IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 21, 2022, accepted March 10, 2022, date of publication March 22, 2022, date of current version March 30, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3161459

Modified Particle Filters for Detection of False Data Injection Attacks and State Estimation in Networked Nonlinear Systems

NARGESS SADEGHZADEH-NOKHODBERIZ[1], NADER MESKIN[2], (Senior Member, IEEE), AND SAEED HASANZADEH[1]

[1]Department of Electrical and Computer Engineering, Qom University of Technology, Qom 151937195, Iran
[2]Department of Electrical Engineering, Qatar University, Doha, Qatar

Corresponding author: Nader Meskin (nader.meskin@qu.edu.qa)

Open Access funding provided by the Qatar National Library.

ABSTRACT Networked control systems which transfer data over communication networks may suffer from malicious cyber attacks by injecting false data to the transferred information. Such attacks can cause performance degradation of the closed-loop system and the filtering problem. The sequential importance sampling (SIS) particle filtering (PF) methods employ the sequential Monte Carlo approach to estimate the generally non-Gaussian posterior probability density function (pdf) for Bayesian estimation of generally non-linear non-Gaussain systems. In this paper, it is firstly shown that with the normal SIS PF, the injected false data to the networked systems remains stealthy and therefore it is not possible to reduce the degrading effect of the attack on the estimation. However, with a modification in the proposal pdf, a modified SIS PF is then proposed which guarantees the attack detectability where the attacked measurements are incorporated in the particle generation process and thus the particles are updated and make the attack detectable. Using the derived thresholds and under small enough measurement noises, it is also proved that no false alarm occurs. After estimation of the attack value, the posterior pdf conditioned on truly detected attack leads to an estimation equivalent to the attack free SIS PF in terms of estimation bias and estimation covariance error. Finally, the accuracy of the presented concepts is demonstrated for a networked interconnected four-tank system.

INDEX TERMS Networked control systems (NCS), cyber-security, sequential Monte Carlo, particle filtering, convergence analysis.

I. INTRODUCTION

Recently, many industrial systems such as smart grids rely on communication networks to send their information to a computational unit. The combination of physical systems, communication networks, and computational devices forms a cyber-physical system (CPS) [1]. There are many research works devoted to the problem of networked control systems (NCS), more recently, in different control theory areas, on top of them networked controller design and state estimation [2], [3]. However, in spite of advantageous of such systems such as remote computations, they may suffer from network constraints and security issues [4]. Limited computational and communication resources lead to event-triggered and protocol based approaches [1], [5], [6]. The problem of networked systems under communication constrains such as packet dropouts and delays have also recently attracted a lot of research attentions [7]–[9].

Apart from the aforementioned problems, cyber attackers may be able to compromise the information transferring via network and therefore degrade the system performance. The attackers may inject denial of service (DoS) attacks in which data packets cannot be delivered by the computational unit through for example jamming packets or packet loss attacks [10]. In another type of attack, called deception attack, data packets are modified by attackers during transmission [11] and false data can be injected to the information exchanges in the network. Normally deception

The associate editor coordinating the review of this manuscript and approving it for publication was Hosam El-Ocla.

attacks are more difficult to be detected and it can be kept stealthy to detectors [12]. Both 0-stealthy (zero-dynamics) and α-stealthy (bias) attacks can be employed by the attackers to inject false data where in the latter case, the attackers use a low-pass filter which slowly converges to the steady state values called bias injection attack and it can be stealthy during the transient time [13].

Control and filtering problems under such cyber attacks require novel approaches and analyses. A networked game-theoretic finite horizon state estimation method under DoS attack is presented in [14] when a sensor estimates the states and decides to transmit the data or not and similarly the attacker decides to attack or not at each time. In the game theoretic approach presented in [15] and [16], the sensor attempts transmission at each time step but attack strategies try to maximize the average estimation error.

Estimation problem for linear stochastic systems under random false data injection is studied in [12] in which a novel state estimator is presented and boundedness of mean square error covariance is ensured under some sufficient conditions. If the cyber attack is detectable, preventive measures can be devised to design a secure estimation method (from the perspective of estimation convergence) and to avoid performance degradation. Therefore, detectors are applied mainly through residue analysis to detect false data injection cyber attacks in some research works as [11], [12], [17], [18]. However, in many cases the attacks remain undetectable as their effects does not appear in residuals which can lead to an insecure estimation problem. Therefore, it is important to analyze estimation strategies under cyber attacks in terms of detectability.

Security conditions for the state estimation problem of a stochastic linear system under false data injection attacks is studied in [11] where a new necessary and sufficient condition for the insecurity is derived when all communication channels are under attacks. A Kalman filtering (KF) based estimation problem under false data injection is presented in [19] where the estimator is equipped with a residual based false data detector and the degradation of the remote estimator is analyzed using the evaluation of estimation covariance error.

Particle filtering (PF) [20], [21] algorithms are very effective filtering approaches for non-linear and non-Gaussian systems which are appropriate for most of industrial systems. In PF framework, the posterior probability density function (pdf), which is required for the minimum mean square error (MMSE) estimators [22], is approximated using Monte Carlo (MC) method [23] and by generation of sample points (particles). This is indeed the main advantage of particle filtering over other Bayesian MMSE estimators such as Kalman, Extended and Unscented Kalman Filters [24], [25]. Two main PF categories are sequential importance sampling (SIS) and sampling importance re-sampling (SIR) methods where in the latter the generated particles are re-sampled using approximated pdf [26].

Recently, development of PFs have been considered in networked control systems [1], [6], [27], [28]. More specifically, the problem of cyber attack detection is briefly and generally considered using PF in [29] where the residual norm is simply compared with a deterministic threshold for a three tank system. However, there exists no detectability analysis presented and no attack compensation in the paper. A similar method has been proposed in [30] where the normal SIR PF is used to detect different types of FDI deception attack in the networked Automatic Generation Control (AGC) systems which adjust the power output of multiple generators at different power plants in response to changes in the load. However, there exist no scheme to guarantee the detection and also no compensation scheme. More recently, in [31], the problem of PF for networked systems under multiple attacks is studied based on a new likelihood computation method where randomly occurring denial of service (DOS) attacks, deception attacks and flipping attacks are considered. Since no detectability analysis is performed in [31] and the attacks are not detected, the proposed likelihood function involves both cases of probable attacks and no attack which may degrade the estimation performance.

Due to the importance of PFs in handling any functional non-linearity in the systems, and the lack of research works for PF based state estimation under cyber attacks, in this paper, the SIS PF is employed for the networked system under false data injection deception attack (bias data injection). The occurrence rate of the attack is modeled by a random binary-valued process (an i.i.d. Bernoulli distribution). After studying the drawback of the normal SIS PF to detect such attacks, a modified one is proposed in which a new proposal distribution is presented to involve the measurements in the particle generation process to update the particles. Our approach is updating the particles and therefore marking them with the affect of the attacks is some how similar to watermarking idea in the literature of attack detection [17], [32]–[34]. However, in watermarking an extra signal is incorporated and passes through the network with adversary attacks to make the attack detectable and in this paper we are directly incorporating the attacks in the particle generation process to make it detectable.

The main idea of using measurements in the particle generation process, was firstly presented in FastSLAM 2.0 using the idea of FatSLAM 2.0 algorithm in the context of robot localization and mapping using Rao-Blackwellised PF (RBPF) [35]–[37]. In [38], the inverse sensor model is employed in the particle generation process in SLAM application which cannot be employed in general non-linear measurement models. In this paper, however, we are proposing a proposal distribution in which measurements are appeared to make the FDI attack detectable.

In this paper, we use the idea of updating the particles to make the FDI attack detectable. For this purpose, using a modified proposal distribution, the measurements are involved in the particle generation process and therefore the effect of the probable attacks is appeared in the particles and

thus in the residual signal. It is shown for the systems under Gaussian assumption that the particles can be generated in two steps, firstly using the system dynamics and secondly corrected using the measurements (similar to the prediction and update steps in the Kalman filtering (KF) [24]). After detection, only the primarily generated particles using the system dynamics are incorporated in the estimation process to avoid a biased estimation. The necessary comparing thresholds are derived to guarantee the detectability of the attacks and to avoid false alarms under the assumption of small enough measurement noises. Thus, the result of the detection mode can be easily employed to estimate the value of the injected attack using some approaches such as the one presented in [39].

The posterior pdf after the FDI detection and estimation can be truly approximated using the weights corresponding to each particle conditioned on the known value of the bias attack. It is shown in the paper that such an estimator which is equivalent to the attack free SIS PF in estimation bias and estimation covariance error.

To summarize, the contributions of this paper are as follows:

1) The detectability of the normal SIS PF is analyzed and it is proved that the FDI attack may remain stealthy using the normal SIS PF.

2) A modified SIS PF with the modified proposal distribution incorporating the probable manipulated measurements in the particle generations process to update the particles, is proposed and the appropriate threshold to compare with the residual norm proportional to the minimum norm of the attack is obtained to guarantee the detectability.

3) The method is generalized to a generally non-Gaussian systems where the threshold to compare with the probability of false alarm is derived to avoid false alarms under the assumption of small enough measurement noises compared to the attack value.

4) The SIS PF is extended after the attack detection leading to an unbiased estimation with the estimation error covariance equivalent to the normal SIS PF for the attack free situation.

The rest of this paper is organized as follows. The problem is formulated in Section II where both system and attack model are formulated. The normal SIS PF under the attack with detectability analysis is presented in Section III. Section IV provides a modified SIS PF to update particles with detectability and false alarm analysis and extended PF after the attack removal. Simulation results are presented in Section V to demonstrate the accuracy of the presented concepts. Finally, conclusions are presented in Section VI.

II. PROBLEM FORMULATION

Consider a discrete-time non-linear process noise and a linear measurement model both with an additive non-Gaussian as follows:

$$x_{k+1} = f(x_k, u_k) + \varpi_k, \tag{1}$$

$$y_k = G_k x_k + \nu_k, \tag{2}$$

where $x_k \in \mathbb{R}^{n_x}$, $k \geq 0$, is the system state vector at time instant k, x_0 is the initial value of the state vector with the mean value μ_0 and the covariance matrix P_0, and a known non-Gaussian probability distribution, $u_k \in \mathbb{R}^{n_u}$, $k \geq 0$, is the input vector, $y_k \in \mathbb{R}^{n_y}$, $k \geq 0$, is the measurement vector at the time instant k, $\varpi_k \in \mathbb{R}^{n_x}$, $\nu_k \in \mathbb{R}^{n_y}$, $k \geq 0$, are independent and identically distributed (i.i.d) zero mean non-Gaussian random processes with known probability density functions and covariance matrices Q and R, respectively, $f(\cdot,\cdot) \in \mathbb{R}^{n_x} \times \mathbb{R}^{n_u} \longrightarrow \mathbb{R}^{n_x}$ is a general non-linear function, and $G_k \in \mathbb{R}^{n_y \times n_x}$ is the measurement matrix.

It is intended to design an estimator for the system presented in (1) and (2) where data is transmitted to estimator through a communication network in which an attacker can modify the observation by injecting a random false data. The status of true or false packet transmissions is identified with a Bernoulli process $l_k \in \{0, 1\}$ where $l_k = 1$ represents false data injection in the transmitted packet with probability of p_l, and $l_k = 0$ represents the true packet transmission with probability of $q_l = 1 - p_l$ [10], [12], [40]. Accordingly, the measurement model under false data injection can be presented as:

$$\tilde{y}_k = y_k + l_k \gamma_k, \tag{3}$$

where $\gamma_k \in \mathbb{R}^{n_y}$ is the injected false data and slowly converges to the desired bias value to ensure the stealthiness of the attack [39]. For this purpose, the attack is normally described using an asymptotically convergent model [13]:

$$\gamma_{k+1} = \tau \gamma_k + (1 - \tau)\bar{\gamma}, \tag{4}$$

where, $\gamma_0 = 0$, $0 < \tau < 1$ and $\bar{\gamma}$ is the steady state value of the attack. The general framework of the method is depicted in Figure 1.

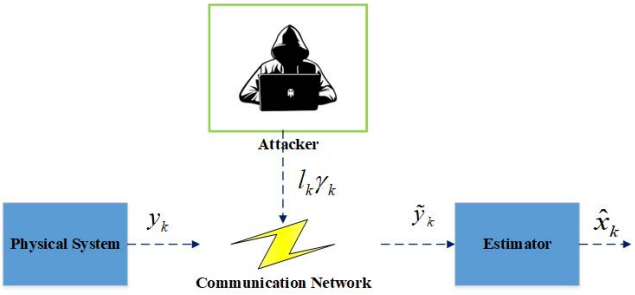

FIGURE 1. General schematic of the considered remote estimation problem.

III. THE NORMAL SIS PF UNDER FDI ATTACK: DETECTABILITY ANALYSIS

The particle filtering method is mainly based on Sequential Importance Sampling (SIS) to approximate the generally non-Gaussian marginalized posterior density function (pdf) of $\pi(x_k) = p(x_k|y_{1:k})$ [41] and this probability density function is then employed for the minimum mean square error estimation (MMSE) [42]. In this method, particles are generated using the proposal density function $q(x_k) = p(x_k|x_{k-1})$ which is the probabilistic model of the system presented

in (1). The posterior pdf is approximated as follows applying the SIS approach [21]:

$$p(x_k|y_{1:k}) \approx \sum_{i=1}^{N} w_k^{i*}\delta(x_k - x_k^i), \tag{5}$$

where x_k^i is the i-th particle and N refers to the number of particles. Besides, w_k^{i*} refers to the corresponding normalized weights which are computed recursively as follows:

$$w_k^{i*} = \frac{p(y_k|x_k^i)w_{k-1}^{i*}}{\sum_{j=1}^{N} p(y_k|x_k^j)w_{k-1}^{j*}}. \tag{6}$$

Now, consider the case in which the measurements are transferred to the estimator through a network under malicious attacks. In this case, the PF method is applied to system (1) with the measurement model of (3). The weights $\tilde{w}_k^{i*}$ are computed similar to (6) with the measurement model (3) as follows:

$$\tilde{w}_k^{i*} = \frac{p(\tilde{y}_k|x_k^i)\tilde{w}_{k-1}^{i*}}{\sum_{j=1}^{N} p(\tilde{y}_k|x_k^j)\tilde{w}_{k-1}^{j*}}, \tag{7}$$

and similar to (5), the posterior density function in this case can be approximated as follows:

$$p(x_k|\tilde{y}_{1:k}) \approx \sum_{i=1}^{N} \tilde{w}_k^{i*}\delta(x_k - x_k^i), \tag{8}$$

where x_k is the state process described by the posterior pdf of $p(x_k|\tilde{y}_{1:k})$. It is worth mentioning that the proposal distribution, $p(x_k|x_{k-1})$, is the same in both normal PF without attack and the one under the FDI attack. Therefore, the same set of particles is considered in both cases (5) and (8).

A. DEFINITIONS AND PRELIMINARIES

Detectors are applied mainly through residual analysis to detect false data injection cyber attacks. Normally in the literature, χ^2 detector, which is a residual based detector, is applied to detect cyber attacks in the literature [17], [19], [43]. The detector makes a decision based on the sum of squared residuals which is normalized by the steady-state innovation covariance matrix. However, since the posterior pdf $p(x_k|y_{1:k})$ is approximated using Monte Carlo approach, it is also possible to approximate the pdf of the residual stochastic process and therefore to analyze the residual behavior using directly computation of the probability of the residual norm to be greater than a selected threshold at each sample time.

For this purpose, firstly, the residual signal for the systems without attacks is defined:

$$z_k := y_k - G_k x_k, \tag{9}$$

where $x_k \sim p(x_k|y_{1:k})$ and $p(x_k|y_{1:k})$ is estimated in (5) and (6) using PF. The probability of attack (PoA) is then defined as follows:

$$\beta_k := \Pr(\|z_k\| > \eta_k), \tag{10}$$

where $\|\cdot\|$ refers to the Euclidean norm and η_k is also an appropriately selected threshold. The PoA β_k is calculated through Monte Carlo method using generated particles as $z_k^i = y_k - G_k x_k^i$. The corresponding unnormalized weight for z_k^i is simply the likelihood function of $p(y_k|x_k^i)$ and after normalization, the probability of each particle z_k^i is:

$$w_{z,k}^{i*} = \frac{p(y_k|x_k^i)}{\sum_{j=1}^{N} p(y_k|x_k^j)}. \tag{11}$$

The reason behind this weight is clarified as follows using Chapman–Kolmogorov equation and Bayes' rule:

$$\begin{aligned} p(z_k) = p(z_k|x_{k-1}) &= \int p(z_k, y_k, x_k|x_{k-1})dy_k dx_k \\ &= \int p(z_k|y_k, x_k)p(y_k|x_k)p(x_k|x_{k-1})dy_k dx_k. \end{aligned} \tag{12}$$

and (11) is obtained based on the fact that z_k is sampled using $p(z_k|y_k, x_k)p(x_k|x_{k-1})$, Thus, the residual signal pdf can be approximated as follows:

$$p_z(z_k) \approx \sum_{i=1}^{N} w_{z,k}^{i*}\delta(z_k - z_k^i). \tag{13}$$

Now, using (10) and (13), β_k can be obtained as follows:

$$\beta_k = \sum_{i\in\Im} w_{z,k}^{i*}, \tag{14}$$

where $\Im = \{i \mid \|z_k^i\| > \eta_k\}$. Finally, the FDI attack is detected if the obtained PoA β_k exceeds the attacked detection threshold ζ.

Now, in order to provide detectability analysis for the system under the attack, similar to (9), the residual signal is defined:

$$\tilde{z}_k := \tilde{y}_k - G_k x_k, \tag{15}$$

where $x_k \sim p(x_k|\tilde{y}_{1:k})$ and $p(x_k|\tilde{y}_{1:k})$ is approximated in (7) and (8) using the normal PF. Similarly, the pdf of $p(\tilde{z}_k|\tilde{y}_k, x_k)$ is approximated as follows:

$$p_{\tilde{z}}(\tilde{z}_k) \approx \sum_{i=1}^{N} \tilde{w}_{\tilde{z},k}^{i*}\delta(\tilde{z}_k - \tilde{z}_k^i), \tag{16}$$

where $\tilde{z}_k^i = \tilde{y}_k - G_k x_k^i$ and:

$$\tilde{w}_{\tilde{z},k}^{i*} = \frac{p(\tilde{y}_k|x_k^i)}{\sum_{j=1}^{N} p(\tilde{y}_k|x_k^j)}. \tag{17}$$

This can be easily obtained using (12) and by replacing z_k and y_k by $\tilde{z}_k$ and $\tilde{y}_k$, respectively.

Now, to analyze the detectability of the normal PF under the attack, the error between the residual signals is defined:

$$\Delta z_k := z_k - \tilde{z}_k. \tag{18}$$

Definition 1: The injected false data with minimum value of $\|\gamma\|_{\min}$ in its norm on the system measurement (see (3)) is called detectable by the PF if

$$\Pr(\|\Delta z_k\| > \xi_k) = 1, \quad \text{for } l_k = 1. \tag{19}$$

where ξ_k is a positive threshold which should be determined such that (19) holds for an attack with the minimum value of $\|\gamma\|_{\min}$.

As mentioned in the introduction earlier, now, it is intended to solve the following problems in the rest of the paper:

Problem 1: Does the normal PF guarantee the detectability of the FDI attack? For this purpose, it will be shown that there exist some cases in which the detectability is not guaranteed.

Problem 2: How the normal PF should be modified in order to detect the FDI attack? How the threshold should be selected to guarantee the FDI detectability for a given value of attack?

Problem 3: After the attack detection, how the normal PF should be modified to provide a state-estimation close enough to the normal one without any attack.

B. DETECTABILITY ANALYSIS OF THE NORMAL PF

Now, according to the preliminaries in previous subsection, we are intended to solve **Problem 1**. For this purpose, the normal PF under FDI attack is investigated for detectability. Toward this, according to Definition 1 and (19), at first the pdf of Δz_k is computed using (13) and (16) and the pdf of Δz_k, as a function of two independent random variables z_k and $\tilde{z}_k$ is computed as follows [44]:

$$p(\Delta z_k) = \int_{-\infty}^{+\infty} p_z(\Delta z_k + \tilde{z}_k) p_{\tilde{z}}(\tilde{z}_k) d\tilde{z}_k. \tag{20}$$

Using the approximated pdfs of (13) and (16), it can be concluded that:

$$\begin{aligned} &p(\Delta z_k) \\ &= \int_{-\infty}^{+\infty} \sum_{i=1}^{N} w_{z,k}^{i*} \delta(\Delta z_k + \tilde{z}_k - z_k^i) \sum_{j=1}^{N} \tilde{w}_{\tilde{z},k}^{j*} \delta(\tilde{z}_k - \tilde{z}_k^j) d\tilde{z}_k \\ &= \sum_{i=1}^{N} \sum_{j=1}^{N} w_{z,k}^{i*} \tilde{w}_{\tilde{z},k}^{j*} \delta(\Delta z_k - z_k^i + \tilde{z}_k^j) \end{aligned} \tag{21}$$

Then, it follows that:

$$\begin{aligned} &\Pr(\|\Delta z_k\| < \xi) \\ &= \int_{\|\Delta z_k\|=0}^{\|\Delta z_k\|=\xi} p(\Delta z_k) d\Delta z_k \\ &= \sum_{i=1}^{N} \sum_{j=1}^{N} w_{z,k}^{i*} \tilde{w}_{z,k}^{j*} \underbrace{\int_{\|\Delta z_k\|=0}^{\|\Delta z_k\|=\xi} \delta(\Delta z_k - z_k^i + \tilde{z}_k^j) d\Delta z_k}_{:=\mathbf{A}}, \end{aligned} \tag{22}$$

where

$$\mathbf{A} = \begin{cases} 1 & \text{if } \|z_k^i - \tilde{z}_k^j\| < \xi_k, \\ 0 & \text{elsewhere,} \end{cases}$$

Therefore,

$$\Pr(\|\Delta z_k\| < \xi_k) = \sum_{i=1}^{N} \sum_{j \in J} w_{z,k}^{i*} \tilde{w}_{\tilde{z},k}^{j*}, \tag{23}$$

where $J = \{j \mid \|z_k^i - \tilde{z}_k^j\| < \xi_k\}$. Moreover, using (18) it is concluded that:

$$\|z_k^i - \tilde{z}_k^j\| = \|G_k(x_k^j - x_k^i) - l_k \gamma_k\|. \tag{24}$$

Now, we want to show that there exist some cases in which the probability of (23) is not guaranteed to be converged to zero. Toward this, using triangle reverse inequality, (24) can be rewritten as follows:

$$\|z_k^i - \tilde{z}_k^j\| \geq |\|G_k(x_k^j - x_k^i)\| - l_k \|\gamma_k\||, \tag{25}$$

where $|\cdot|$ refers to the absolute value function. Since $x_k^i|_{i=1}^N$ are generated randomly depending on the proposal distribution of $p(x_k|x_{k-1})$, it is impossible to select a threshold ξ which guarantees $\|z_k^i - \tilde{z}_k^j\| > \xi_k$.

This drawback of the normal PF in detecting the FDI attacks can be more analyzed using the decision logic as explained in (14). It is worth mentioning that $w_{z,k}^{i*}$ (see (11)), is replaced with $\tilde{w}_{z,k}^{i*}$ (see (17)), when the attack happens and depending on its value, a model mismatch happens between the system model (the generated particle x_k^i) and the measurement model (the likelihood function $p(\tilde{y}_k|x_k^i)$).

For small valued attacks, the model mismatch is not significant and as expected, the small valued attacks remain stealthy. However, the appearance of larger attacks does not also guarantee the detectability. It is due to the fact that the values of $\tilde{w}_{z,k}^{i*}|_{i=1}^N$ may decrease considerably due to the system and measurement model mismatch resulted from the attack. This causes the attack to remain stealthy for the attacks which are large in the value. The amount of model mismatch increases as the attack value increases. So, the greater the attack value, it is less probable to be detected.

This procedure is clarified in Figure 2 in which four different cases of no attack, small, medium and large valued attacks are considered in Figure 2-a to 2-d, respectively. The likelihood pdf in this figure is depicted for Gaussian case, however, it can be easily extended for general non-Gaussian cases. It can be seen from Figure 2-a and Figure 2-b that the likelihood value for the residuals less than the threshold η_k is significantly greater than the other residuals' likelihoods. So, the attack in the second case is not detected. For the medium valued attacks, as depicted in Figure 2-c, the weights of the shifted residual particles are still great enough to trigger the decision logic. However, according to Figure 2-d, for large valued attacks, the weights decrease significantly and therefore the decision logic is not triggered.

IV. PF MODIFICATION FOR SYSTEMS UNDER FDI ATTACK

In this section, we are intended to solve **Problem 2** and **Problem 3**. A framework is proposed in which two interconnected PFs are presented to firstly detect the FDI attack and secondly to provide an unbiased estimation from the system states. In other words, using the result of first modified PF which guarantees the detectability of the FDI attack, second PF estimates the states of the system. The reason behind using two modified filters is that the filter employed for the FDI

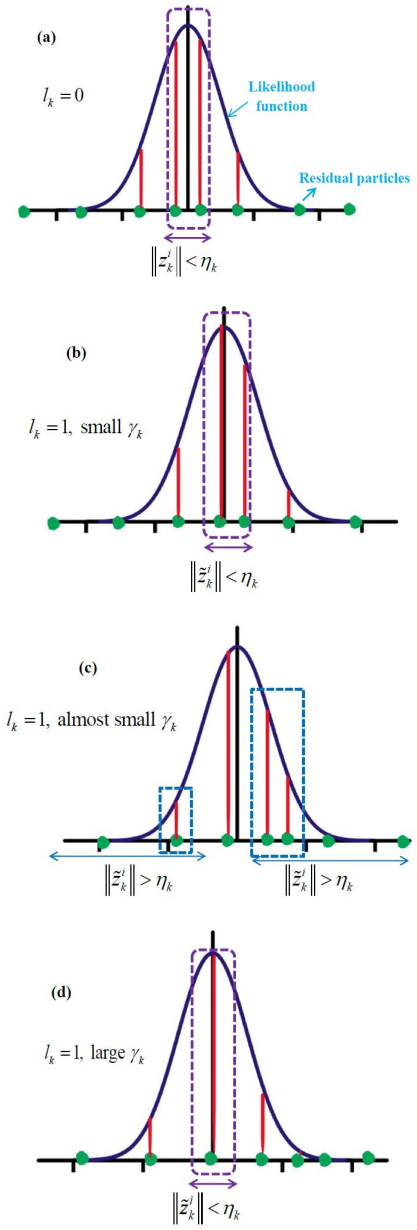

FIGURE 2. Likelihood values and PoA computation in the normal PF for a system under four different without, small valued, medium valued and large valued FDI attacks.

detection is a biased estimator while it is required to use the result of the detection filter in the PF to provide an unbiased estimation.

A. MODIFIED PF FOR FDI DETECTION

In order to overcome the drawback of the normal PF to detect the injected false data cyber attack, in this section a modified PF with a modified proposal pdf similar to the one used in FastSLAM 2.0 [36] is presented. The applied pdf incorporates measurements in the particle generation process which helps to detect the manipulated measurements. This approach is almost similar to watermarking approaches in the literature [17], [32] in the sense that in both the effect of attacks are incorporated intentionally to make the attack detectable as mentioned in the introduction. However, in order to avoid a biased estimation, the particles are generated in two steps and only the generated ones in the first step is propagated over time. The proposal pdf decomposed using Bayes' rule is as follows:

$$p(x_k|\tilde{y}_k, x_{k-1}) \propto p(\tilde{y}_k|x_k)p(x_k|x_{k-1}), \tag{26}$$

where only the particles generated using $p(x_k|x_{k-1})$, denoted as x_k^i, are propagated over time and the particles modified using $p(\tilde{y}_k|x_k)$, denoted as $\tilde{x}_k^{i+}$, are used for detection. Using Chapman-kolmogorov equation and Bayes' rule, it is concluded that:

$$p(x_k|\tilde{y}_{1:k}) = \int p(x_k|x_{k-1}, \tilde{y}_k)p(x_{k-1}|\tilde{y}_{1:k-1})dx_{k-1}. \tag{27}$$

Using the fact that particles' weights are computed by the ratio of the target to the proposal distribution, the corresponding weight function is:

$$\tilde{w}^+(x_k) = \frac{p(x_k|\tilde{y}_{1:k})}{p(x_k|x_{k-1}, \tilde{y}_k)}. \tag{28}$$

Thus, the corresponding normalized weight of $\tilde{x}_k^{i+}$, that is $\tilde{w}_k^{i*+}$, are obtained by replacing (27) in (28) and approximating $p(x_{k-1}|\tilde{y}_{1:k-1}) = \sum_{i=1}^{N} \tilde{w}_{k-1}^{i*}\delta(x_{k-1} - x_{k-1}^i)$ as follows:

$$\tilde{w}_k^{i*+} = \tilde{w}_{k-1}^{i*}, \tag{29}$$

where $\tilde{w}_k^{i*}$ is the corresponding weight of x_k^i (see (7)). Therefore, the posterior pdf is approximated:

$$p(x_k|\tilde{y}_{1:k}) \approx \sum_{i=1}^{N} \tilde{w}_k^{i*+}\delta(x_k - \tilde{x}_k^{i+}). \tag{30}$$

It is worth mentioning that for the systems without any cyber attack, if the proposed PF is applied, the following notations are employed: the particles x_k^i are generated using the pdf of $p(x_k|x_{k-1})$ with the corresponding weight of w_k^{i*} and the particles are modified using $p(y_k|x_k)$ which leads to new particles x_k^{i+} with the corresponding normalized weight of w_k^{i*+} with the weight function of $w^+(x_k)$.

Remark 1: The proposed PF is a biased estimator, because:

$$\mathbb{E}_{p(x_k|\tilde{y}_{1:k})}\{x_k\} = \int x_k \tilde{w}^+(x_k)\frac{p(x_k|x_{k-1}, \tilde{y}_k)}{p(x_k|x_{k-1}, y_k)}p(x_k|x_{k-1}, y_k)dx_k, \tag{31}$$

while,

$$\mathbb{E}_{p(x_k|y_{1:k})}\{x_k\} = \int x_k w^+(x_k)p(x_k|x_{k-1}, y_k)dx_k, \tag{32}$$

where $\mathbb{E}_p\{\cdot\}$ refers to expected value with respect to p as a pdf. It is obvious that (31) and (32) are not equal and therefore the estimator is a biased one.

Although the proposed PF is a biased estimator, due to the incorporation of the probable attacked measurement in the particle generation process, it can help detecting the attack. The detectability of the FDI attack using the modified

PF under Gaussian assumption is proved in the following. As soon as, the attack is detected, the proposed PF can be modified resulting in an unbiased estimator. In order to reduce the ambiguities, notations employed for different weights in this paper with their corresponding pdfs are summarized in Table 1.

TABLE 1. Different PF weight notations defined through this paper to approximate some pdfs.

pdf	weight function	pdf	weight function
$p(x_k\|y_{1:k})$	$w_k(x_k)$	$p(x_k\|\tilde{y}_{1:k})$	$\tilde{w}_k(x_k)$
$p(x_k\|y_{1:k})$ (proposal pdf: $p(x_k\|x_{k-1}, y_k)$)	$\tilde{w}_k^+(x_k)$	$p(x_k\|\tilde{y}_{1:k})$ (proposal pdf: $p(x_k\|x_{k-1}, y_k)$)	$\tilde{w}_k^+(x_k)$
$p(z_k)$	$w_{z,k}(z_k)$	$p(\tilde{z}_k)$	$\tilde{w}_{\tilde{z},k}(\tilde{z}_k)$
$p(z_k)$ (proposal pdf: $p(x_k\|x_{k-1}, y_k)$)	$w_{z,k}^+(z_k)$	$p(\tilde{z}_k)$ (proposal pdf: $p(x_k\|x_{k-1}, y_k)$)	$\tilde{w}_{\tilde{z},k}^+(\tilde{z}_k)$

1) THE MODIFIED PF UNDER GAUSSIAN ASSUMPTION

In order to provide a better understanding of the proposed PF and to easily evaluate the performance in terms of false data injection detectability and estimation performance, in the following, the PF is fully derived for the systems with Gaussian noises, that is referring to (1) and (2), let $\varpi_k \sim \mathcal{N}(0, Q)$ and $\nu_k \sim \mathcal{N}(0, R)$ where Q and R are covariance matrices. In other words, ϖ_k and ν_k are assumed to be zero mean Gaussian noises with covariance matrices of Q and R, respectively.

Now, the proposal distribution of $p(x_k|\tilde{y}_k, x_{k-1})$ is computed with the Gaussian assumption and linearization, almost similar to the method used to derive FastSLAM 2.0 and EKF [37]. Toward this, $p(\tilde{y}_k|x_k)$ and $p(x_k|x_{k-1})$, according to (26), are approximated as follows in the canonical form:

$$p(\tilde{y}_k|x_k) \propto \exp\{-\frac{1}{2}x_k^T \Lambda_y x_k + \kappa_y^T x_k + \Gamma_y\}, \tag{33}$$

where $\Lambda_y = G_k^T R^{-1} G_k$, $\kappa_y = G_k^T R^{-1}\tilde{y}_k$ and $\Gamma_y = -\frac{1}{2}\tilde{y}_k^T R^{-1}\tilde{y}_k$. Moreover, it follows that:

$$p(x_k|x_{k-1}) \propto \exp\{-\frac{1}{2}x_k^T \Lambda_x x_k + \kappa_x^T x_k + \Gamma_x\}, \tag{34}$$

where $\Lambda_x = Q^{-1}$, $\kappa_x = Q^{-1}f(x_{k-1}, u_{k-1})$ and $\Gamma_x = -\frac{1}{2}f(x_{k-1}, u_{k-1})^T Q^{-1} f(x_{k-1}, u_{k-1})$. Replacing (33) and (34) in (26) and using the matrix inversion lemma, it is concluded that:

$$p(x_k|\tilde{y}_k, x_{k-1}) \sim \mathcal{N}(\mu_x, \Sigma_x), \tag{35}$$

where

$$\begin{aligned}
\mu_x &= f(x_{k-1}, u_{k-1}) + K_k(\tilde{y}_k - G_k f(x_{k-1}, u_{k-1})),\\
K_k &= QG_k^T(R + G_k Q G_k^T)^{-1},\\
\Sigma_k &= Q - K_k G_k Q.
\end{aligned}$$

Therefore, the particles $\tilde{x}_k^{i+}$, $i = 1, \ldots, N$ are generated using the pdf presented in (35). In other words, at first the particles, x_k^i, $i = 1, \ldots, N$, are generated using $p(x_k|x_{k-1})$ or the process model and then using (35) it is corrected as follows:

$$\tilde{x}_k^{i+} = x_k^i + K_k(\tilde{y}_k - G_k x_k^i). \tag{36}$$

Theorem 1: For system (3), under the Gaussian assumption and under the injected false data cyber attack, using a SIS PF with the proposal pdf of (35) and the corresponding weights of (7) and (29) gives the following result:

The attack *is detectable* with an infinite number of particles, that is $N \to \infty$ when the threshold for ξ_k and therefore η_k is selected as $\varsigma_k\|\gamma\|_{\min}$ for where, $\varsigma_k = |\bar{\sigma}_k - 1|$ and $\bar{\sigma}_k$ is the nearest singular value of $G_k K_k$ to 1 and $\|\gamma\|_{\min} = \min_k \|\gamma_k\|$ or a lower bound on $\|\gamma_k\|$.

Proof: Let $\tilde{z}_k^{i+} = \tilde{y}_k - G_k\tilde{x}_k^{i+}$. Since the likelihood function of $p(\tilde{y}_k|x_k)$ is incorporated in the particle generation process as presented in (26), its corresponding weight is $\tilde{w}_{\tilde{z},k}^{i*+} = \frac{1}{N}$ and similarly $w_{z,k}^{i*+} = \frac{1}{N}$. These weights can be easily obtained similar to (12). Firstly, consider $w_{z,k}^{i*+} = \frac{1}{N}$. In this case, sampling of z_k^{i+} is performed using the proposal distribution of $p(z_k|y_k, x_k)p(y_k|x_k)p(x_k|x_{k-1})$ instead of $p(z_k|y_k, x_k)p(x_k|x_{k-1})$. $p(y_k|x_k)$ is involved in the sampling procedure as the proposal distribution to sample x_k is $p(x_k|x_{k-1}, y_k)$ in the modified PF. Similarly, the weight of $\tilde{w}_{\tilde{z},k}^{i*+}$ is obtained. Therefore:

$$p_{\tilde{z}}(\tilde{z}_k) \approx \frac{1}{N}\sum_{i=1}^{N}\delta(\tilde{z}_k - \tilde{z}_k^{i+}), \tag{37}$$

and

$$p_z(z_k) \approx \frac{1}{N}\sum_{i=1}^{N}\delta(z_k - z_k^{i+}). \tag{38}$$

So, according to (23) one can conclude that:

$$\Pr(\|\Delta z_k\| < \xi) = \sum_{i=1}^{N}\sum_{j\in J^+}\frac{1}{N^2}, \tag{39}$$

where, $J^+ = \{j \mid \|z_k^{i+} - \tilde{z}_k^{j+}\| < \xi\}$ and,

$$\|z_k^{i+} - \tilde{z}_k^{j+}\| = \|G_k(x_k^{i+} - \tilde{x}_k^{j+}) - l_k\gamma_k\|. \tag{40}$$

For $i = j$:

$$\begin{aligned}
\|z_k^{i+} - \tilde{z}_k^{i+}\| &\approx \|G_k(x_k^{i+} - \tilde{x}_k^{i+}) - l_k\gamma_k\|\\
&= l_k\|G_K K_k\gamma_k - \gamma_k\|.
\end{aligned} \tag{41}$$

If $l_k = 1$, that is for the system under the attack, using reverse triangle inequality, it can be concluded that:

$$\|z_k^{i+} - \tilde{z}_k^{i+}\| \geq ||G_k K_k\gamma_k| - \|\gamma_k\||. \tag{42}$$

Now, Singular Value Decomposition (SVD) of $G_k K_k$ gives:

$$\|z_k^{i+} - \tilde{z}_k^{i+}\| \geq \varsigma_k\|\gamma\|_{\min}, \tag{43}$$

So, if ξ_k is selected as $\varsigma_k\|\gamma\|_{\min}$ then for $i = j$, condition $\|z_k^{i+} - \tilde{z}_k^{j+}\| < \xi_k$ does not hold and it is not included in

the summation. Therefore according to (39) the following is obtained:

$$\Pr(\|\Delta z_k\| < \xi_k) \leq \sum_{i=1}^{N} \sum_{j=1, j\neq i}^{N} \frac{1}{N^2} = \frac{1}{N}, \quad l_k = 1, \quad (44)$$

where with an infinite number of particles, that is $N \to \infty$, $\Pr(\|\Delta z_k\| < \xi_k) \to 0$ and according to Definition 1, the attack is detectable. Now, let compare (44) with (14) and (18) and with the assumption of $\|z_k\| \to \epsilon$ (assuming that the states and therefore the measurements are truly estimated using the PF under no-attack), where ϵ is a small positive real number, the threshold η_k can be approximated as following at sample time k:

$$\eta_k = \varsigma_k \|\gamma\|_{\min}. \quad (45)$$

This complete the proof. ■

Remark 2: According to (44), when the number of particles is limited, the attack with the minimum value of $\|\gamma\|_{\min}$ in its norm may remain stealthy with a probability smaller than $\frac{1}{N}$.

Remark 3: To obtain the threshold ζ, with the assumption of $\|z_k\| \to \epsilon$ and referring to (10), it can be concluded from (44) that the value for the threshold ζ can be selected as:

$$\zeta = \alpha \frac{N-1}{N}, \quad \alpha \in (0, 1), \quad (46)$$

where the greater the α the less sensitive is the detection method. A selection range for the value of α will be derived in Theorem 2 for generally non-Gaussian systems in case the value of p_l is known, otherwise, α can be selected as in (46).

Remark 4: To primarily evaluate the probability of false alarms, let $l_k = 0$. Then according to (41), $\|z_k^{i+} - \tilde{z}_k^{i+}\| \approx 0$ and therefore:

$$\Pr(\|\Delta z_k\| \geq \xi) \leq \frac{N-1}{N}, \quad l_k = 0, \quad (47)$$

where $\frac{N-1}{N}$ shows the maximum probability of false alarms. During Theorem 2, it will be shown that this probability is less than p_l for generally non-Gaussian systems.

According to (47), when the number of particles increases, the upper bound for the probability of false alarms increases. At first sight, this can be interpreted as an increase in the number of false alarms. However, this is compensated automatically as the value of the threshold ζ is also increased.

Remark 5: Since the initial value of γ_k is selected as zero according to (4), that is $\gamma_0 = 0$, the detectability of the attack is not guaranteed at the beginning of the attack at sample times k such that $\|\gamma_k\| \leq \|\gamma\|_{\min}$.

2) GENERALLY NON-GAUSSIAN CASE

Now, the detectability and the probability of false alarms of the proposed modified PF are analyzed for a general non-Gaussian system through the following theorem.

Theorem 2: The detectability of the general non-linear and non-Gaussian system presented in (1) under the measurement FDI attack presented in (3) and (4), is guaranteed using the proposed modified PF when the threshold η_k in (14) is selected as $\varsigma_k \|\gamma\|_{\min}$, where ς_k and $\|\gamma\|_{\min}$ are introduced in Theorem 1. Moreover, no false alarms happen if α in (46) is selected as $p_l \frac{N}{N-1}$ and if trace(R) is small compared with $\varsigma_k \|\gamma\|_{\min}$ where the covariance matrix of R is related to the measurement noise ν_k. In the normal distributions, a suitable limit for trace(R) is $3 \times \text{trace}(R)^{\frac{1}{2}} \leq \eta$.

Proof: It follows from (2), (3) and (15) that:

$$\begin{aligned} \tilde{z}_k &= y_k + l_k \gamma_k - G_k x_k \\ &= l_k \gamma_k + \nu_k. \end{aligned} \quad (48)$$

Using the fact that l_k is a Bernoulli distributed random process, as described earlier, gives:

$$p_l(l_k) = p_l \delta(l_k - 1) + q_l \delta(l_k), \quad (49)$$

where p_l and q_l are described before (3). Now, using the fact that $\tilde{z}_k$ is equal with the summation of two random variables, $l_k \gamma_k$ and ν_k, one can conclude that:

$$p(\tilde{z}_k) = p_l p_{\nu_k}(\tilde{z}_k - \gamma_k) + q_l p_{\nu_k}(\tilde{z}_k), \quad (50)$$

where $p_{\nu_k}(\cdot)$ refers to the pdf of ν_k. So, $\tilde{\beta}_k$ is computed as:

$$\begin{aligned} \tilde{\beta}_k &= \Pr(\|\tilde{z}_k\| > \eta) \\ &= p_l \int_{\tilde{z}_k \in \tilde{\kappa}} p_{\nu_k}(\tilde{z}_k - \gamma_k) d\tilde{z}_k \\ &\quad + q_l \int_{\tilde{z}_k \in \tilde{\kappa}} p_{\nu_k}(\tilde{z}_k) d\tilde{z}_k, \end{aligned} \quad (51)$$

where $\tilde{\kappa} = \{\tilde{z}_k \mid \|\tilde{z}_k\| > \eta\}$.

Firstly, to consider the probability of false alarms in the proposed detector, let $l_k = 0$ in (48) which gives $\tilde{z}_k = \nu_k$. Since, ν_k is a zero mean random process with the covariance matrix of R, for $\eta_k = \varsigma_k \|\gamma\|_{\min}$, if trace($R$) is small compared with $\varsigma_k \|\gamma\|_{\min}$, the second part of the summation tends to zero. In order to have a measure for the trace of the covariance matrix for the Gaussian cases, since 99.7% of the random variable fall within three standard deviation [45] in normal distributions, a suitable limit can be $3 \times \text{trace}(R)^{\frac{1}{2}} \leq \eta$.

According to the above discussions, the probability of false alarms should be upper limited as follows:

$$\tilde{\beta}_k \leq p_l. \quad (52)$$

Accordingly, as it was expected, the probability of false alarms is reduced if the measurement noises are small enough in the value.

Moreover, since the threshold ζ is selected as $\alpha \frac{N-1}{N}$ to guarantee the attack detectability in Theorem 1, no false alarm happens if $\alpha \frac{N-1}{N} \geq p_l$. Thus, if α is computed as follows,

$$p_l \frac{N}{N-1} \leq \alpha < 1, \quad (53)$$

it is guaranteed that no false alarm happens. If $l_k = 1$, then $\tilde{z}_k = \gamma_k + \nu_k$. Thus, since the condition $\|\tilde{z}_k\| > \eta_k$ always hold if $\eta_k = \varsigma_k \|\gamma_k\|_{\min}$, $\tilde{\beta}_k$ tends to 1 and as it

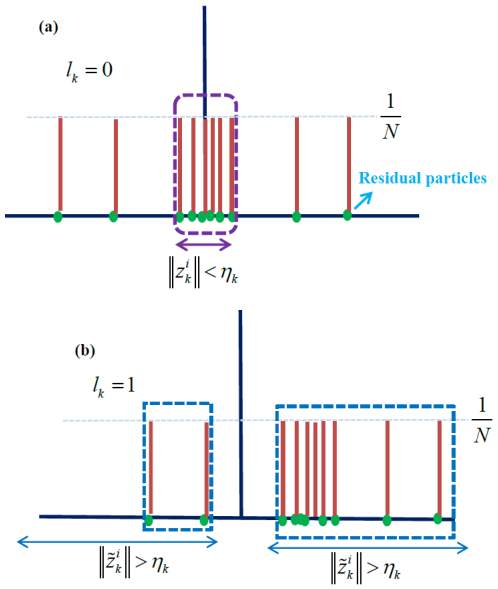

FIGURE 3. The residual samples, the corresponding weights and PoA computation in the proposed method of this paper.

was expected according to Theorem 1, the injected false data is detectable. □

Remark 6: It is worth mentioning that, normally, the value of p_l is not known. Hence, after selection of $\alpha \in (0, 1)$ for some initial sampling instances, p_l can be approximated after detection of the attacks through the ratio of the number of the attacks to the total number of the sampling instances according to (46). Since, selection of $\alpha \in (0, 1)$ can cause false alarms if (53) does not hold, the estimated p_l, say $\hat{p}_l$, may be greater than the real one and therefore some error in the estimation exists, that is $\hat{p}_l \geq p_l$. This error neither affects (46) nor (53) and therefore still detectability and no false alarm occurrence is guaranteed.

Figure 3 depicts how the proposed modified PF of this paper and the selected threshold for the residual norms, lead to a correct detection. Incorporating the measurements in the particles, removes the model mismatch between the system and measurement model and avoids degeneracy of the residual samples in the presence of the attacks. Then using the truly selection of the introduced thresholds, the decision logic triggers if an attack greater than $\|\gamma\|_{\min}$ occurs and there is no false alarm in the attack free situations.

B. UNBIASED PF

As soon as the attack is truly detected, the value of the bias attack can be estimated. For example, [39] proposes an observer to estimate the attack using an observer design for the attack with the dynamic model presented in (4) leading to $\hat{\gamma}_k$. Using the estimated attack $\hat{\gamma}_k$, in a normal PF, an unbiased estimation can be provided conditioned on the detection and estimation results. Accordingly, it is proposed to use the posterior pdf under the assumption of known l_k for the estimation. The posterior pdf is formulated as:

$$p(x_k|l_k, \tilde{y}_{1:k}) = p(\tilde{y}_k|x_k, l_k)p(x_k|l_k, \tilde{y}_{1:k-1}), \tag{54}$$

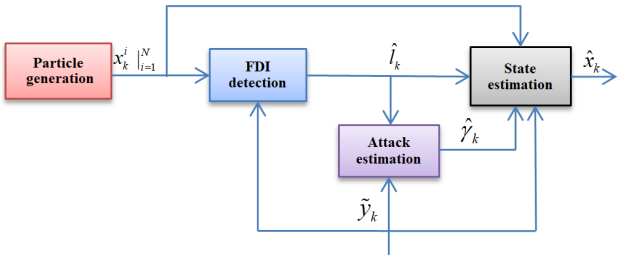

FIGURE 4. General framework of the proposed method.

where

$$p(x_k|l_{1:k}, \tilde{y}_{1:k-1}) = \int p(x_k|x_{k-1})p(x_{k-1}|, l_{1:k-1}, \tilde{y}_{1:k-1})dx_{k-1}.$$

Besides,

$$p(\tilde{y}_k|x_k, l_k) = p(y_k|x_k). \tag{55}$$

Therefore, the same weight function as $w(x_k)$ (see (6)) is obtained where the proposal sampling function is selected as $p(x_k|x_{k-1})$.

Therefore:

$$\mathbb{E}_{p(x_k|l_{1:k},\tilde{y}_{1:k})}\{x_k\} = \mathbb{E}_{p(x_k|y_{1:k})}\{x_k\}. \tag{56}$$

So, the proposed estimator gives an unbiased estimation with the same estimation error covariance as the PF without any attack. In other words:

$$\mathbb{E}_{p(x_k|l_{1:k},\tilde{y}_{1:k})}\{e_k e_k^T\} = \mathbb{E}_{p(x_k|y_{1:k})}\{e_k e_k^T\}, \tag{57}$$

where $e_k = x_k - \mathbb{E}_{p(x_k|y_{1:k})}\{x_k\}$.

The proposed method is presented in Table 2 in details as a pseudo code and the general framework of the proposed method is summarized in Figure 4 for more clarification.

Remark 7: It is obvious that the estimation error of $e_\gamma = \gamma_k - \hat{\gamma}_k$ can affect our estimator accuracy, however, during this paper, it is assumed that $\hat{\gamma}_k$ is an unbiased minimum variance estimation from γ_k.

V. SIMULATION RESULTS

In this section, the proposed concepts are evaluated through simulations on a four-tank system. The highly non-linear state equation of a four-tank system is presented in [46] and [1]. Simulations are performed in MATLAB 2019b SIMULINK environment.

A. EVALUATION OF THE PROPOSED METHOD AND DISCUSSIONS

In this part, the proposed method of this paper is evaluated precisely. For this purpose, firstly, the FDI attack detectability is compared with the normal PF for different values of attack. Then, different scenarios are considered to provide an appropriate evaluation of the method. For this purpose, the effects of changes in the noise covariance and error in estimating the value of the attack γ_k are studied. The proposed method in

TABLE 2. Pseudo code corresponding to the proposed PF method under FDI attack.

Step 0: *Initialization*: Sample initial particles, that is $\{x_0^i\}_{i=1}^N$, using initial distributions of states $(p(x_0))$, where $x_0 \sim p(x_0)$.

At the time instant k :

Step 1: *Prior estimate*: Generate the prior state particles using the system model that is $x_k^i \sim p(x_k|x_{k-1})$.

Step 2: Detection Mode:

2-1: *Particle updating*: Update particles using measurement model of $p(\tilde{y}_k|x_k)$ and generate new updated particles x_k^{i+}.

For systems under Gaussian assumption use (36). For general non-Gaussian system, the updating procedure can be determined depending on the pdf.

2-2: *Residue computation*: Compute the residue using (14) and (17) as follows:

$$\tilde{\beta}_k := \Pr(\|\tilde{z}_k\| > \eta) = \sum_{i \in \Im} \tilde{w}_{z,k}^{i*}, \tag{58}$$

where the set $\Im$ is defined in (14) and $\tilde{w}_{z,k}^{i*} = \frac{1}{N}$ and η for i^{th} particle is selected using (45).

2-3: *FDI Detection*: Compare $\tilde{\beta}_k$ with a threshold ζ as presented in (46) with α which is given in (53) to detect a probable FDI attack and therefore l_k is estimated $(\hat{l}_k)$.

Step 3: Estimation Mode:

3-0: *Injected false data estimation*: Use the detection result in the previous stage to estimate the value of γ_k using the proposed method in [39] leading to $\hat{\gamma}_k$.

3-1: *Weight computation*: Compute the normalized corresponding weight to each particle x_k^i generated in Step 1 and using $\hat{l}_k$ and $\hat{\gamma}_k$, as follows:

$$w_k^{i*} = \frac{p(\tilde{y}_k|\hat{l}_k, x_k^i) w_{k-1}^{i*}}{\sum_{j=1}^N p(\tilde{y}_k|\hat{l}_k, x_k^j) w_{k-1}^{j*}}. \tag{59}$$

3-2: *State estimation*: Estimate the system states as follows:

$$\hat{x}_k = \sum_{i=1}^N x_k^i w_k^{i*}. \tag{60}$$

these scenarios is then compared with the normal PF without any attack and the normal PF under the FDI attack.

The false data are injected with the probability of $p_l = 0.5$ and with $\tau = 0.9$ and $\gamma_0 = [0\ 0\ 0\ 0]^T$. For $\bar{\gamma} = 0.5[1\ 1\ 1\ 1]^T$ Figure 5 depicts the considered γ_k and l_k. It can be seen from Figure 5 that the value of the attack, $\|\gamma_k\|$, is slowly converging to its final value and l_k is one when the attack happens and zero, otherwise. The real measurements (y_k) versus the measurements under the FDI attack $(\tilde{y}_k)$ is depicted in Figure 6. It is obvious from the figure that at some sampling times a bias vector of γ_k has been added to the measurement vector. It is worth mentioning that the number of particles is selected as $N = 100$ to have an acceptable CPU computation time.

For $\bar{\gamma} = 0.5[1\ \ 1\ \ 1\ \ 1]^T$, estimation results related to three different cases of the normal PF without any attack, the normal PF under FDI attack and finally the proposed PF based approach under FDI attack are depicted in Figure 7 when the measurement noises are zero mean Gaussian ones

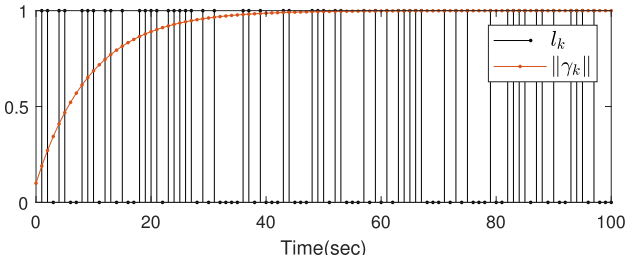

FIGURE 5. The injected FDI attack $\|\gamma_k\|$ with $\bar{\gamma} = 0.5[1\ 1\ 1\ 1]^T$ and l_k with $p_l = 0.5$.

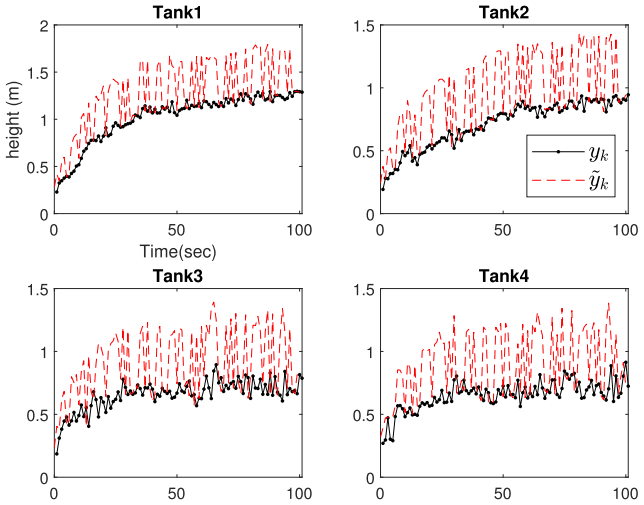

FIGURE 6. Real versus attacked measurements with $R = 10^{-3}\text{diag}(1, 1, 0.5, 0.5)$, $\bar{\gamma} = 0.5[1\ 1\ 1\ 1]^T$.

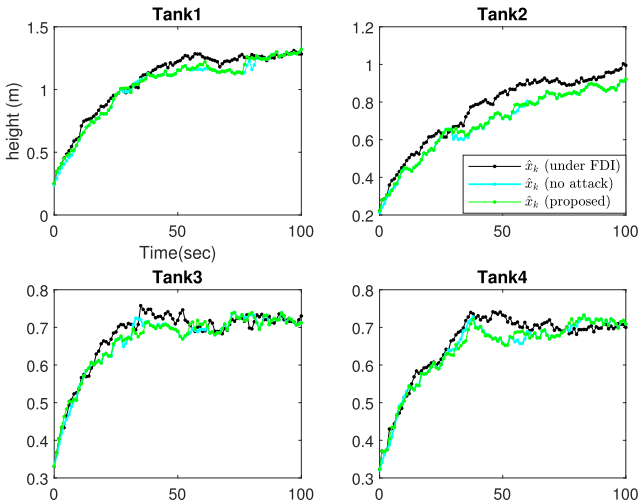

FIGURE 7. Comparison of different estimation scenarios for (the normal PF(no-attack), the normal PF (under-attack), the proposed PF (under-attack) with $R = 10^{-3}\text{diag}(1, 1, 0.5, 0.5)$ and $\bar{\gamma} = 0.5[1\ 1\ 1\ 1]^T$.

with the covariance matrix of $R = 10^{-3}\text{diag}(1, 1, 0.5, 0.5)$. It can be easily understood from the figure that the estimation results of the proposed method of the paper are close to the normal PF with no attack while the normal PF does not show a good performance in the presence of the attack.

The considered minimum norm for γ_k is selected as 0.28 which gives $\eta_k = 0.233$ for all of the particles in this system, according to Theorem 1. The detectability of

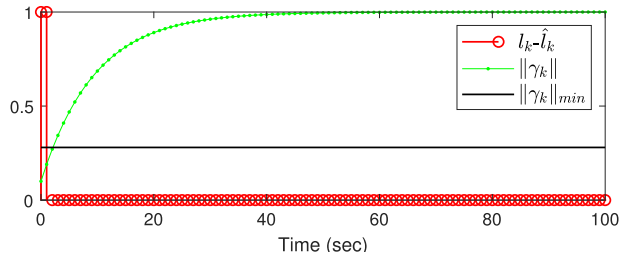

FIGURE 8. The injected FDI attack $\|\gamma_k\|$ and the detection performance $l_k - \hat{l}_k$ for $R = 10^{-3}\text{diag}(1, 1, 0.5, 0.5)$ and $\bar{\gamma} = 0.5[1\ 1\ 1\ 1]^T$.

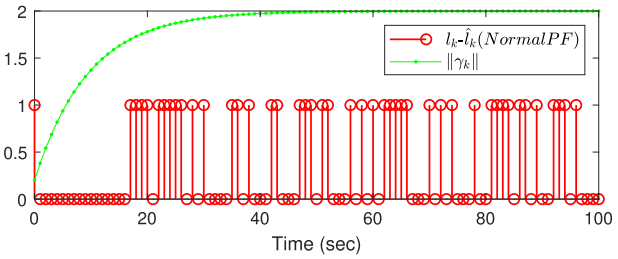

FIGURE 9. The injected FDI attack $\|\gamma_k\|$ and the detection performance $l_k - \hat{l}_k$ for $R = 10^{-3}\text{diag}(1, 1, 0.5, 0.5)$ and $\bar{\gamma} = [1\ 1\ 1\ 1]^T$ for the normal PF.

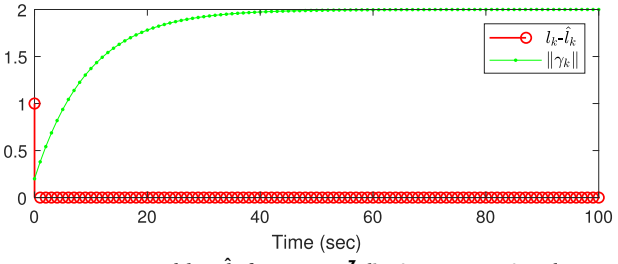

FIGURE 10. $\|\gamma_k\|$ and $l_k - \hat{l}_k$ for $R = 10^{-3}diag(1, 1, 0.5, 0.5)$ and $\bar{\gamma} = [1\ 1\ 1\ 1]^T$.

the method is evaluated in Figure 8 through computation of $l_k - \hat{l}_k$. In this regard, $l_k - \hat{l}_k = 0$ means true detection or no false alarm while $l_k - \hat{l}_k = 1$ and $l_k - \hat{l}_k = -1$ imply the FDI is not detected and false alarm, respectively. Therefore, Figure 8 shows that the algorithm is one hundred percent detectable when the $\|\gamma_k\|$ exceeds $\|\gamma\|_{\min} = 0.28$.

In order to provide a comparison with the normal PF a larger valued attack with $\bar{\gamma} = [1\ \ 1\ \ 1\ \ 1]^T$ is considered. Figure 9 depicts the detection result of the normal PF. The value of the attack, $\|\gamma_k\|$, is increased from zero to two, slowly. It is obvious from Figure 9 that when the value of the FDI attack is small and large, the normal PF cannot detect the attack while the attack can be detected using the normal PF, for the attack in between. The reason behind this, is explained in III-B. However, in the proposed method of this paper, only the minimum value of the attack, $\|\gamma\|_{\min}$, should be known and for the attacks larger than this value the detectability is guaranteed as shown in Figure 10.

Now, the method is evaluated from the aspect of false alarms when the covariance values of the measurement noises are changed. In this case, $\bar{\gamma} = 0.5[1\ \ 1\ \ 1\ \ 1]^T$. As it can be seen in Figure 8, there is no false alarm when $R = 10^{-3}\text{diag}(1, 1, 0.5, 0.5)$ since $\text{trace}(R)^{0.5} = 0.0548$ and

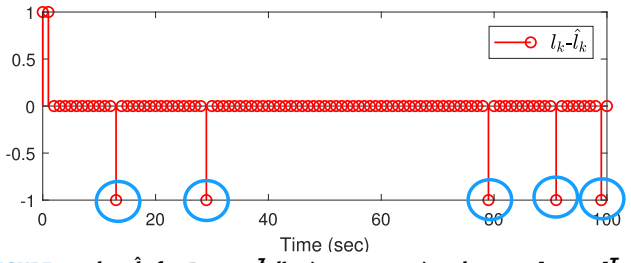

FIGURE 11. $l_k - \hat{l}_k$ for $R = 10^{-3}diag(5, 5, 2.5, 2.5)$ and $\bar{\gamma} = 0.5[1\ 1\ 1\ 1]^T$.

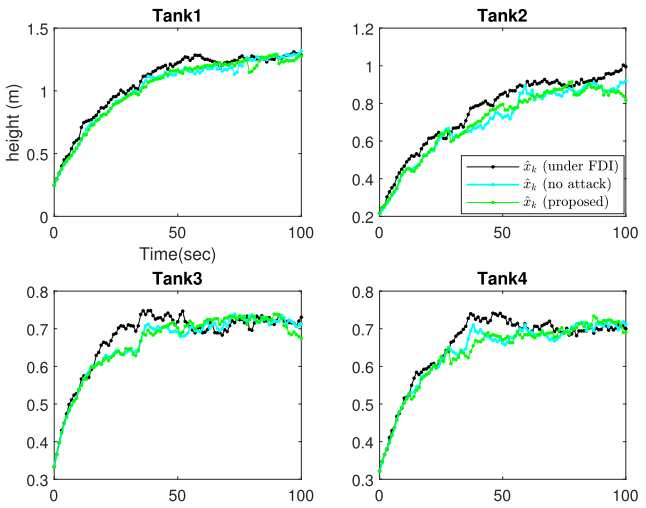

FIGURE 12. Comparison of different estimation scenarios for (the normal PF(no-attack), the normal PF (under-attack), the proposed PF (under-attack) with $R = 10^{-3}\text{diag}(5, 5, 2.5, 2.5)$ and $\bar{\gamma} = 0.5[1\ 1\ 1\ 1]^T$.

therefore the condition $3 \times \text{trace}(R)^{0.5} \leq \eta$ holds. Next, the measurement noise covariance matrix is increased to $R = 10^{-3}\text{diag}(5, 5, 2.5, 2.5)$ which leads to $\text{trace}(R)^{0.5} = 0.1225$ in which the condition $3 \times \text{trace}(R)^{0.5} \leq \eta$ does not hold anymore. The detection results are depicted in Figure 11 through $l_k - \hat{l}_k$ which shows 5 false alarms as highlighted by blue circles. Although, such false alarms were expected according to Theorem 2, normally the adversaries try to make the attacks large enough not to be faded in the measurement noise.

The estimation results in this case has been depicted in Figure 12 in which false alarms are attenuating the estimation accuracy. In order to provide a numerical analysis, the RMSE (Root Mean Squared Error) criterion is employed. The RMSE in this case is increased from 2.8×10^{-3} to 4.6×10^{-3} which shows a deterioration in the estimation as it was expected.

In order to see the effect of estimation error in estimating γ_k, it is assumed that an unbiased estimation with a covariance matrix of $10^{-2}I_{4\times4}$ is provided. Figure 13 depicts the norm of the estimated attack versus the real one. Although, this does not affect the detection results and all the attack are detected truly with no false alarm, the estimation is deteriorated since equation (55) does not hold anymore. The RMSE is also computed in this case and it increased from 2.8×10^{-3} to 8×10^{-3} which shows a deterioration in the estimation. The estimation results compared to the normal PF under attack, the normal PF without attack and the proposed method of this

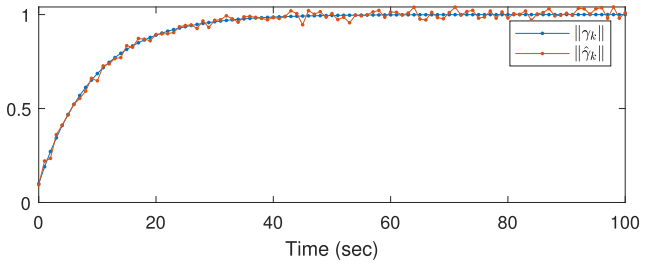

FIGURE 13. $\|\gamma_k\|$ versus $\|\hat{\gamma}_k\|$ with a large error covariance matrix of $10^{-2}I_{4\times4}$ ($\bar{\gamma} = 0.5[1\ 1\ 1\ 1]^T$).

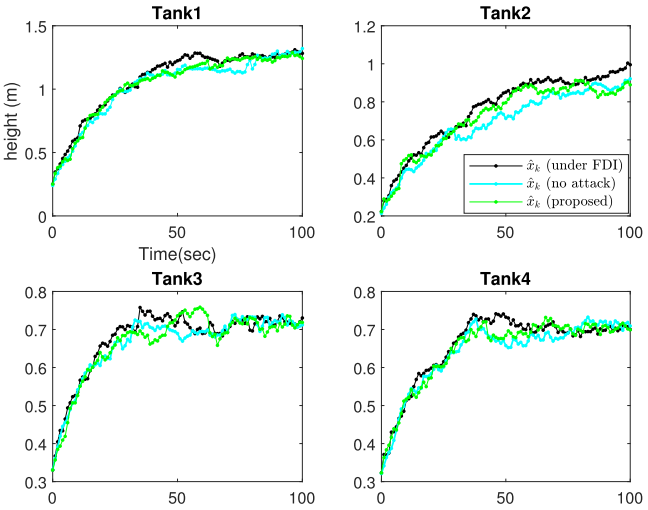

FIGURE 14. Comparison of different estimation scenarios for (the normal PF (no-attack), the normal PF (under-attack), the proposed PF (under-attack) with estimated attack, $\hat{\gamma}_k$, with a large error covariance matrix of $10^{-2}I_{4\times4}$ ($\bar{\gamma} = 0.5[1\ 1\ 1\ 1]^T$).

paper, are also depicted in Figure 14. In this case, as it can be seen form the figure, the estimation result of our proposed method is deviated from the normal PF without attack. The numerical results to compare different scenarios provided in this section are summarized in Table 3 for $\bar{\gamma} = 0.5[1\ 1\ 1\ 1]^T$. As it was also explained previously, when the measurement noise covariance increases, the probability of false alarm also increases while still there exist no stealthy attack when $\|\gamma_k\| > \|\gamma\|_{min}$. It is obvious that the RMSE increases when false alarms occur. Moreover, in spite of no false alarm and true detection, the estimation accuracy is reduced when the value of γ_k is not truly estimated.

B. COMPARISON STUDY

For more evaluation, in this part, comparisons are provided with the proposed method in [31]. As mentioned in the introduction section, there are still few research works devoted to the PF for systems under cyber attacks. Recently, a PF based method for non-linear non-Gaussain systems under randomly occurring denial of service (DOS) attacks, deception attacks and flipping attacks has been proposed in [31] where the attacks are compensated through an appropriate likelihood computation and no detection method is proposed in the paper. Although the considered deception attack is not the FDI one, it can be easily extended to include the bias deception attack as in our case.

TABLE 3. Evaluation of the proposed method in different scenarios ($\bar{\gamma} = 0.5[1\ 1\ 1\ 1]^T$).

Scenario	trace$(R) = 0.003$, $\hat{\gamma}_k = \gamma_k$	trace$(R) = 0.015$, $\hat{\gamma}_k = \gamma_k$	trace$(R) = 0.003$, $\hat{\gamma}_k = \gamma_k \pm 10^{-2}$
RMSE	2.8×10^{-3}	4.6×10^{-3}	8×10^{-3}
No of false alarms	0	5	0
No of stealthy attacks	2	2	2

TABLE 4. RMSE and CPU time for the proposed method of this paper versus the normal PF under attack and the method of [31] with $R = 10^{-3}diag(1, 1, 0.5, 0.5)$ and $\hat{\gamma} = \gamma_k$ ($\bar{\gamma} = 0.5[1\ 1\ 1\ 1]^T$).

Method	The normal PF (under attack)	Method of [31]	The proposed method
RMSE	1.3×10^{-2}	8.2×10^{-3}	2.8×10^{-3}
CPU computation time (average)	1.9593×10^{-4}	6.1460×10^{-5}	6.9782×10^{-4}

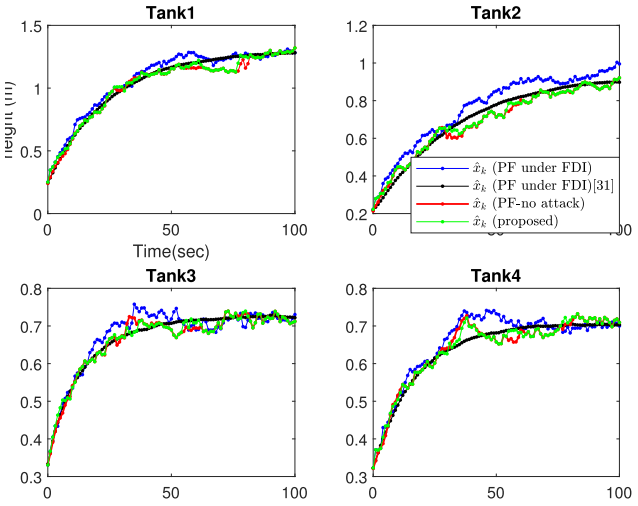

FIGURE 15. The estimation results of the method in [31] compared with the normal PFs without and under attack and the proposed method of this paper all with $R = 10^{-3}diag(1, 1, 0.5, 0.5)$ ($\bar{\gamma} = 0.5[1\ 1\ 1\ 1]^T$).

For this purpose, due to no DOS attack in our case, $\bar{\phi}^s$ and $\bar{\alpha}^s$ which are the probability of the DOS attack and the flip attack in sensor s, are set as zero, that is $\bar{\phi}^s = 0$ and $\bar{\alpha}^s = 0$ for $s = 1, \ldots, 4$. The probability of the deception attack occurrence, $\bar{\varphi}^s$ for $s = 1, \ldots, 4$, is set as p_l which is the probability of $l_k = 1$ in our paper. Besides, $\rho_k = \bar{\gamma}$ where ρ_k is the vector of the deception attack. Therefore, according to equations (13) to (15) of [31], the likelihood of each particle is 1 and thus the normalized weights are $\frac{1}{N}$ for all particles. It is obvious that the estimator is a biased estimator. Figure 15 depicts the estimation results of the method in [31] compared with the normal PFs without and under attack and the proposed method of this paper. It can be easily seen from the figure that the estimator of [31] is a biased one.

In order to provide a numerical evaluation criterion, RMSE is computed to compare the estimation results with the normal

PF without the attack and the results are summarized in Table 4. According to this table, the performance of the proposed method of this paper is greater than the normal PF under attack for both of the attack scenarios. The performance is also greatly improved compared with the proposed method of [31]. CPU computation time has also been computed using tic-toc command and the averages are reported in Table 4. Since our proposed method performs both detection and estimation, it is obviously more time consuming than the normal PF and the method of [31].

VI. CONCLUSION

The problem of PF based state estimation for networked systems under FDI malicious cyber attacks was studied in this paper. The normal SIS PF was firstly studied from the perspective of its ability to detect the attack and it was shown that the attack may remain stealthy using the normal PF and therefore the degrading effect cannot be truly compensated accordingly. To overcome this drawback the proposal pdf was modified to incorporate measurements in the particle generation process and therefore the particles were updated. The updated particles were derived under special case of the Gaussian assumption where the detectability of the attack is guaranteed with an infinite number of particles and the corresponding threshold values were derived. The first one is proportional to the attack minimum norm and the latter proportional to the probability of the attack occurrence. It was then proved that with these threshold selection, the attacks in generally non-Gaussian systems are detectable and if the measurement noises value are small enough in their standard deviations compared with the attack value, there is no probability of false alarms.

Since the updated particles lead to a biased estimation, the non-updated particles were then employed for the estimation after the attack detection and estimation. The particles were employed to approximate the posterior pdf conditioned on the detected attack which can provide an unbiased estimation with an estimation error covariance matrix equivalent with the normal SIS PF with no attack.

The accuracy of the proposed method were evaluated through simulations on an interconnected highly non-linear four-tank system where the measurement covariance matrix changes. The results were compared to non-attack situation and the attacked one with the normal SIS PF. The method was also compared to a recently presented one from different perspectives of accuracy and cpu computation time. Although the performance of the method is greatly improved, it is slightly more time consuming as it contains both detection and estimation modes.

Due to the lack of research works on PF for networked systems under cyber attacks, there exists still a long way in considering different types of attacks when PF methods are desired. Thus, it is suggested to consider other cyber attack scenarios such as the replay one for state estimation of networked non-linear non-Gaussain systems. Moreover, applying the proposed method on some practical applications, such as detection of the FDI attack on smart grids, is of our interest, as the future research work.

REFERENCES

[1] N. Sadeghzadeh-Nokhodberiz and N. Meskin, "Protocol-based particle filtering and divergence estimation," *IEEE Syst. J.*, vol. 15, no. 3, pp. 4537–4544, Sep. 2021.
[2] N. Sadeghzadeh, A. Afshar, and M. B. Menhaj, "An MLP neural network for time delay prediction in networked control systems," in *Proc. Chin. Control Decis. Conf.*, Jul. 2008, pp. 5314–5318.
[3] X.-M. Zhang, Q.-L. Han, X. Ge, D. Ding, L. Ding, D. Yue, and C. Peng, "Networked control systems: A survey of trends and techniques," *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 1, pp. 1–17, Jun. 2020.
[4] Z.-H. Pang, L.-Z. Fan, J. Sun, K. Liu, and G.-P. Liu, "Detection of stealthy false data injection attacks against networked control systems via active data modification," *Inf. Sci.*, vol. 546, pp. 192–205, Feb. 2021.
[5] M. Xia, V. Gupta, and P. J. Antsaklis, "Networked state estimation over a shared communication medium," *IEEE Trans. Autom. Control*, vol. 62, no. 4, pp. 1729–1741, Apr. 2017.
[6] N. Sadeghzadeh-Nokhodberiz, M. Davoodi, and N. Meskin, "Event-triggered particle filtering and Cramér–Rao lower bound computation," *Proc. Inst. Mech. Eng., I, J. Syst. Control Eng.*, vol. 235, no. 4, pp. 503–516, 2020.
[7] Q. Liu, R. Ding, and C. Chen, "State estimation of networked control systems over limited capacity and dropout channels," *Arch. Control Sci.*, vol. 29, no. 4, pp. 1–11, 2019.
[8] Y. Tipsuwan and M.-Y. Chow, "Control methodologies in networked control systems," *Control Eng. Pract.*, vol. 11, no. 10, pp. 1099–1111, Oct. 2003.
[9] M. S. Mahmoud and M. M. Hamdan, "Fundamental issues in networked control systems," *IEEE/CAA J. Autom. Sinica*, vol. 5, no. 5, pp. 902–922, Sep. 2018.
[10] A. Cetinkaya, H. Ishii, and T. Hayakawa, "An overview on denial-of-service attacks in control systems: Attack models and security analyses," *Entropy*, vol. 21, no. 2, p. 210, Feb. 2019.
[11] L. Hu, Z. Wang, Q. Han, and X. Liu, "State estimation under false data injection attacks: Security analysis and system protection," *Automatica*, vol. 87, pp. 176–183, Jan. 2018.
[12] L. Li, H. Yang, Y. Xia, and H. Yang, "State estimation for linear systems with unknown input and random false data injection attack," *IET Control Theory Appl.*, vol. 13, no. 6, pp. 823–831, Apr. 2019.
[13] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, Jan. 2015.
[14] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, "Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach," *IEEE Trans. Autom. Control*, vol. 60, no. 10, pp. 2831–2836, Oct. 2015.
[15] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 3023–3028, Nov. 2015.
[16] J. Qin, M. Li, L. Shi, and X. Yu, "Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks," *IEEE Trans. Autom. Control*, vol. 63, no. 6, pp. 1648–1663, Jun. 2018.
[17] Y. Mo, S. Weerakkody, and B. Sinopoli, "Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs," *IEEE Control Syst.*, vol. 35, no. 1, pp. 93–109, Feb. 2015.
[18] P. Griffioen, S. Weerakkody, B. Sinopoli, O. Ozel, and Y. Mo, "A tutorial on detecting security attacks on cyber-physical systems," in *Proc. 18th Eur. Control Conf. (ECC)*, Jun. 2019, pp. 979–984.
[19] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, "Optimal linear cyber-attack on remote state estimation," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 4–13, Mar. 2017.
[20] A. Doucet, S. Godsill, and C. Andrieu, "On sequential Monte Carlo sampling methods for Bayesian filtering," *Statist. Comput.*, vol. 10, no. 3, pp. 197–208, Jul. 2000.
[21] M. S. Arulampalam, S. Maskell, N. Gordon, and T. Clapp, "A tutorial on particle filters for online nonlinear/non-Gaussian Bayesian tracking," *IEEE Trans. Signal Process.*, vol. 50, no. 2, pp. 174–188, Feb. 2002.
[22] S. M. Kay, *Fundamentals of Statistical Signal Processing*. Upper Saddle River, NJ, USA: Prentice-Hall, 1993.
[23] F. Lindesten, "Particle filters and Markov chains for learning of dynamical systems," Ph.D. dissertation, Linkoping Univ. Electron. Press, 2013.

[24] M. S. Grewal and A. P. Andrews, *Kalman Filtering: Theory and Practice With MATLAB*. Hoboken, NJ, USA: Wiley, 2014.
[25] N. Sadeghzadeh-Nokhodberiz, J. Poshtan, and Z. Shahrokhi, "Particle filtering based gyroscope fault and attitude estimation with uncertain dynamics fusing camera information," in *Proc. 22nd Iranian Conf. Electr. Eng. (ICEE)*, May 2014, pp. 1221–1226.
[26] M. Klaas, N. de Freitas, and A. Doucet, "Toward practical N2 Monte Carlo: The marginal particle filter," 2012, *arXiv:1207.1396*.
[27] W. Li, Z. Wang, Y. Yuan, and L. Guo, "Particle filtering with applications in networked systems: A survey," *Complex Intell. Syst.*, vol. 2, no. 4, pp. 293–315, Dec. 2016.
[28] C. Yang and H. Fang, "Modified particle filter and Gaussian filter with packet dropouts," *Int. J. Robust Nonlinear Control*, vol. 28, no. 8, pp. 2961–2975, May 2018.
[29] H. Li, X. He, Y. Zhang, and W. Guan, "Attack detection in cyber-physical systems using particle filter: An illustration on three-tank system," in *Proc. IEEE 8th Annu. Int. Conf. CYBER Technol. Automat., Control, Intell. Syst. (CYBER)*, Jul. 2018, pp. 504–509.
[30] M. Khalaf, A. Youssef, and E. El-Saadany, "A particle filter-based approach for the detection of false data injection attacks on automatic generation control systems," in *Proc. IEEE Electr. Power Energy Conf. (EPEC)*, Oct. 2018, pp. 1–6.
[31] W. Song, Z. Wang, J. Wang, F. E. Alsaadi, and J. Shan, "Secure particle filtering for cyber-physical systems with binary sensors under multiple attacks," *IEEE Syst. J.*, early access, Mar. 26, 2021, doi: 10.1109/JSYST.2021.3064920.
[32] A. M. H. Teixeira and R. M. G. Ferrari, "Detection of sensor data injection attacks with multiplicative watermarking," in *Proc. Eur. Control Conf. (ECC)*, Jun. 2018, pp. 338–343.
[33] J. Huang, D. W. C. Ho, F. Li, W. Yang, and Y. Tang, "Secure remote state estimation against linear man-in-the-middle attacks using watermarking," *Automatica*, vol. 121, Nov. 2020, Art. no. 109182.
[34] D. Wang, J. Huang, Y. Tang, and F. Li, "A watermarking strategy against linear deception attacks on remote state estimation under K–L divergence," *IEEE Trans. Ind. Informat.*, vol. 17, no. 5, pp. 3273–3281, May 2021.
[35] S. T. M. Montemerlo, "FastSLAM 2.0," in *FastSLAM: A Scalable Method for the Simultaneous Localization and Mapping Problem in Robotics*. Berlin, Germany: Springer, pp. 63–90, doi: 10.1007/978-3-540-46402-0_4.
[36] M. Montemerlo, S. Thrun, D. Koller, and B. Wegbreit, "FastSLAM 2.0: An improved particle filtering algorithm for simultaneous localization and mapping that provably converges," in *Proc. IJCAI*, vol. 3, 2003, pp. 1151–1156.
[37] J.-A. Fernández-Madrigal, *Simultaneous Localization and Mapping for Mobile Robots: Introduction and Methods: Introduction and Methods*. Hershey, PA, USA: IGI Global, 2012.
[38] N. Sadeghzadeh-Nokhodberiz, A. Can, R. Stolkin, and A. Montazeri, "Dynamics-based modified fast simultaneous localization and mapping for unmanned aerial vehicles with joint inertial sensor bias and drift estimation," *IEEE Access*, vol. 9, pp. 120247–120260, 2021.
[39] Y. Gu, X. Yu, K. Guo, J. Qiao, and L. Guo, "Detection, estimation, and compensation of false data injection attack for UAVs," *Inf. Sci.*, vol. 546, pp. 723–741, Feb. 2021.
[40] J. Lu, W. Wang, L. Li, and Y. Guo, "Unscented Kalman filtering for nonlinear systems with sensor saturation and randomly occurring false data injection attacks," *Asian J. Control*, vol. 23, no. 2, pp. 871–881, Mar. 2021.
[41] A. Doucet and A. M. Johansen, "A tutorial on particle filtering and smoothing: Fifteen years later," in *Handbook of Nonlinear Filtering*, vol. 12, nos. 656–704. Cambridge, U.K.: Cambridge Univ. Press, 2009, p. 3.
[42] N. Sadeghzadeh-Nokhodberiz, M. Davoodi, and N. Meskin, "Stochastic event-triggered particle filtering for state estimation," in *Proc. 2nd Int. Conf. Event-based Control, Commun., Signal Process. (EBCCSP)*, Jun. 2016, pp. 1–4.
[43] P. E. Greenwood and M. S. Nikulin, *A Guide to Chi-Squared Testing*, vol. 280. Hoboken, NJ, USA: Wiley, 1996.
[44] J. L. Speyer and W. H. Chung, *Stochastic Processes, Estimation, and Control*, vol. 17. Philadelphia, PA, USA: SIAM, 2008.
[45] N. A. Weiss and M. J. Hassett, *Introductory Statistics*. Boston, MA, USA: Addison-Wesley, 1999.
[46] N. S. Nokhodberiz and J. Poshtan, "Belief consensus–based distributed particle filters for fault diagnosis of non-linear distributed systems," *Proc. Inst. Mech. Eng., I, J. Syst. Control Eng.*, vol. 228, no. 3, pp. 123–137, Mar. 2014.

NARGESS SADEGHZADEH-NOKHODBERIZ received the B.Sc. and M.Sc. degrees in control engineering from the Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran, in 2006 and 2008, respectively, and the Ph.D. degree in control engineering from the Iran University of Science and Technology, Tehran, in collaboration with the Automation Laboratory, Heidelberg University, Heidelberg, Germany, in September 2014. She was with the Department of Engineering, Islamic Azad University Central Tehran Branch, Tehran, as an Assistant Professor, from 2015 to 2019. She was as a Visiting Scholar with the Department of Electrical Engineering, Qatar University, Doha, Qatar, in 2016, and the Department of Engineering, Lancaster University, Lancaster, U.K., in 2018. Since 2019, she has been as an Assistant Professor with the Department of Electrical and Computer Engineering, Qom University of Technology, Qom, Iran. Her research interests include control systems theory, Monte Carlo state estimation, cyber-physical systems and networked control systems, mobile robot localization and mapping (SLAM), fault diagnosis, and distributed computing for control system applications.

NADER MESKIN (Senior Member, IEEE) received the B.Sc. degree from the Sharif University of Technology, Tehran, Iran, in 1998, the M.Sc. degree from the University of Tehran, Tehran, in 2001, and the Ph.D. degree in electrical and computer engineering from Concordia University, Montreal, QC, Canada, in 2008. He was a Postdoctoral Fellow with Texas A&M University at Qatar, Doha, Qatar, from January 2010 to December 2010. He is currently an Associate Professor with Qatar University, Doha, and an Adjunct Associate Professor with Concordia University. He has authored more than 190 refereed journals and conference papers. He is also the coauthor (with K. Khorasani) of the book *Fault Detection and Isolation: MultiVehicle Unmanned Systems* (Springer, 2011). His research interests include fault detection and isolation, multiagent systems, active control for clinical pharmacology, and linear parameter varying systems.

SAEED HASANZADEH was born in Shirvan, Iran, in 1981. He received the B.Sc. degree in electrical engineering from the Shahroud University of Technology, Shahroud, Iran, in 2003, and the M.Sc. and Ph.D. degrees in electrical engineering from the University of Tehran (UT), Tehran, Iran, in 2006 and 2012, respectively. His M.Sc. thesis and Ph.D. dissertation have been conducted in the field of high voltage engineering and wireless power transfer (WPT), respectively. In 2013, he joined the Department of Electrical and Computer Engineering, Qom University of Technology, as an Assistant Professor. He is currently the Dean of the Department of Electrical and Computer Engineering (ECE), Qom University of Technology. His current research interests include power electronics, electrical machines, wireless power transfer, and high voltage engineering. He was a recipient of the Top Research Prize of Qom University of Technology, in 2019. He was also recognized as an Outstanding Lecturer with the Qom University of Technology, in 2020. He is a TPC Member of the IEEE Power Electronics & Drives: Systems and Technologies Conference (PEDSTC). He is an Editorial Board of the Power Electronics Society of Iran (PELSI).