attack, and replay attack) is illustrated by simulations.

The major contributions of this article are as follows:

- Modifying the cluster-based distributed filtering presented in [3] and [22];
- Considering non-linearity for both process and observation dynamics (rotational manoeuvring target movement and non-linear sensors);
- Investigating the robustness of the proposed estimation method against different cyber-attacks (random attack, FDI attack, and replay attack);
- Applicability of the proposed estimation method to other applications, such as secure state estimation of power networks.

The article is structured as follows. Section 2 presents preliminaries and problem statements consisting of WSN architecture, cyber-attacks, and the dynamic model of the manoeuvring target. The trust-based unscented Kalman filter is proposed in Section 3. The trust-based fusion scheme is also described in detail in this section. Simulation results on a manoeuvring target over a WSN are presented in Section 4, where the results are compared to the related works. The conclusion is given in Section 5.

2 | PROBLEM STATEMENT

This paper studies the distributed trust-based estimation problem of a non-linear system over a WSN under cyber-attacks. WSN architecture, the model of moving target, and the measurement model are presented in this section. Moreover, different cyber-attacks are described.

2.1 | WSN architecture

A manoeuvring moving target is considered in a 2D environment covered by a WSN equipped with N sensor nodes. The sensor nodes measure the distance and direction of the target. The nodes would be divided into two groups; secure and non-secure nodes, belonging to the sets $\mathcal{N}_S$ and $\mathcal{N}_{NS}$, respectively. The secure nodes would be selected to apply intensified physical and cyber protection. Due to a large number of sensor nodes, it is costly to protect all nodes against attackers. Instead, some strategic and crucial nodes, namely the secure nodes, are selected to be specially protected. It is assumed that the attackers cannot compromise the secure nodes because of the additional protection schemes. The implementation of this idea could be feasible and requires less cost. n_S and n_{NS} denote the number of secure nodes and non-secure nodes, respectively. It is clear that $N = n_S + n_{NS}$. The attackers could not compromise the secure nodes' data, whereas the measurements and/or estimates of non-secure nodes might be compromised by the attackers. The set of neighbours of node s is represented as $\mathcal{N}_s$.

2.2 | Cyber-attacks

Three types of cyber-attacks that manipulate local measurements or estimates are considered as follows:

- Random attack: The sensor measurements are manipulated by an attacker. It is assumed that the measurements of some nodes are manipulated by an attacker. The random attack vectors can be random zero-mean signals with different variances. The attack vectors are added to the measurements and manipulate the sensor measurements.
- FDI attack: It is assumed that the attackers have access to some estimators. They inject malicious data to compromise the local estimates covertly.
- Replay attack: The attacker records valid data (sensor measurement or local estimation) in a period of time. Then, the recorded data is repeated to modify the true data.

2.3 | Manoeuvring target dynamic model

A manoeuvring target moving in a 2D plane over a WSN is considered [31]. The state vector is described by

$$\boldsymbol{x}(k) = \left[p_x(k)\ v_x(k)\ p_y(k)\ v_y(k)\ \omega(k)\right]^T, \tag{1}$$

where $p_x(k)$ and $p_y(k)$ denote the target position, and $v_x(k)$ and $v_y(k)$ represent the target velocity in x-axis and y-axis, respectively. $\omega(k)$ is the turn rate. As presented in [32], the target movement is expressed by a nearly coordination turn (NCT) model described as follows

$$\boldsymbol{x}(k+1) = \boldsymbol{f}(\boldsymbol{x}(k)) + Gw(k), \tag{2}$$

where $\boldsymbol{f}(\boldsymbol{x}(k))$ and G are described in (3).

$$\boldsymbol{f}(\boldsymbol{x}(k)) = \begin{bmatrix} p_x(k) + \dfrac{\sin(\omega(k)T)}{\omega(k)} v_x(k) - \dfrac{1-\cos(\omega(k)T)}{\omega(k)} v_y(k) \\ \cos(\omega(k)T)v_x(k) - \sin(\omega(k)T)v_y(k) \\ \dfrac{1-\cos(\omega(k)T)}{\omega(k)} v_x(k) + p_y(k) - \dfrac{\sin(\omega(k)T)}{\omega(k)} v_y(k) \\ \sin(\omega(k)T)v_x(k) + \cos(\omega(k)T)v_y(k) \\ \beta\omega(k) \end{bmatrix},$$

$$G = \begin{bmatrix} T^2/2 & 0 & 0 \\ T & 0 & 0 \\ 0 & T^2/2 & 0 \\ 0 & T & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{3}$$

T is the sampling time and $\beta = e^{-\frac{T}{\tau_\omega}} = e^{-\alpha T}$. The parameter $\alpha = 1/\tau_\omega$ depends on the manoeuvre duration, and τ_ω is the correlation time constant for the turn rate. $w(k) = [w_x(k)\ w_y(k)\ w_\omega(k)]^T$ represents a zero-mean white noise, whose first and second elements are noisy accelerations in x and y orientations, respectively, and $w_\omega(k)$ is noise term for turn rate. The covariance of $w(k)$ is presented as

$$Q = \text{cov}(w(k)) = \text{diag}\{S_w Q_1, Q_\omega\}, \tag{4}$$

where S_w is the power spectral density of a continuous-time white noise $w(t)$, Q_ω denotes the covariance of $w_\omega(k)$, and Q_1 is described as (5).

$$Q_1 = \begin{bmatrix} \dfrac{2(\omega T - \sin\omega T)}{\omega^3} & \dfrac{1-\cos\omega T}{\omega^2} & 0 & \dfrac{\omega T - \sin\omega T}{\omega^2} \\ \dfrac{1-\cos\omega T}{\omega^2} & T & -\dfrac{\omega T - \sin\omega T}{\omega^2} & 0 \\ 0 & -\dfrac{\omega T - \sin\omega T}{\omega^2} & \dfrac{2(\omega T - \sin\omega T)}{\omega^3} & \dfrac{1-\cos\omega T}{\omega^2} \\ \dfrac{\omega T - \sin\omega T}{\omega^2} & 0 & \dfrac{1-\cos\omega T}{\omega^2} & T \end{bmatrix}. \tag{5}$$

The nodes of the aforementioned WSN are equipped with a distance sensor, a bearing sensor, and an estimator. The non-linear observation model of ith node is represented by

$$y_i(k) = \boldsymbol{h}\big(\boldsymbol{x}(k)\big) + v_i(k) = \begin{bmatrix} \sqrt{p_x^2(k) + p_y^2(k)} \\ \arctan\left(\dfrac{p_y(k)}{p_x(k)}\right) \end{bmatrix} + v_i(k). \tag{6}$$

In (6), $v_i(k)$ is measurement noise in the form of $\mathcal{N}(0, R_i(k))$, where $\mathcal{N}$ denotes Gaussian distribution and $R_i(k) = \text{diag}\{\sigma_d^2, \sigma_\theta^2\}$ is the variance of measurement noise for ith node at kth time step.

3 | TRUST-BASED UNSCENTED KALMAN FILTERING

In this section, a trust-based unscented Kalman filter is described to track a manoeuvring target under cyber-attacks over a WSN. Both process model and observation model are non-linear. To cope with the non-linearities in the model and estimate the target state variables, an unscented Kalman filter is utilised. A new secure fusion non-linear filter is proposed by modifying the K-means clustering approach presented in [3] and [22]. The proposed method prevents destroying the estimates of secure nodes by the compromised nodes. The proposed method is robust against different cyber-attacks.

In the trust-based UKF, each node i computes the predicted state mean and its covariance, then the local data is exchanged among the nodes belonging to the trusted neighbourhood. A trusted node is a node whose information is not compromised and is appropriate to use in data fusion. A trusted node is determined by the clustering approach. It is obvious that the compromised nodes are unknown. The clustering approach specifies which neighbour nodes have not been compromised and can participate in data fusion. These nodes are called trusted nodes. Using the clustering approach, the secure nodes are recognised as trusted nodes. But non-secure nodes can be either trusted or non-trusted depending on whether they are under attack or not. After information fusion, state mean and covariance are updated.

In the time step $k = 0$, for each node i, initial mean and covariance are considered as $\hat{X}_i^+(0)$ and $P_i^+(0)$, respectively. According to (2) by applying an unscented transformation (UT), $\hat{X}_i(1)$ and $P_i(1)$ are obtained.

3.1 | UKF update step

Given predicted mean $\hat{X}_i(k)$ and covariance $P_i(k)$, the sigma points $X_i^{(j)}(k)$ are calculated as follows [33]

$$X_i^{(j)}(k) = \hat{X}_i(k) + \tilde{x}_i^{(j)},\ j = 1, \dots, 2n$$

$$\tilde{x}_i^{(j)} = \left(\sqrt{nP_i(k)}\right)_j^T,\ j = 1, \dots, n$$

$$\tilde{x}_i^{(j+n)} = -\left(\sqrt{nP_i(k)}\right)_j^T,\ j = 1, \dots, n, \tag{7}$$

where n denotes the number of state variables.

Using the non-linear observation model as presented in (6), the sigma points $X_i^{(j)}(k)$ are transformed into $\hat{y}_i^{(j)}$ as

$$\hat{y}_i^{(j)} = \boldsymbol{h}\left(X_i^{(j)}(k)\right). \tag{8}$$

The predicted measurement at time k is obtained by

$$\hat{y}_i(k) = \frac{1}{2n}\sum_{j=1}^{2n}\hat{y}_i^{(j)}. \tag{9}$$

The predicted measurement covariance and the cross-covariance between $\hat{X}_i(k)$ and $\hat{y}_i(k)$ are calculated as presented in (10) and (11), respectively.

$$P_{i,y} = \frac{1}{2n}\sum_{j=1}^{2n}\left(\hat{y}_i^{(j)} - \hat{y}_i(k)\right)\left(\hat{y}_i^{(j)} - \hat{y}_i(k)\right)^{\mathrm{T}} + R_i(k), \tag{10}$$

$$P_{i,xy} = \frac{1}{2n}\sum_{j=1}^{2n}\left(\hat{X}_i^{(j)}(k) - \hat{X}_i(k)\right)\left(\hat{y}_i^{(j)} - \hat{y}_i(k)\right)^{\mathrm{T}}. \tag{11}$$

As presented in [33], the updated mean and covariance are calculated using a conventional Kalman filter as follows

$$K_i(k) = P_{i,xy}P_{i,y}^{-1} \tag{12}$$

$$\hat{X}_i^+(k) = \hat{X}_i(k) + K_i(k)\left(y_i(k) - \hat{y}_i(k)\right) \tag{13}$$

$$P_i^+(k) = P_i^-(k) - K_i(k)P_{i,y}K_i^T(k). \tag{14}$$

3.2 | Clustering approach

After measurement update, for each node k, the obtained mean $\hat{X}_i^+(k)$ and covariance $P_i^+(k)$ are exchanged with corresponding trusted neighbours. In the information fusion step, appropriate weights should be allocated to each neighbour node information. The trusted nodes with more accurate estimates get larger weights, but the weights of non-trusted nodes are considered zero. Thus, the information of non-trusted nodes is dissembled in information fusion. Using the clustering K-means algorithm, the neighbour nodes are classified into two clusters, named trusted nodes and non-trusted nodes. It is assumed that there are some secure nodes in WSN, such that the attackers could not compromise their data (consisting of measurements and estimations). The cluster that contains at least one secure node is considered a trusted cluster. If none of the two clusters include any secure node, the majority voting strategy is used to determine which cluster is the trusted cluster. According to the majority voting strategy, the cluster with more nodes is selected as the trusted cluster.

The information fusion stage based on clustering using a secure node strategy that was used in [22], perform the same for all nodes (secure nodes and non-secure nodes). According to the proposed algorithm [22], the compromised nodes in the neighbourhood of a secure node may deteriorate the resulting estimates of the secure nodes after fusion. Therefore, the secure node strategy is modified in a way that each secure node exchanges the information only between the neighbour nodes which are secure nodes. This cooperative manner between secure nodes could lead to a more accurate estimation. The new trust-based information fusion is summarised in Remark 1.

Remark 1. The new trust-based information fusion:

i. For the neighbours of non-secure nodes, the trusted cluster is determined such that at least one secure node is in that cluster;
ii. If none of the two clusters include any secure node, the majority voting strategy is used to determine which cluster is the trusted cluster;
iii. For the secure nodes, the data is exchanged only between the neighbour nodes, which are secure nodes.

3.2.1 | State clustering

For non-secure node$i$, $i \in \mathcal{N}_{NS}$, the goal is to classify n_i estimated state means $\{\hat{X}_l^+(k), l \in \mathcal{N}_i\}$ into two clusters (trusted and non-trusted). n_i is the number of neighbours of node i. The centres of clusters are specified by $x_i^{(1)}$ and $x_i^{(2)}$ with random initial values. Based on squared Euclidean distance $d(.)$ between the estimated state mean $\hat{X}_l^+(k)$ and the centres of clusters, the estimated state means $\{\hat{X}_l^+(k), l \in \mathcal{N}_i\}$ are allocated to cluster z, if

$$z = \arg\min_t \left\{d\left(x_i^{(t)}, \hat{X}_l^+(k)\right)\right\},\ \text{for } t = 1, 2. \tag{15}$$

The indicator $r_l^{(z)}$ is defined to illustrate the allocation. The value of $r_l^{(z)}$ is determined as explained below.

$$r_l^{(1)} = \begin{cases} 1, & d\left(x_i^{(1)}, \hat{X}_l^+(k)\right) < d\left(x_i^{(2)}, \hat{X}_l^+(k)\right) \\ 0, & d\left(x_i^{(2)}, \hat{X}_l^+(k)\right) < d\left(x_i^{(1)}, \hat{X}_l^+(k)\right) \end{cases} \tag{16}$$

$$r_l^{(2)} = \begin{cases} 0, & d\left(x_i^{(1)}, \hat{X}_l^{+}(k)\right) < d\left(x_i^{(2)}, \hat{X}_l^{+}(k)\right) \\ 1, & d\left(x_i^{(2)}, \hat{X}_l^{+}(k)\right) < d\left(x_i^{(1)}, \hat{X}_l^{+}(k)\right). \end{cases} \tag{17}$$

The cluster centres are updated as follows

$$x_i^{(t)} = \frac{\sum_l r_l^{(t)} \hat{X}_l^{+}(k)}{\sum_l r_l^{(t)}}, \text{ for } t = 1, 2. \tag{18}$$

The aforementioned procedure described by (15)–(18) is repeated until the allocation indicators $r_l^{(z)}$, $z = 1, 2$ do not change. If there is at least one secure node in the set $\mathcal{T}_{i,1} = \{l \in \mathcal{N}_i | r_l^{(1)} = 1\}$, cluster 1 is selected as the trusted cluster. Similarly, if there is at least one secure node in the set $\mathcal{T}_{i,2} = \{l \in \mathcal{N}_i | r_l^{(2)} = 1\}$, cluster 2 is selected as the trusted cluster. If none of the clusters include any secure node, the majority voting strategy is used to determine which cluster is the trusted cluster. In this case, trusted cluster is selected as follows

$$\mathrm{T}rustedcluster = \begin{cases} 1, & \mathrm{card}(\mathcal{T}_{i,1}) > \mathrm{card}(\mathcal{T}_{i,2}) \\ 2, & \text{otherwise}, \end{cases} \tag{19}$$

where card(.) denotes the set cardinality, which means the number of elements of the set.

A subset of $\mathcal{N}_i$ including the trusted nodes is denoted as the set Φ_i. The weights of trusted neighbour nodes for node i are calculated by

$$w_{m,i}(k) = \frac{1}{\mathrm{card}(\Phi_i)}, \text{ for } i \in \Phi_i, \tag{20}$$

whereas the weights of other neighbour nodes that are not trusted are considered zero.

For secure node I, $I \in \mathcal{N}_S$, the number of secure neighbour nodes is denoted by $N_{SecureNeighbor,I}$. Thus, weights of secure neighbour nodes for node I are computed as follows

$$w_{m,I}(k) = \frac{1}{N_{SecureNeighbour,I}}, \text{ for } I \in \mathcal{N}_S. \tag{21}$$

3.2.2 | Covariance clustering

Similar to the state clustering procedure, covariance clustering is performed. The vector of diagonal elements $p_J^{+}(k)$ is used in calculations instead of the covariance matrix $P_J^{+}(k)$, for $j = 1, \ldots, N$.

For non-secure node$i$, $i \in \mathcal{N}_{NS}$, the goal is to classify n_i neighbour nodes into two clusters based on the covariance matrix. The cluster centres are specified by $p_i^{(1)}$ and $p_i^{(2)}$ with random initial values. According to squared Euclidean distance between $p_l^{+}(k)$ and the centres of clusters, the covariance $\{p_l^{+}(k), l \in \mathcal{N}_i\}$ are allocated to cluster z, if

$$z = \arg\min_t \left\{ d\left(p_i^{(t)}, p_l^{+}(k)\right) \right\}, \text{ for } t = 1, 2. \tag{22}$$

The value of indicator $r_l^{(z)}$ is determined as explained below.

$$r_l^{(1)} = \begin{cases} 1, & d\left(p_i^{(1)}, p_l^{+}(k)\right) < d\left(p_i^{(2)}, p_l^{+}(k)\right) \\ 0, & d\left(p_i^{(2)}, p_l^{+}(k)\right) < d\left(p_i^{(1)}, p_l^{+}(k)\right) \end{cases} \tag{23}$$

$$r_l^{(2)} = \begin{cases} 0, & d\left(p_i^{(1)}, p_l^{+}(k)\right) < d\left(p_i^{(2)}, p_l^{+}(k)\right) \\ 1, & d\left(p_i^{(2)}, p_l^{+}(k)\right) < d\left(p_i^{(1)}, p_l^{+}(k)\right) \end{cases} \tag{24}$$

The cluster centres are updated as follows

$$p_i^{(t)} = \frac{\sum_l r_l^{(t)} p_l^{+}(k)}{\sum_l r_l^{(t)}}, \text{ for } t = 1, 2. \tag{25}$$

The procedure described by (22)–(25) is repeated until the allocation indicators $r_l^{(z)}$, $z = 1, 2$ do not change. The determination of the trusted nodes is similar to what is described in the state clustering part.

A subset of $\mathcal{N}_i$ including the trusted nodes is denoted as the set Ψ_i. The weights of trusted neighbour nodes for node i are calculated as

$$w_{p,i}(k) = \frac{1}{\mathrm{card}(\Psi_i)}, \text{ for } i \in \Psi_i. \tag{26}$$

For secure node$I$, $I \in \mathcal{N}_S$, the weights of secure neighbour nodes for node I are computed as

$$w_{p,I}(k) = \frac{1}{N_{SecureNeighbour,I}}, \text{ for } I \in \mathcal{N}_S. \tag{27}$$

3.3 | Information fusion

The fused state means for secure and non-secure nodes are denoted by $\tilde{X}_I^{+}$ and $\tilde{X}_i^{+}$, respectively. Moreover, $\tilde{P}_I^{+}$ and $\tilde{P}_i^{+}$ denote the fused covariances for secure and non-secure nodes. The fused state means and covariances using trust-base clustering are computed as follows

$$\tilde{X}_I^{+}(k) = \sum_{l \in \Phi_i} w_{m,I}(k) \hat{X}_l^{+}(k), \text{ for } I = 1, \ldots, N_S, \tag{28}$$

$$\tilde{X}_i^{+}(k) = \sum_{l \in \Phi_i} w_{m,i}(k) \hat{X}_l^{+}(k), \text{ for } i = 1, \ldots, N_{NS}, \tag{29}$$

$$\tilde{P}_I^{+}(k) = \sum_{l\in\Psi_i} w_{p,I}(k)P_l^{+}(k), \ \text{for } I = 1, \dots, N_S, \tag{30}$$

$$\tilde{P}_i^{+}(k) = \sum_{l\in\Psi_i} w_{p,i}(k)P_l^{+}(k), \ \text{for } i = 1, \dots, N_{NS}. \tag{31}$$

3.4 | UKF prediction step

As presented in [33], the propagation from time step k to $(k+1)$ needs calculating new sigma points $X_i^{(j)}(k+1)$ as

$$X_i^{(j)}(k) = \tilde{X}_i^{+}(k) + \tilde{x}_i^{(j)}; \ j = 1, \dots, 2n$$

$$\tilde{x}_i^{(j)} = \left(\sqrt{n\tilde{P}_i^{+}(k)}\right)_j^T, \ j = 1, \dots, n$$

$$\tilde{x}_i^{(j+n)} = -\left(\sqrt{n\tilde{P}_i^{+}(k)}\right)_j^T, \ j = 1, \dots, n. \tag{32}$$

The sigma points $X_i^{(j)}(k)$ are transformed into $\hat{X}_i^{(j)}(k+1)$ according to the non-linear model as presented in (2) and (3). The transformed sigma points are calculated as

$$\hat{X}_i^{(j)}(k+1) = \boldsymbol{f}(X_i^{(j)}(k)). \tag{33}$$

The state estimation and covariance matrix at time step $(k+1)$ are updated as (34) and (35).

$$\hat{X}_i(k+1) = \frac{1}{2n}\sum_{j=1}^{2n} \hat{X}_i^{(j)}(k+1) \tag{34}$$

$$P_i(k+1) = \frac{1}{2n}\sum_{j=1}^{2n} \left(\hat{X}_i^{(j)}(k+1) - \hat{X}_i(k+1)\right) \left(\hat{X}_i^{(j)}(k+1) - \hat{X}_i(k+1)\right)^T + Q(k). \tag{35}$$

Algorithm 1 sums the proposed non-linear trust-based filter. It is mentioned that the application of this algorithm is not limited to the problem of moving targets and can be used for any similar class of non-linear system, because no restrictive conditions on the parameters of the model have been used in the proposed method.

ALGORITHM 1 Distributed trust-based unscented Kalman filter

```
Initialization: For k = 0 and i = 1, ..., N, initialize
  X̂_i^+(0) and P_i^+(0) then Compute X̂_i(1) and P_i(1).
for k = 1 to k_max do
    for i = 1 to N do
        UKF update step:
        Calculate X̂_i^+(k) and P_i^+(k) Using (8)-(14).
    for I = 1 to N_S do
        Exchange X̂_l^+(k) and P_l^+(k) with node I, l ∈ 𝒩_S.
        Information fusion:
        Calculate the weights w_{m,I}(k) and w_{p,I}(k)
          according to (21) and (27).
        Calculate X̃_I^+(k) and P̃_I^+(k) according to (28) and
          (30).
    for i = 1 to N_NS do
        Exchange X̂_l^+(k) and P_l^+(k) with node i,
          l ∈ 𝒩_NS.
        Cluster-based information fusion:
        Calculate the weights w_{m,i}(k) and w_{p,i}(k)
          according to (20) and (26).
        Calculate X̃_i^+(k) and P̃_i^+(k) according to (29) and
          (31).
    for i = 1 to N do
        UKF prediction step:
        Calculate X̂_i(k+1) and P_i(k+1) according to
          (34) and (35).
```

4 | SIMULATIONS

The performance of proposed trust-based unscented Kalman filtering based on modified secure node strategy is evaluated for the problem of manoeuvring target tracking under different types of cyber-attacks via computer simulations in this section. Besides, the results are compared with the related methods which have used a majority voting strategy [3], secure node strategy [22], and also standard data fusion. Forasmuch as a rotational manoeuvre is considered in the target tracking problem, the moving target model is highly non-linear. Hence, the similar proposed method based on EKF diverges, therefore, the simulations are performed only based on the trust-based UKF. The convergence proof of a distributed UKF approach could be followed in [34]. Moreover, some Monte Carlo simulations are done to illustrate the improved performance of the proposed method by comparing root-mean-square errors (RMSEs).

A WSN with 10 nodes is considered, that is, $N = 10$. The corresponding graph of the WSN is shown in Figure 2. The nodes 1 and 7 are the secure nodes and the attackers cannot manipulate their measurements and estimations. Two kinds of links are used to demonstrate the information exchange between two kinds of nodes. The bi-directional links show the information exchange between two similar nodes (two secure nodes or two non-secure nodes). The uni-directional links from secure nodes to non-secure nodes show that the information of a non-secure node does not participate in secure node calculations, but the information of a secure node is utilised in non-secure node calculations.

A manoeuvring target moves over the aforementioned WSN. The dynamic model of the target has been described in Section 2.3 by (2)–(6). The sample time and correlation time constant are considered as $T = 1$ and τ_ω, respectively. The simulation is performed in 100 s. The power spectral density of a continuous-time white noise $w(t)$ is set to be 0.01, and the covariance of $w_\omega(k)$ is 0.01. The variance of measurement noise is selected to be the same for all nodes with the value of $R_i(k) = R = \text{diag}\{0.1, 0.001\}$. The initial value of the target's states is considered as $X(0) = [0, 0, 0, 0, 0]^T$ with covariance

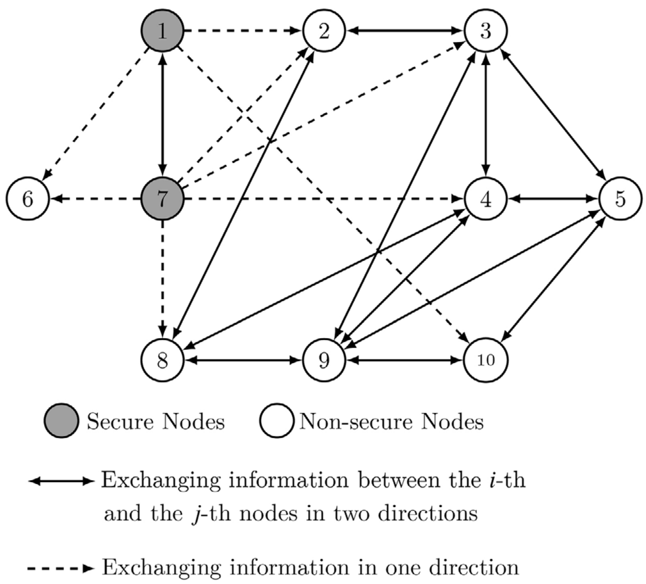

FIGURE 2 The graph topology of a typical WSN

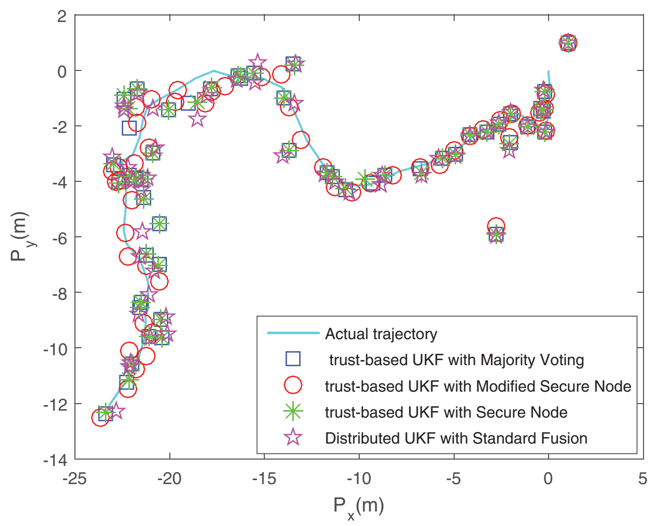

FIGURE 3 The actual and estimated trajectories under a random attack

matrix $P(0) = 0.001 \times \mathbf{I}$. The initial estimated state and covariance are considered being $\hat{X}_i^+(0) = [1, 1, 1, 1, 1]^T$ and $P_i^+(0) = 1 \times \mathbf{I}$, respectively.

4.1 | Test results

To illustrate the effectiveness of the proposed trust-based unscented Kalman filter, it is applied to three following scenarios:

- The first scenario: random attack;
- The second scenario: FDI attack;
- The third scenario: replay attack.

4.1.1 | The first scenario: Random attack

In the first scenario, it is assumed that the measurements of nodes 3, 5, and 8 are manipulated by an attacker. The random attack vectors are random zero-mean signals with variances 0.2, 0.16, and 0.2 for the nodes 3, 5, and 8, respectively. Figure 3 demonstrates the actual trajectory of the target and the estimated trajectories applying the proposed trust-based unscented Kalman filter based on modified secure node strategy, the majority voting strategy, the secure node strategy, and the standard data fusion for one of the compromised nodes, for example, node 8. As shown in Figure 3, the performance of the proposed method in presence of random attacks is not the best in some limited time steps, but there is not a gross tracking error. Due to the random nature of the attack, it is normal for the results and this does not indicate the worse performance of the proposed method. Since the pointwise comparison of methods is not reliable, the Monte Carlo method has been used in order to make a more accurate comparison considering the position RMSEs. Moreover, in the time steps in which the proposed method is not the best, its performance is reasonable, and, according to Table 2, the proposed method is totally better than the others. Therefore, to overcome the inherent nature of randomness that has led to this problem, the Monte Carlo method has been used in order to make a more accurate comparison between the methods. To compare the performance of the proposed method and the related works, the position RMSEs have been shown in Figure 4 for 50 independent Monte Carlo runs. As shown in Figure 4, the Monte Carlo method reduces the effect of the randomness nature of the random attack, and in most of the time steps, the proposed method has less RMSE than the other methods.

TABLE 2 Position RMSEs in 50 Monte Carlo runs

Position RMSE	Random attack	FDI attack	Replay attack
Trust-based UKF with majority voting	691.87×10^{-3}	3.2917	699.23×10^{-3}
Trust-based UKF with modified secure node	651.55×10^{-3}	1.0396	629.18×10^{-3}
Trust-based UKF with secure node	696.34×10^{-3}	1.2886	687.98×10^{-3}
Distributed UKF with standard fusion	825.70×10^{-3}	2.0788	825.97×10^{-3}

4.1.2 | The second scenario: FDI attack

The attacker injects false data to local estimations of nodes 3, 5, 8, and 10 in the second scenario. The estimated positions (p_x and p_y) have been compromised by random vectors with Gaussian distribution with mean 2 and variance 1. The actual and estimated trajectories under the FDI attack have been illustrated in Figure 5 for node 8. The position RMSEs under the FDI attack

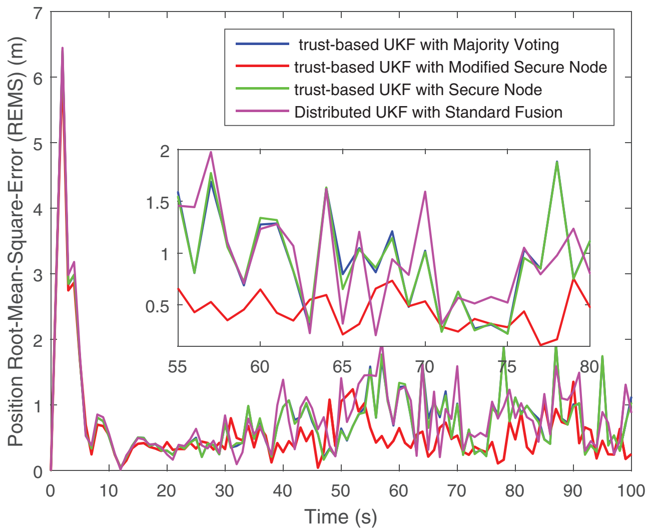

FIGURE 4 The position RMSEs under a random attack

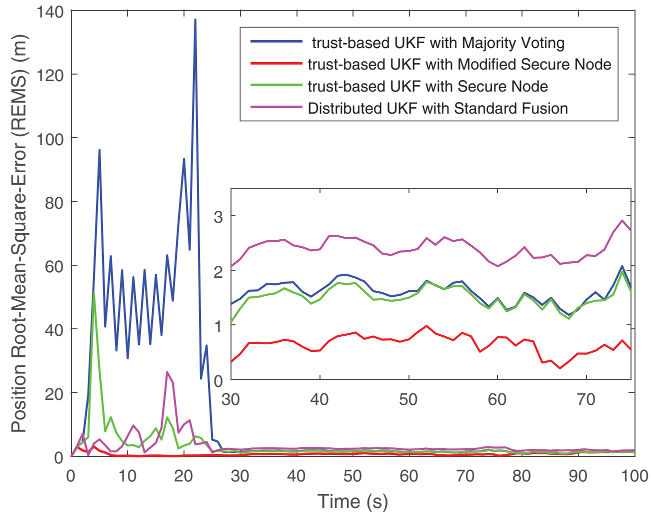

FIGURE 6 The position RMSEs under an FDI attack

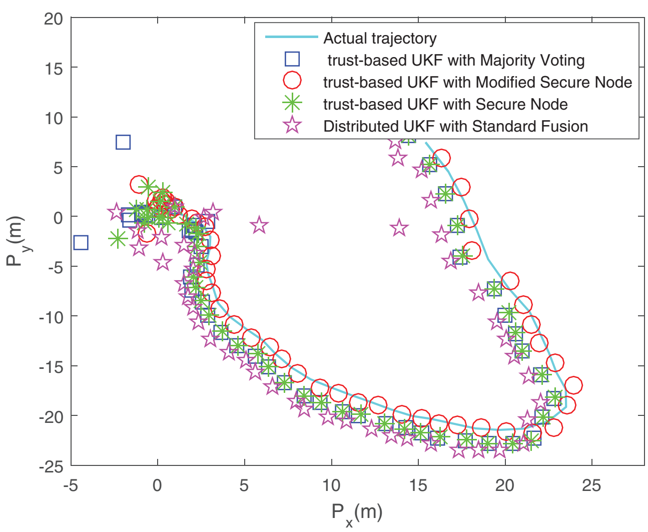

FIGURE 5 The actual and estimated trajectories under an FDI attack

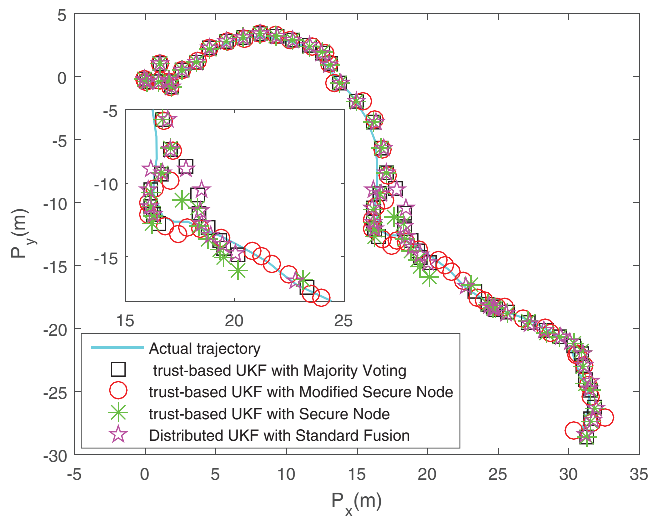

FIGURE 7 The actual and estimated trajectories under a replay attack

have been shown in Figure 6 for 50 independent Monte Carlo runs. Figures 5 and 6 demonstrate the better performance of the proposed method under FDI attacks, in comparison with the other methods.

4.1.3 | The third scenario: replay attack

In the third scenario, the attacker records a valid estimation in a period of time, and then, repeats the recorded date to destroy the tracking or to dupe the operators. It is assumed that the nodes 3, 8, and 10 are under replay attack. In computer simulations, it is assumed that the attacker repeats in the time interval from the time step 53 to 68, the previous time interval from the time step 37 to 52. Figure 7 represents the actual and estimated trajectories under the replay attack. Moreover, the position RMSEs under a replay attack have been illustrated in Figure 8 for 50 independent Monte Carlo runs. As shown in Figures 7 and 8, especially, from the time step 53 to 68, when the replay attack is launched, the error between real and estimated trajectory is less than the other methods, and the RMSE from Monte Carlo simulation results confirm the superiority of the proposed method in comparison with the other methods.

Therefore, Figures 5–8 show that the proposed method has better performance in the presence of FDI and replay attacks even in one run, and Figure 4 shows the better performance in multi-run simulations. According to the model of the system described by (1)–(7), after each run, different trajectories have been obtained due to the existence of process noise. Therefore, in order to make sure that the results are not limited to a specific trajectory, three different trajectories have been investigated in simulation results. The average RMSEs of the aforementioned methods in three scenarios are compared in Table 2. As revealed by Table 2, the proposed method achieves a better average RMSE in comparison with the related methods in all scenarios.

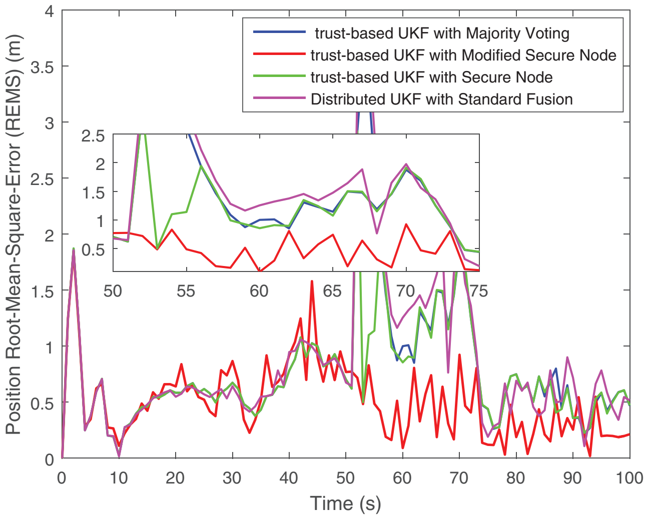

FIGURE 8 The position RMSEs under a replay attack

Regarding the comparison of the performance of the proposed method and others during all time steps, it should be noted that the RMSE for different simulations could be reasonable to judge the performance of any method. As seen in some time steps, the performance of the trust-based UKF based on modified secure node strategy is not better than other approaches. However, its accuracy is desired. To guarantee that the discussed issue cannot affect the performance of the proposed method, numerous simulations have been studied to examine the effectiveness of the proposed method.

5 | CONCLUSION

In this article, the distributed estimation problem of non-linear systems under malicious cyber-attacks has been investigated. Both process and observation models have been considered to be non-linear. A new trust-based unscented Kalman filter based on a modified secure node strategy has been proposed to estimate the state vector of a manoeuvring target over a WSN under cyber-attacks. A cluster-based fusion approach has been developed using majority voting and secure node strategies to prevent broadcasting the compromised data through the network. As revealed by the simulation results, the proposed method gives the lowest average RMSE. Moreover, it is inferred that the proposed method is robust against different cyber-attacks, such as random, FDI, and replay attacks.

NOMENCLATURE

K_i	Kalman gain
n	The number of state variables
N	The number of sensor nodes
n_S, n_{NS}	The number of secure nodes and non-secure nodes, respectively
$\mathcal{N}_s$	The set of neighbours of node s
$\mathcal{N}_S$, $\mathcal{N}_{NS}$	The set of secure nodes and non-secure nodes, respectively
$N_{SecureNeighbour,I}$	The number of secure neighbour nodes
P_i, P_i^+	The predicted and updated covariances
$p_i^{(t)}$	The updated covariance cluster centre
$P_{i,xy}$, $P_{i,y}$	The predicted measurement covariance and the cross-covariance between $\hat{X}_i(k)$ and $\hat{y}_i(k)$, respectively
$\tilde{P}_I^+$, $\tilde{P}_i^+$	The fused covariances for secure and non-secure nodes, respectively
p_x, p_y	The target position in x-axis and y-axis
Q	The covariance matrix of $w(t)$
Q_ω	The covariance matrix of w_ω
R_i	The variance of measurement noise
$r_l^{(z)}$	The allocation indicator
S_w	The power spectral density of a continuous-time white noise $w(t)$
T	The sample time
v_i	The measurement noise
v_x, v_y	The target velocity in x-axis and y-axis
w	The zero-mean white noise
$w(t)$	The continuous-time white noise
$w_{m,i}$	The weights of trusted neighbour nodes for node i in state clustering
$w_{m,I}$	The weights of secure neighbor nodes for node I in state clustering
$w_{p,i}$	The weights of trusted neighbor nodes for node i in covariance clustering
$w_{p,I}$	The weights of secure neighbor nodes for node I in covariance clustering
w_x, w_y	The noisy accelerations in x and y orientations, respectively
w_ω	The noise term of turn rate
$\boldsymbol{x}(k)$	The state vector
$\tilde{X}_I^+$, $\tilde{X}_i^+$	The fused state means for secure and non-secure nodes, respectively
$\hat{X}_i$, $\hat{X}_i^+$	The predicted and updated mean, respectively
$X_i^{(j)}$	The sigma points
$x_i^{(t)}$	The updated mean cluster centre
y_i, $\hat{y}_i$	The observation and predicted measurement of node i
α	The manoeuvre duration
τ_ω	The correlation time constant for the turn rate
ω	The turn rate
$*$	The index i corresponds to the ith node

ORCID

Mahdieh Adeli https://orcid.org/0000-0003-4836-0825
Majid Hajatipour https://orcid.org/0000-0002-7949-8555
Mohammad Javad Yazdanpanah https://orcid.org/0000-0001-7098-8331
Mohsen Shafieirad https://orcid.org/0000-0002-3239-8987
Hamed Hashemi-Dezaki https://orcid.org/0000-0003-2056-2388

REFERENCES

1. Kazemi, Z., Safavi, A.A., Setoodeh, P.: Efficient resilient dynamic co-estimation framework for cyber-physical systems under sensor attacks. IET Control Theory Appl. 14(20), 3526–3536 (2021)
2. Deshmukh, R., et al.: Distributed state estimation for a stochastic linear hybrid system over a sensor network. IET Control Theory Appl. 12(10), 1456–1464 (2018)
3. Liang, C., Wen, F., Wang, Z.: Trust-based distributed Kalman filtering for target tracking under malicious cyber attacks. Information Fusion 46, 44–50 (2019)
4. Zhu, F., et al.: Distributed robust filtering for wireless sensor networks with Markov switching topologies and deception attacks. Sensors 20(7), 1948 (2020)
5. Keshavarz-Mohammadiyan, A., Khaloozadeh, H.: Adaptive consensus-based distributed state estimator for non-linear systems in the presence of multiplicative noise. IET Signal Proc. 11(8), 986–997 (2017)
6. Wang, G., Li, N., Zhang, Y.: Diffusion nonlinear Kalman filter with intermittent observations. Proc. Inst. Mech. Eng. Part G: J. Aerosp. Eng. 232(15), 2775–2783 (2018)
7. Talebi, S.P., Werner, S.: Distributed Kalman filtering and control through embedded average consensus information fusion. IEEE Trans. Autom. Control 64(10), 4396–4403 (2019)
8. Li, W., Jia, Y., Du, J.: Distributed consensus extended Kalman filter: a variance-constrained approach. IET Control Theory Appl. 11(3), 382–389 (2016)
9. Chen, Q., et al.: Hybrid consensus-based cubature Kalman filtering for distributed state estimation in sensor networks. IEEE Sens. J. 18(11), 4561–4569 (2018)
10. Cattivelli, F.S., Sayed, A.H.: Diffusion strategies for distributed Kalman filtering and smoothing. IEEE Trans. Autom. Control 55(9), 2069–2084 (2010)
11. Lu, J., et al.: Distributed fusion estimation for non-linear networked systems with random access protocol and cyber attacks. IET Control Theory Appl. 14(17), 2491–2498 (2020)
12. Song, W., et al.: Event-triggered cooperative unscented Kalman filtering and its application in multi-UAV systems. Automatica 105, 264–273 (2019)
13. Yu, Y.: Distributed multimodel bernoulli filters for maneuvering target tracking. IEEE Sens. J. 18(14), 5885–5896 (2018)
14. Keshavarz.Mohammadiyan, A., Khaloozadeh, H.: Consensus-based distributed unscented target tracking in wireless sensor networks with state-dependent noise. Signal Process. 144, 283–295 (2018)
15. Battistelli, G., Chisci, L.: Stability of consensus extended Kalman filter for distributed state estimation. Automatica 68, 169–178 (2016)
16. Cattivelli, F.S. & Sayed, A.H.: Distributed nonlinear Kalman filtering with applications to wireless localization. 2010 IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 3522–3525. IEEE, Piscataway, NJ (2010)
17. Yang, C., Yang, W., Shi, H.: DoS attack in centralised sensor network against state estimation. IET Control Theory Appl. 12(9), 1244–1253 (2018)
18. Zhao, Z., et al.: Data-driven false data-injection attack design and detection in cyber-physical systems. IEEE Trans. Cybern. 1–9 (2020), https://doi.org/10.1109/TCYB.2020.2969320
19. Fang, C., et al.: Optimal periodic watermarking schedule for replay attack detection in cyber–physical systems. Automatica 112, 108698 (2020)
20. Peng, C., et al.: A survey on security communication and control for smart grids under malicious cyber attacks. IEEE Trans. Syst. Man Cybern. Syst. 49(8), 1554–1569 (2019)
21. Xu, R., et al.: Achieving efficient detection against false data injection attacks in smart grid. IEEE Access 5, 13787–13798 (2017)
22. Wen, F., Wang, Z.: Distributed Kalman filtering for robust state estimation over wireless sensor networks under malicious cyber attacks. Digital Signal Process. 78, 92–97 (2018)
23. Feng, X., et al.: Secure fusion filtering and clustering for distributed wireless sensor networks. 2019 IEEE 28th International Symposium on Industrial Electronics (ISIE), pp. 1661–1666. IEEE, Piscataway, NJ (2019)
24. Yang, C., et al.: A novel data fusion algorithm to combat false data injection attacks in networked radar systems. IEEE Trans. Signal Inf. Process. Networks 4(1), 125–136 (2018)
25. Shui, Y., et al.: Consensus-based distributed target tracking with false data injection attacks over radar network. Appl. Sci. 11(10), 4564 (2021)
26. Chen, Y., et al.: Trust-based distributed Kalman filter estimation fusion under malicious cyber attacks. 2019 IEEE 21st International Conference on High Performance Computing and Communications, pp. 2255–2260. IEEE, Piscataway, NJ (2019)
27. Vazquez.Olguin, M., et al.: Object tracking over distributed WSNs with consensus on estimates and missing data. IEEE Access 7, 39448–39458 (2019)
28. Ding, D., et al.: A survey on model-based distributed control and filtering for industrial cyber-physical systems. IEEE Trans. Ind. Inf. 15(5), 2483–2499 (2019)
29. Olguin, M.A.V., et al.: Design of unbiased state estimators for WSNs with consensus on measurements and estimates and improved robustness. Ph.D Thesis, University of Guanajuato (2019)
30. Chen, J., et al.: Weighted optimization-based distributed Kalman filter for nonlinear target tracking in collaborative sensor networks. IEEE Trans. Cybern. 47(11), 3892–3905 (2016)
31. Keshavarz–Mohammadiyan, A., Khaloozadeh, H.: Interacting multiple model and sensor selection algorithms for manoeuvring target tracking in wireless sensor networks with multiplicative noise. Int. J. Syst. Sci. 48(5), 899–908 (2017)
32. Li, X.R., Jilkov, V.P.: Survey of maneuvering target tracking. Part I. Dynamic models. IEEE Trans. Aerosp. Electron. Syst. 39(4), 1333–1364 (2003)
33. Simon, D.: Optimal State Estimation: Kalman, H Infinity, and Nonlinear Approaches. John Wiley & Sons, Hoboken, NJ (2006)
34. Tnunay, H., Li, Z., Ding, Z.: Distributed nonlinear Kalman filter with communication protocol. Information Sciences 513, 270–288 (2020)

How to cite this article: Adeli, M., et al.: Distributed trust-based unscented Kalman filter for non-linear state estimation under cyber-attacks: The application of manoeuvring target tracking over wireless sensor networks. IET Control Theory Appl. 15, 1987–1998 (2021). https://doi.org/10.1049/cth2.12173