This article has been accepted for publication in a future proceedings of this conference, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/ICAC65379.2025.11196717, 2025 30th International Conference on Automation and Computing (ICAC)

Encryption-Decryption-Based Particle Filtering for Stochastic Systems With Randomly Switching Nonlinearities and Sensor Resolutions

Weihao Song[1,2], Zidong Wang[2], and Zhongkui Li[1]
[1] School of Advanced Manufacturing and Robotics, Peking University, Beijing 100871, China
[2] Department of Computer Science, Brunel University London, Uxbridge, Middlesex, UB8 3PH, United Kingdom
Emails: weihao.song@pku.edu.cn, Zidong.Wang@brunel.ac.uk, zhongkli@pku.edu.cn

***Abstract*—In this paper, the secure particle filtering problem is investigated for a class of stochastic nonlinear systems subject to non-Gaussian noises and randomly switching nonlinearities. As an essential characteristic of real-world sensors, the sensor resolution is incorporated into the measurement model to provide a realistic representation of the available data. By resorting to the exclusive or logical operations, an encryption-decryption-based scheme is leveraged to enhance the transmission security of measurements and lower the communication overhead. The objective of this paper is to design a novel particle filtering scheme in the coexistence of randomly switching nonlinearities, non-Gaussian noises, sensor resolution effects and decrypted measurements. Specifically, a mixture distribution, employing the statistical property of the randomly switching nonlinearities, is constructed to generate the new particles. By considering the effects of sensor resolutions and decryption errors, the likelihood function is parameterized to facilitate the update of weights. Finally, a numerical example with Monte Carlo simulations is presented to illustrate the effectiveness of the proposed filtering algorithm.**

***Index Terms*—Encryption-decryption scheme, particle filtering, randomly switching nonlinearities, sensor resolution, non-Gaussian noises.**

I. Introduction

Over the past several decades, nonlinear state estimation or filtering problem has remained an active area of research due mainly to its indispensable role across diverse engineering domains which include, but are not limited to, robotics, industrial process control, power systems, environmental monitoring, and autonomous vehicles [1]–[3]. Consequently, a plethora of nonlinear filtering approaches, customized for various system dynamics and noise specifications, has been developed in the literature. Several typical strategies are extended Kalman filtering, unscented Kalman filtering, set-membership filtering, and H_∞ filtering [4]–[6]. For example, a dynamic event-triggered H_∞ state estimator has been designed in [7] for a class of delayed neural networks with sector-bounded nonlinear activation functions, gain fluctuations and energy-bounded noises. In [8], the distributed extended Kalman filtering problem has been solved for saturated systems with differentiable nonlinearity, amplify-and-forward relays and Gaussian noises.

This work was supported in part by the National Natural Science Foundation of China under Grant 62203016, in part by the China Postdoctoral Science Foundation under Grant 2021TQ0009, in part by the Royal Society of the U.K., and in part by the Alexander von Humboldt Foundation of Germany.

With the increasing demand for the accurate state estimation in practical applications involving strong nonlinearities and non-Gaussian noises, particle filtering has attracted considerable research attention in recent years. Different from the traditional linearization-based or Gaussian-assumption-based methods, the particle filtering approach aims to approximate the posterior distribution of the system state based on a group of weighted particles [9]–[11]. Such a sampling-based strategy endows particle filter with the outstanding ability to deal with various complicated system dynamics and non-Gaussian noises. Recently, the phenomenon of randomly switching nonlinearities, caused probably by abrupt environmental perturbations and intermittent switchings between subsystems, has begun to receive initial attention [12]. Nevertheless, the corresponding state estimation problem, where the switched nonlinearities are not restricted to any specific type, would be particularly challenging (if not impossible) by using the traditional methods. Therefore, a seemingly natural approach is to address such nonlinearities within the particle filtering framework.

In the context of remote state estimation, the signal transmission between sensors and the remote estimator typically depends on the network communication technology. Nevertheless, in practical engineering, the open and shared nature of communication networks noticeably increase the vulnerability of signal transmission to cybersecurity threats, particularly the risk of data eavesdropping [13]. These vulnerabilities are highly likely to threaten the measurement integrity and leak the confidential information, thereby resulting in deteriorated estimation performance. To this end, considerable research attention has been devoted to the study of secure state estimation problem, see [14] and the references therein. For example, the secure set-membership filtering problem has been studied in [15] for two-dimensional systems under the exclusive-or-based encryption-decryption strategy and the unknown but bounded noises. Nevertheless, when it comes to the stochastic systems subject to randomly switching nonlinearities and non-Gaussian noises, the available results have been really scattered, which motivates this current investigation.

On the other hand, in real-world applications, it is almost impossible for sensors to detect arbitrarily minute changes in measurement signals owing to the technical limitations

This article has been accepted for publication in a future proceedings of this conference, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/ICAC65379.2025.11196717, 2025 30th International Conference on Automation and Computing (ICAC)

[16]. The sensor resolution is typically determined by the manufacturing cost, and the inexpensive sensors often feature low resolving ability and large measurement biases. Therefore, some research efforts have been directed toward the state estimation problem under the sensor resolution effects [17]. Particularly, the state estimator has been developed in [18] for artificial neural networks with Lipschitz continuous nonlinearities, sensor resolution effects and unknown but bounded noises. Unfortunately, in case that the randomly switching general nonlinearities and non-Gaussian noises are concerned, the corresponding state estimation problem has not been thoroughly investigated yet.

Summarizing the above discussions, this paper aims to tackle the encryption-decryption-based state estimation problem for a class of stochastic systems with randomly switching nonlinearities, sensor resolution effects, and non-Gaussian noises. In doing so, two difficulties arise as follows: 1) how to develop a suitable secure filtering framework capable of handling the considered complexities? and 2) how to diminish the impact of these complicated phenomena on the filtering performance? The contributions of this paper can be highlighted from the following two aspects: 1) the encryption-decryption-based secure state estimation problem is, for the first time, investigated for a class of stochastic systems subject to randomly switching nonlinearities, sensor resolution effects and non-Gaussian noises; and 2) an easy-to-implement particle filtering scheme is proposed by carefully designing the particle generation process and parameterizing the expression of likelihood function based on the decrypted measurements.

II. Problem Formulation and Preliminaries

A. System Description

Consider a class of stochastic nonlinear systems governed by the following dynamics:

$$\begin{cases} x(t+1) = F(t)x(t) + \gamma(t)f(x(t)) \\ \qquad\quad + (1-\gamma(t))g(x(t)) + \eta(t) \\ z_s(t) = h_s(x(t)) + \zeta_s(t),\ s = 1, 2, \ldots, N \end{cases} \tag{1}$$

where $x(t) \in \mathbb{R}^{n_x}$ and $z_s(t) \in \mathbb{R}$ represent, respectively, the system state vector and the measurement output of the sth sensor at time instant t. $F(t) \in \mathbb{R}^{n_x \times n_x}$ denotes a known real-valued matrix. $h_s(\cdot) : \mathbb{R}^{n_x} \mapsto \mathbb{R}$ signifies the known measurement function of the sth sensor. $\eta(t) \in \mathbb{R}^{n_x}$ stands for the process noise satisfying $p_{\eta(t)}(\cdot)$ and $\zeta_s(t) \in \mathbb{R}$ denotes the measurement noise of the sth sensor satisfying $p_{\zeta_s(t)}(\cdot)$. $f(\cdot) : \mathbb{R}^{n_x} \mapsto \mathbb{R}^{n_x}$ and $g(\cdot) : \mathbb{R}^{n_x} \mapsto \mathbb{R}^{n_x}$ indicate the known nonlinear vector-valued functions, and the switching behavior between them is characterized by a Bernoulli distributed random variable $\gamma(t)$ with the following probability distribution:

$$\begin{cases} \Pr\{\gamma(t) = 1\} = \bar{\gamma}_f \\ \Pr\{\gamma(t) = 0\} = 1 - \bar{\gamma}_f \end{cases} \tag{2}$$

where the known constant $\bar{\gamma}_f \in [0, 1]$ represents the probability that the nonlinear function $f(\cdot)$ is activated in the system dynamics.

Before proceeding further, let us present the following two common assumptions.

Assumption 1: The initial state vector $x(0)$ follows a prior distribution with known $p_{x(0)}(\cdot)$.

Assumption 2: The process noise $\eta(t)$, the measurement noises $\zeta_s(t)$ $(s = 1, 2, \ldots, N)$, the random variable $\gamma(t)$, and the initial state vector are mutually independent.

In engineering practice, it is well recognized that the sensors cannot detect arbitrarily small changes in measurements due to the inherent limitations of sensor resolution. Similar to [17]–[19], the actual measurement output $\vec{z}_s(t)$ of the sth sensor at time instant t under the effect of sensor resolution can be described by

$$\vec{z}_s(t) = \begin{cases} \left\lfloor \frac{z_s(t)}{l_s} \right\rfloor l_s, & z_s(t) \geq l_s \\ 0, & z_s(t) \in (-l_s, l_s) \\ \left\lceil \frac{z_s(t)}{l_s} \right\rceil l_s, & z_s(t) \leq -l_s \end{cases} \tag{3}$$

where l_s signifies the sensor resolution of the sth sensor and the notation $\lfloor \cdot \rfloor$ ($\lceil \cdot \rceil$) represents the floor (ceil) function.

B. Encryption-Decryption-Based Transmission Scheme

In this paper, the measurement outputs are transmitted to the remote state estimator over a wireless communication network. Following the similar line of [15], the exclusive-or-based encryption-decryption scheme is adopted to enhance the transmission security and reduce the communication overhead.

1) Encrypter: To begin with, let us consider the following uniform quantizer $\mathcal{U}(\cdot)$ with input signal λ and range $[-\Lambda, \Lambda]$:

$$\mathcal{U}(\lambda) = \begin{cases} \Lambda, & \lambda \geq \Lambda \\ -\Lambda + \frac{(2k-1)\Lambda}{K}, & \lambda \in \left[-\Lambda + \frac{2(k-1)\Lambda}{K}, -\Lambda + \frac{2k\Lambda}{K} \right) \\ -\Lambda, & \lambda < -\Lambda \end{cases} \tag{4}$$

where $k \in \{1, 2, \ldots, K\}$ and K denotes the quantization level. To avoid the occurrence of quantizer saturation, let us define $\mathcal{U}_{\omega_s}(\vec{z}_s(t)) \triangleq \omega_s(t)\mathcal{U}(\frac{\vec{z}_s(t)}{\omega_s(t)})$, where $\omega_s(t)$ signifies an adjustable scaling parameter, ensuring that $|\frac{\vec{z}_s(t)}{\omega_s(t)}| < \Lambda$ when the actual measurement output exceeds the range. It is not difficult to see that the quantization error, denoted by $\xi_s(t) \triangleq \vec{z}_s(t) - \mathcal{U}_{\omega_s}(\vec{z}_s(t))$, satisfies the following condition:

$$|\xi_s(t)| \leq \frac{\omega_s(t)\Lambda}{K}. \tag{5}$$

The quantized measurement $\mathcal{U}_{\omega_s}(\vec{z}_s(t))$ for the sth sensor, corresponding to the index $k(t) \in \{1, 2, \ldots, K\}$, is encoded into a binary bit string denoted by $\mathcal{B}_s(t) \triangleq \{b_{s,1}(t), b_{s,2}(t), \ldots, b_{s,L}(t)\}$, $b_{s,i}(t) \in \{0, 1\}$, $i = 1, 2, \ldots, L$, where L represents the length of the binary bit string and satisfies $K = 2^L$. Subsequently, such a binary bit string, referred to as the plaintext, is encrypted by resorting to the following operation:

$$\bar{\mathcal{B}}_s(t) = \mathrm{XOR}(\mathcal{B}_s(t), \mathcal{E}_s(t)) \tag{6}$$

where $\bar{\mathcal{B}}_s(t)$ and $\mathcal{E}_s(t)$ represent, respectively, the ciphertext to be transmitted and the pregenerated key sequence. The

This article has been accepted for publication in a future proceedings of this conference, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/ICAC65379.2025.11196717, 2025 30th International Conference on Automation and Computing (ICAC)

notation $\mathrm{XOR}(\cdot,\cdot)$ denotes the componentwise exclusive or logical operation on pairs of binary bit strings.

Assumption 3: The binary bit strings are transmitted over the wireless channel without any bit errors or time delays.

2) Decrypter: Based on the received ciphertext $\bar{\mathcal{B}}_s(t)$, the decrypted bit string $\tilde{\mathcal{B}}_s(t)$ can be obtained as follows:

$$\tilde{\mathcal{B}}_s(t) = \mathrm{XOR}(\bar{\mathcal{B}}_s(t), \mathcal{E}_s(t)). \tag{7}$$

Obviously, according to Assumption 3, the binary bit strings $\tilde{\mathcal{B}}_s(t)$ and $\mathcal{B}_s(t)$ are identical, which means that $\mathcal{B}_s(t)$ can be recovered by using the key sequence $\mathcal{E}_s(t)$. The decrypted binary bit string $\tilde{\mathcal{B}}_s(t)$ is subsequently transformed into a decimal-valued measurement signal $\tilde{z}_s(t)$ for estimation purposes.

Remark 1: It is important to note that Assumption 3 is critical for ensuring the successful decryption. If the wireless channels are prone to cyber attacks and potential data tampering, error-detecting techniques such as cyclic redundancy check [20] can be utilized to identify transmission errors and enhance data integrity. When errors are detected in the binary data, a straightforward yet feasible solution is to discard such erroneous data and treat the corresponding measurement information as unavailable.

C. Preliminaries on Particle Filtering Approach

To begin with, let us define all the available measurements up to time instant t as $\mathcal{Z}_1^N(1:t) \triangleq \left[\mathcal{Z}_1^N(1)^T \quad \mathcal{Z}_1^N(2)^T \quad \cdots \quad \mathcal{Z}_1^N(t)^T\right]^T$, where $\mathcal{Z}_1^N(t) \triangleq \left[\tilde{z}_1(t) \quad \tilde{z}_2(t) \quad \cdots \quad \tilde{z}_N(t)\right]^T$. It is well known that based on the measurements $\mathcal{Z}_1^N(1:t)$, the minimum mean-square error estimate for the state vector, denoted by $\hat{x}(t)$, can be calculated by

$$\hat{x}(t) = \int x(t) p(x(t)|\mathcal{Z}_1^N(1:t))\mathrm{d}x(t) \tag{8}$$

where $p(x(t)|\mathcal{Z}_1^N(1:t))$ denotes the posterior probability density function and is updated in the following manner [21]:

$$\begin{cases} p(x(t)|\mathcal{Z}_1^N(1:t-1)) \\ \quad = \displaystyle\int p(x(t)|x(t-1))p(x(t-1)|\mathcal{Z}_1^N(1:t-1))\mathrm{d}x(t-1) \\ p(x(t)|\mathcal{Z}_1^N(1:t)) \\ \quad = \dfrac{p(\mathcal{Z}_1^N(t)|x(t))p(x(t)|\mathcal{Z}_1^N(1:t-1))}{\int p(\mathcal{Z}_1^N(t)|x(t))p(x(t)|\mathcal{Z}_1^N(1:t-1))\mathrm{d}x(t)}. \end{cases}$$

It should be noted that such a recursive propagation is generally not analytically tractable due to the complexity of the involved integrals. To this end, the particle filtering method [9] is developed to provide a numerical approximation solution for the posterior probability density function as follows:

$$p(x(t)|\mathcal{Z}_1^N(1:t)) \approx \sum_{m=1}^{M} w^m(t)\Delta(x(t) - x^m(t)) \tag{9}$$

$$w^m(t) = w^m(t-1)p(\mathcal{Z}_1^N(t)|x^m(t)) \tag{10}$$

where $\Delta(\cdot)$ signifies the Dirac delta function, M denotes the number of sampled particles, and $x^m(t)$, sampled from the prior density $p(x(t)|x^m(t-1))$ at time instant t, represents the mth particle with the importance weight $w^m(t)$.

The objective of this paper is to design a state estimation scheme such that: 1) the transmission security of the measurement outputs can be ensured by leveraging the exclusive-or-based encryption-decryption scheme; and 2) the joint impacts of the randomly switching nonlinearities, non-Gaussian noises, sensor resolutions and decryption errors can be effectively compensated for by carefully designing the particle filtering algorithm.

III. Design of Encryption-Decryption-Based Particle Filtering Algorithm

In this section, we are going to develop a modified particle filtering algorithm to tackle the complexities arising from the concurrent presence of randomly switching nonlinearities, non-Gaussian noises, sensor resolutions and decryption errors.

As indicated in (9) and (10), the new particle $x^m(t)$ is typically sampled from the prior density $p(x(t)|x^m(t-1))$ in standard particle filtering algorithm, where the sampling process is primarily determined by the known statistics of the process noise $\eta(t)$. Nevertheless, due to the existence of randomly switching nonlinearities, the statistical property of the random variable $\gamma(t)$ (specified in (2)) should also be taken into consideration. Subsequently, following the similar line of [11], it can be obtained from the law of total probability, the system dynamics (1), and Assumption 2 that

$$\begin{aligned} & p\left(x(t)|x^m(t-1)\right) \\ &= p\left(x(t)|x^m(t-1), \gamma(t-1)=0\right)\left(1-\bar{\gamma}_f\right) \\ &\quad + p\left(x(t)|x^m(t-1), \gamma(t-1)=1\right)\bar{\gamma}_f \\ &= p\left(x(t)|F(t-1)x^m(t-1) + g(x^m(t-1))\right)\left(1-\bar{\gamma}_f\right) \\ &\quad + p\left(x(t)|F(t-1)x^m(t-1) + f(x^m(t-1))\right)\bar{\gamma}_f. \end{aligned} \tag{11}$$

In other words, the particles should be sampled from a mixture distribution described by (11), where the mixture weight is governed by the statistical property of nonlinearity switching behaviors.

To proceed, let us focus on formulating an update expression for the importance weight $w^m(t)$ associated with the mth particle $x^m(t)$. It is clear from (10) that the key procedure is to parameterize the likelihood function $p(\mathcal{Z}_1^N(t)|x^m(t))$ by accounting for the cumulative effects of sensor resolutions and decryption errors.

Based on (3)-(7), it is not difficult to obtain that

$$\begin{aligned} & |z_s(t) - \tilde{z}_s(t)| \\ =\ & |z_s(t) - \mathcal{U}_{\omega_s}(\vec{z}_s(t))| \\ \le\ & |z_s(t) - \vec{z}_s(t)| + |\vec{z}_s(t) - \mathcal{U}_{\omega_s}(\vec{z}_s(t))| \\ <\ & \frac{\omega_s(t)\Lambda}{K} + l_s \triangleq \bar{L}_s(t). \end{aligned} \tag{12}$$

Then, according to (12) and the measurement model in (1), the likelihood function associated with the sth sensor and the mth particle $x^m(t)$, denoted by $p(\tilde{z}_s(t)|x^m(t))$, can be evaluated as follows:

$$p\left(\tilde{z}_s(t)|x^m(t)\right)$$

This article has been accepted for publication in a future proceedings of this conference, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/ICAC65379.2025.11196717, 2025 30th International Conference on Automation and Computing (ICAC)

$$\begin{aligned}
&\approx p\left(\tilde{z}_s(t)-\bar{L}_s(t)<z_s(t)<\tilde{z}_s(t)+\bar{L}_s(t)|x^m(t)\right)\\
&=p\left(\bar{H}_s^-(x^m(t))<\zeta_s(t)<\bar{H}_s^+(x^m(t))\right)\\
&=\Phi_{\zeta_s(t)}\left(\bar{H}_s^+(x^m(t))\right)-\Phi_{\zeta_s(t)}\left(\bar{H}_s^-(x^m(t))\right) \qquad (13)
\end{aligned}$$

where $\Phi_{\zeta_s(t)}(\cdot)$ stands for the cumulative distribution function of the measurement noise $\zeta_s(t)$, $\bar{H}_s^-(x^m(t))=\tilde{z}_s(t)-\bar{L}_s(t)-h_s(x^m(t))$, and $\bar{H}_s^+(x^m(t))=\tilde{z}_s(t)+\bar{L}_s(t)-h_s(x^m(t))$.

On the other hand, it follows from Assumption 2 that

$$p(\mathcal{Z}_1^N(t)|x^m(t))=\prod_{s=1}^{N}p\left(\tilde{z}_s(t)|x^m(t)\right). \qquad (14)$$

Therefore, according to (10), (13) and (14), the importance weight $w^m(t)$ associated with the mth particle $x^m(t)$ can be updated by

$$\begin{aligned}
w^m(t)=w^m(t-1)\prod_{s=1}^{N}&\left[\Phi_{\zeta_s(t)}\left(\bar{H}_s^+(x^m(t))\right)\right.\\
&\left.-\Phi_{\zeta_s(t)}\left(\bar{H}_s^-(x^m(t))\right)\right]. \qquad (15)
\end{aligned}$$

In what follows, the developed encryption-decryption-based particle filtering algorithm is detailed in Algorithm 1 for ease of practical implementation.

Algorithm 1 Encryption-decryption-based particle filtering algorithm under sensor resolution effects and randomly switching nonlinearities.

1: **Initialization**: Sample M particles from the prior density $p_{x(0)}(\cdot)$ with equally assigned importance weights and set the maximum recursive time instant as T.
2: **for** $t=1$ to T **do**
3: Decrypt the received ciphertext $\bar{\mathcal{B}}_s(t)$ and accordingly generate the measurement signal $\tilde{z}_s(t)$ with respect to the sth sensor.
4: **for** $m=1$ to M **do**
5: Draw new particle $x^m(t)$ from the mixture distribution specified in (11).
6: Assign unnormalized importance weight $\bar{w}^m(t)$ for the newly generated particle $x^m(t)$ according to (15), where the term on the left-hand side is substituted with $\bar{w}^m(t)$.
7: **end for**
8: **for** $m=1$ to M **do**
9: Update the normalized importance weight by employing $w^m(t)=\frac{\bar{w}^m(t)}{\sum_{i=1}^{M}\bar{w}^i(t)}$.
10: **end for**
11: Generate the state estimate $\hat{x}(t)$ based on the following expression:

$$\hat{x}(t)=\sum_{m=1}^{M}w^m(t)x^m(t).$$

12: Perform the resampling process if necessary (e.g., when the effective sample size is less than a given value).
13: **end for**

Remark 2: It should be noted that, in this paper, although only two nonlinear functions are involved in the system dynamics (1), the proposed sampling method with the form of (11) can also be extended to handle the randomly switching behaviors among multiple nonlinear functions. On the other hand, if the expression of the likelihood function is modified as follows:

$$p(\mathcal{Z}_1^N(t)|x^m(t))=\prod_{s=1}^{N}(p\left(\tilde{z}_s(t)|x^m(t)\right))^{\alpha_s(t)}$$

where $\alpha_s(t)$ is a binary indicator variable characterizing whether or not the ciphertext $\bar{\mathcal{B}}_s(t)$ is successfully received without errors (as discussed in Remark 1), then the proposed algorithm is also applicable to the scenario with transmission errors or packet dropouts. In this sense, the developed algorithm is quite general and exhibits widespread applicability.

IV. Simulation Results

In this section, we would like to offer a numerical example to illustrate the viability and effectiveness of the proposed particle filtering scheme under randomly switching nonlinearities and sensor resolution effects.

Consider a stochastic nonlinear system described by (1) with the following specifications:

$$\begin{aligned}
F(t)&=\begin{bmatrix}0.85 & -0.2\\ -0.2 & 0.76\end{bmatrix},\\
f(x(t))&=\begin{bmatrix}-0.25\tanh(x_2(t))\\ 0.35\tanh(x_1(t))\end{bmatrix},\\
g(x(t))&=\begin{bmatrix}0.32\tanh(x_1(t))\\ -0.28\tanh(x_2(t))\end{bmatrix},\\
h_1(x(t))&=2\sin(x_1(t)-x_2(t)),\\
h_2(x(t))&=-2\cos(x_1(t)+x_2(t)).
\end{aligned}$$

The process noise $\eta(t)$ is considered to obey the Gaussian mixture distribution with the following probability density function:

$$p(\eta(t))=(1-\rho)\mathcal{N}(\bar{\eta}_1,\Sigma_{\eta 1})+\rho\mathcal{N}(\bar{\eta}_2,\Sigma_{\eta 2})$$

where $\rho=0.2$ signifies the mixture weight. The mean parameters are set as zero vectors and the covariance parameters are set as $\Sigma_{\eta 1}=\mathrm{diag}\{0.02^2,0.02^2\}$ and $\Sigma_{\eta 2}=\mathrm{diag}\{0.1^2,0.1^2\}$.

The measurement noises $\zeta_s(t)$ follow the standard Gaussian distribution truncated to the interval $[-2,2]$. Other parameters are chosen as $l_s=0.2$, $\omega_s(t)=1$, $K=8$, $\Lambda=4$, $\bar{\gamma}_f=0.5$, $M=200$, and $T=120$. The initial state vector $x(0)$ satisfies the Gaussian distribution with mean $[2,-2]^T$ and covariance $\mathrm{diag}\{1.2^2,1.2^2\}$.

The simulation results in one realization are displayed in Figs. 1-4. Specifically, Figs. 1 and 2 show the trajectories of the true state and the corresponding state estimate, and Figs. 3 and 4 depict the ideal measurements, actual measurements and decrypted measurements. Clearly, the proposed particle filtering algorithm is able to well track the state behaviors in the presence of randomly switching nonlinearities, sensor resolution effects, and decryption errors.

This article has been accepted for publication in a future proceedings of this conference, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/ICAC65379.2025.11196717, 2025 30th International Conference on Automation and Computing (ICAC)

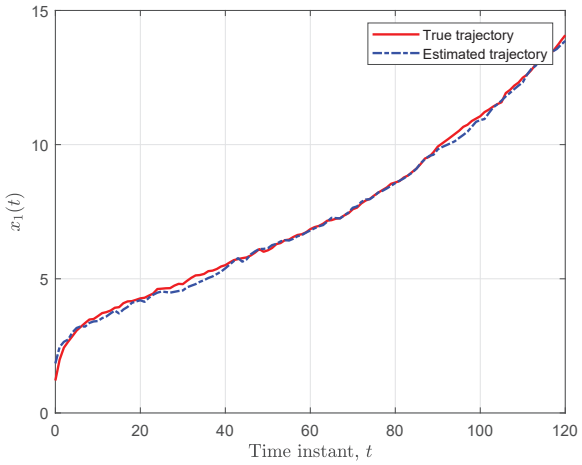

Fig. 1: True and estimated trajectories of the first state component.

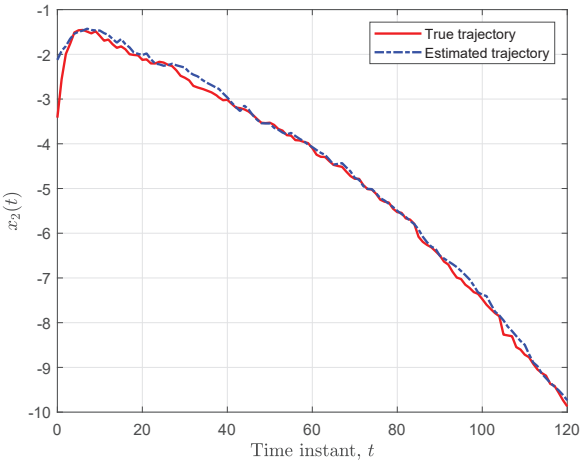

Fig. 2: True and estimated trajectories of the second state component.

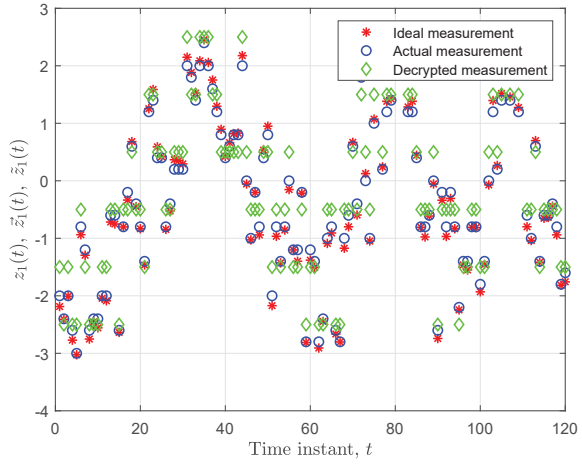

Fig. 3: Ideal, actual, and decrypted measurements of the first sensor.

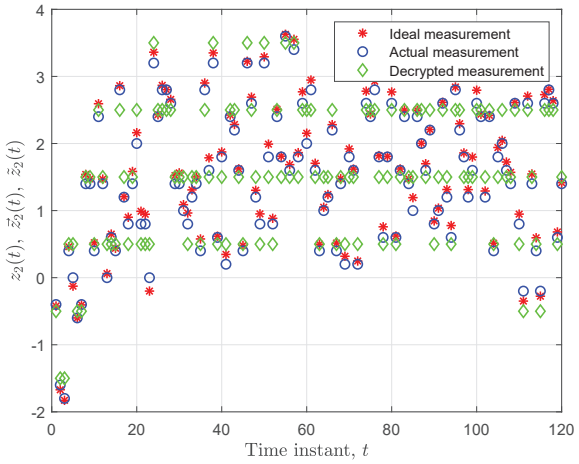

Fig. 4: Ideal, actual, and decrypted measurements of the second sensor.

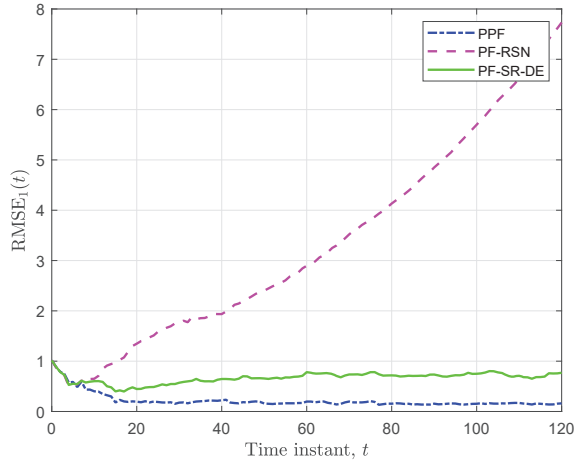

Fig. 5: Behaviors of $\mathrm{RMSE}_1(t)$ under different algorithms.

In what follows, three filtering algorithms are compared to demonstrate the superiority of the proposed scheme. These algorithms include: 1) the proposed particle filtering algorithm (abbreviated as PPF); 2) the particle filtering algorithm neglecting the presence of randomly switching nonlinearities (abbreviated as PF-RSN); and 3) the particle filtering algorithm neglecting the impact of sensor resolutions and decryption errors (abbreviated as PF-SR-DE). The behaviors of the root mean-square error (RMSE) over 50 Monte Carlo simulations under different filtering algorithms are shown in Figs. 5 and 6. Obviously, the proposed algorithm exhibits superior filtering performance when compared with other two algorithms. This is not unexpected since the influence of the considered phenomena is specially compensated for in the design of particle filter. The above results demonstrate the effectiveness of the proposed particle filtering scheme.

This article has been accepted for publication in a future proceedings of this conference, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/ICAC65379.2025.11196717, 2025 30th International Conference on Automation and Computing (ICAC)

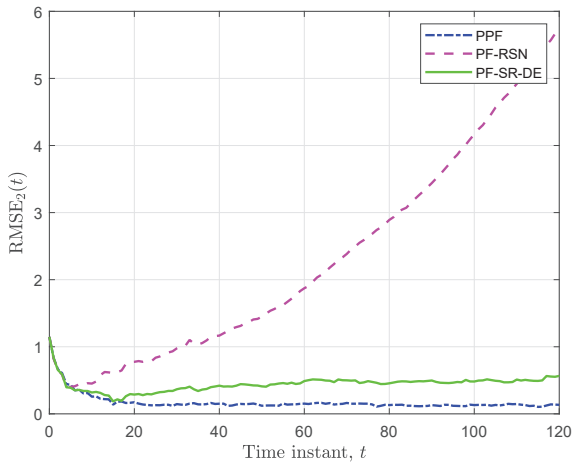

Fig. 6: Behaviors of $\mathrm{RMSE}_2(t)$ under different algorithms.

V. Conclusions

In this paper, the secure state estimation problem has been studied for a class of stochastic systems subject to randomly switching nonlinearities, sensor resolutions and non-Gaussian noises. In order to enhance the transmission security of measurements, an encryption-decryption-based particle filtering algorithm has been put forward, where the particles are drawn from a mixture distribution and the importance weights are calculated by taking into account the joint influence of sensor resolutions and decryption errors. Finally, simulation results have been provided to showcase the effectiveness and superiority of the developed particle filtering algorithm. One of the future topics would be extending the obtained results by exploring other advanced encryption-decryption techniques and analyzing the effect of decryption errors on the estimation performance [22]–[24].

References

[1] R. Caballero-Águila, J. Hu and J. Linares-Pérez, Filtering and smoothing estimation algorithms from uncertain nonlinear observations with time-correlated additive noise and random deception attacks, *International Journal of Systems Science*, vol. 55, no. 10, pp. 2023–2035, 2024.

[2] R. Khodayi-mehr, Y. Kantaros and M. M. Zavlanos, Distributed state estimation using intermittently connected robot networks, *IEEE Transactions on Robotics*, vol. 35, no. 3, pp. 709–724, 2019.

[3] B. Qu, D. Peng, Y. Shen, L. Zou and B. Shen, A survey on recent advances on dynamic state estimation for power systems, *International Journal of Systems Science*, vol. 55, no. 16, pp. 3305–3321, 2024.

[4] W. Li, Y. Jia and J. Du, State estimation for stochastic complex networks with switching topology, *IEEE Transactions on Automatic Control*, vol. 62, no. 12, pp. 6377–6384, 2017.

[5] W. Song, Z. Wang, Z. Li, J. Wang and Q.-L. Han, Nonlinear filtering with sample-based approximation under constrained communication: Progress, insights and trends, *IEEE/CAA Journal of Automatica Sinica*, vol. 11, no. 7, pp. 1539–1556, 2024.

[6] D. Dai, J. Li, Y. Song and F. Yang, Event-based recursive filtering for nonlinear bias-corrupted systems with amplify-and-forward relays, *Systems Science & Control Engineering*, vol. 12, no. 1, art. no. 2332419, 2024.

[7] Y. Liu, B. Shen and H. Shu, Finite-time resilient H_∞ state estimation for discrete-time delayed neural networks under dynamic event-triggered mechanism, *Neural Networks*, vol. 121, pp. 356–365, 2020.

[8] J. Hu, J. Li, H. Yan and H. Liu, Optimized distributed filtering for saturated systems with amplify-and-forward relays over sensor networks: A dynamic event-triggered approach, *IEEE Transactions on Neural Networks and Learning Systems*, vol. 35, no. 12, pp. 17742–17753, 2024.

[9] M. S. Arulampalam, S. Maskell, N. Gordon and T. Clapp, A tutorial on particle filters for online nonlinear/non-Gaussian Bayesian tracking, *IEEE Transactions on Signal Processing*, vol. 50, no. 2, pp. 174–188, 2002.

[10] P. M. Djurić, M. Vemula and M. F. Bugallo, Target tracking by particle filtering in binary sensor networks, *IEEE Transactions on Signal Processing*, vol. 56, no. 6, pp. 2229–2238, 2008.

[11] W. Song, Z. Wang, Z. Li and Q.-L. Han, Particle-filter-based state estimation for delayed artificial neural networks: When probabilistic saturation constraints meet redundant channels, *IEEE Transactions on Neural Networks and Learning Systems*, vol. 35, no. 3, pp. 4354–4362, 2024.

[12] Y. Luo, Z. Wang, Y. Chen and X. Yi, H_∞ state estimation for coupled stochastic complex networks with periodical communication protocol and intermittent nonlinearity switching, *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1414–1425, 2021.

[13] P. Zhao, D. Ding, H. Dong, H. Liu and X. Yi, Secure distributed state estimation for microgrids with eavesdroppers based on variable decomposition, *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 71, no. 7, pp. 3307–3316, Jul. 2024.

[14] X. Yan, G. Zhou, D. E. Quevedo, C. Murguia, B. Chen and H. Huang, Privacy-preserving state estimation in the presence of eavesdroppers: A survey, *IEEE Transactions on Automation Science and Engineering*, vol. 22, pp. 6190–6207, 2025.

[15] K. Zhu, Z. Wang, D. Ding, H. Dong and G. Wei, Encryption-decryption-based set-membership filtering for two-dimensional systems: On security and boundedness, *Automatica*, vol. 173, art. no. 112091, 2025.

[16] X. He and F. Jia, Active fault-tolerant control for nonlinear systems with nonlogarithmic sensor resolution, *IEEE Transactions on Instrumentation and Measurement*, vol. 73, art. no. 3503711, 2024.

[17] J. Zhang, X. He and D. Zhou, Filtering for stochastic uncertain systems with non-logarithmic sensor resolution, *Automatica*, vol. 89, pp. 194–200, 2018.

[18] Y. Shen, Z. Wang, H. Dong, H. Liu and X. Liu, Joint state and unknown input estimation for a class of artificial neural networks with sensor resolution: An encoding-decoding mechanism, *IEEE Transactions on Neural Networks and Learning Systems*, vol. 36, no. 2, pp. 3671–3681, 2025.

[19] Z. Zhao, Z. Wang, L. Zou, Y. Chen and W. Sheng, Zonotopic non-fragile set-membership fusion estimation for nonlinear systems under sensor resolution effects: Boundedness and monotonicity, *Information Fusion*, vol. 105, art. no. 102232, 2024.

[20] A. Das, Block-wise computation of cyclic redundancy code using factored Toeplitz matricesin lieu of look-up table, *IEEE Transactions on Computers*, vol. 72, no. 4, pp. 1110–1121, 2023.

[21] A. H. Jazwinski, *Stochastic processes and filtering theory*, New York, NY, USA: Academic Press, 1970.

[22] P. Zhao, Y. Chen, D. Ding and H. Liu, Privacy-preserving distributed state estimation for microgrids based on encrypted measurements under bit-rate constraints, *International Journal of Systems Science*, vol. 56, no. 10, pp. 2481–2498, 2025.

[23] W. Chen, Z. Wang, Q. Ge, H. Dong and G.-P. Liu, Quantized distributed economic dispatch for microgrids: Paillier encryption-decryption scheme, *IEEE Transactions on Industrial Informatics*, vol. 20, no. 4, pp. 6552–6562, 2024.

[24] L. Sun, D. Ding, H. Dong and X. Yi, Distributed economic dispatch of microgrids based on ADMM algorithms with encryption-decryption rules, *IEEE Transactions on Automation Science and Engineering*, vol. 22, pp. 8427–8438, 2025.