This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TSG.2023.3271949, IEEE Transactions on Smart Grid

Secure Particle Filtering With Paillier Encryption-Decryption Scheme: Application to Multi-machine Power Grids

Bogang Qu, Zidong Wang, Bo Shen, Hongli Dong and Xin Zhang

***Abstract*—This paper is concerned with the encryption-decryption-based state estimation problem for a class of multi-machine power grids with non-Gaussian noises. For the purposes of security enhancement and data privacy protection, the Paillier encryption-decryption scheme is adopted to map the measurement data into the ciphertext space before being transmitted through the communication network. The aim of this paper is to develop a novel secure particle filter algorithm to cope with the nonlinearity/non-Gaussianity from the system plant and the decrypted signals after the measurement transmission. In particular, a modified likelihood function is proposed to obtain the importance weights where the encryption-decryption process of the measurement data is taken into full consideration. The developed algorithm is applied to multi-machine power grids, and it is demonstrated via simulation studies (on three test scenarios of the IEEE 39-bus power system) that our proposed secure state estimation scheme possesses the desired performance index in terms of security and accuracy.**

***Index Terms*—Particle filter, encryption-decryption scheme, nonlinear/non-Gaussian systems, secure state estimation, power grids.**

Abbreviations and Notations

PMU	Phasor measurement unit
PF	Particle filtering
SG	Synchronous generator
PDF	Probability density function
SIR	Sampling importance resampling
EKF	Extend Kalman filter
UKF	Unscented Kalman filter
ACT	Average Computing Time
$\mathbb{R}^p$	The p-dimensional Euclidean space
p_x	The PDF of a random variable x
$\mathbb{Z}$	The set of integers
$\mathbb{Z}^+$	The set of non-negative integers
$\mathbb{Z}_n$	The set of prime numbers less than n
$\mathbb{Z}_n^*$	The set of numbers less than and co-prime to n
$\gcd(p,q)$	The greatest common divisor of p and q
$\mathrm{lcm}(p,q)$	The least common multiple of p and q
$x \sim \mathcal{N}(\mu,\sigma)$	The random variable x following Gaussian distribution with mean μ and variance σ
I	The identity matrix with compatible dimensions

This work was supported in part by the National Natural Science Foundation of China under Grants 61933007, U21A2019 and 62273088, the Program of Shanghai Academic/Technology Research Leader of China under Grant 20XD1420100, the Hainan Province Science and Technology Special Fund of China under Grant ZDYF2022SHFZ105, the UK Research and Innovation Future Leaders Fellowship under Grants MR/W011360/1, the Engineering and Physical Sciences Research Council (EPSRC) of the UK, the Royal Society of the UK, and the Alexander von Humboldt Foundation of Germany. *(Corresponding author: Bo Shen.)*

B. Qu is with the College of Automation Engineering, Shanghai University of Electric Power, Shanghai, 200090, China. (e-mail: bogangqu@163.com).

Z. Wang is with the Department of Computer Science, Brunel University London, Uxbridge, Middlesex, UB8 3PH, United Kingdom (e-mail: Zidong.Wang@brunel.ac.uk).

B. Shen is with the College of Information Science and Technology, Donghua University, Shanghai 200051, China, and also with the Engineering Research Center of Digitalized Textile and Fashion Technology, Ministry of Education, Shanghai 201620, China (e-mail: bo.shen@dhu.edu.cn).

H. Dong is with the Artificial Intelligence Energy Research Institute, Northeast Petroleum University, Daqing 163318, China, also with the Heilongjiang Provincial Key Laboratory of Networking and Intelligent Control, Northeast Petroleum University, Daqing 163318, China, and also with the Sanya Offshore Oil & Gas Research Institute, Northeast Petroleum University, Sanya 572024, China (e-mail: shiningdhl@vip.126.com).

X. Zhang is with the Department of Automatic Control and Systems Engineering, University of Sheffield, Western Bank, Sheffield, S10 2TN, United Kingdom (e-mail: xin.zhang1@sheffield.ac.uk).

I. Introduction

Owing to the rapid progress in developing communication and sensing technologies, the situational awareness issues have recently aroused a lot of interest from both academia and industry with respect to various practical systems, see [1] for electric vehicle systems, [2]–[5] for networked control systems, and [6], [7] for power systems. For instance, the situational awareness problems have been thoroughly investigated in [6] for monitoring photovoltaic power plants and in [7] for detecting load/line/generation events, where the information about the inner states of the power grids have proven to be vitally important in 1) enhancing the situational awareness; 2) benefiting real-time control; and 3) facilitating security assessment of the entire system. In fact, the state estimation techniques have drawn much research attention in revealing the inner dynamics/behaviors of the power grids [8]–[14].

Over the past few decades, the general state estimation issue has been a hot research topic in the fields of signal processing [15]–[18], control engineering [19]–[21] and fault diagnosis [22]–[25]. With respect to power grids, the state estimation techniques have also received an ever-growing research interest, see e.g. [6], [7], [9], [12]–[14], [26], [27]. For example, in [6], the situational awareness of the active distribution systems has been studied with the aid of weighted-least-square-based state estimation algorithm. In [12], a novel

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TSG.2023.3271949, IEEE Transactions on Smart Grid

distributed state estimation scheme has been proposed for the large-scale power networks by resorting to the unscented information filtering technique. It should be noted that most existing state estimation results for power grids have been obtained under the assumption that the noises follow Gaussian distributions. Such an assumption, however, might be violated with the dynamically changeable operating conditions of power grids.

It has been well recognized that the process/measurement noises of practical power grids do not necessarily follow the Gaussian distributions. For example, it has been confirmed that the synchronized voltage measurement (collected from the Indian synchrophasor network [28]) and the phasor measurement unit (PMU) measurement (collected by the Pacific Northwest National Laboratory [29]) actually obey *non-Gaussian* (e.g. logistic or log-normal) distributions. Also, it has been revealed in [11] that the stochastic power flows (caused by the renewable energy generations) follow non-Gaussian distributions as well. All these facts have motivated us to research into the state estimation problems for power grids with non-Gaussian process/measurement noises, where the particle filtering (PF) algorithm appears to be especially suitable due to its distinctive advantages in tackling nonlinearities and non-Gaussian noises [30].

Modern power grids, which rely heavily on open communication networks, are known to be vulnerable to various security threats [3], [26], [31], [32] and, accordingly, a rich body of literature has appeared on the security defense issues for power grids from the perspectives of physical security, information security and communication security [32]. The main idea of the physical defense strategy is to optimize the measuring topology by adjusting the placements of the PMUs and other measuring facilities [33]. For enhancing information security, a common approach is to develop online/offline detection criteria by using the historical measurement data [34]. As for the communication security, a widely used method is to protect the communication channel with the aid of encryption techniques [35].

In the *secure* state estimation of power systems, one of the common used approaches is to detect and eliminate/correct the possible cyber-attacks contained in the measurement data to mitigate the negative influences on the estimation performance, see e.g. [3], [8], [10]. For example, in [10], a distributed state estimation scheme has been developed for the wide-area smart grids where an online anomaly processing mechanism is designed to detect and eliminate the adverse effects caused by the cyber-attack-contaminated measurements. Different from the detection-correction framework, another widely used way is to enhance the robustness against cyber-attacks by embedding special performance indices or penalty functions into the state estimation algorithms, see e.g. [8], [36], [37]. For instance, in order to mitigate the negative influences cause by cyber-attacks, a novel robust unscented Kalman filter has been proposed in [37] with the aid of minimum error entropy criterion.

It is worth pointing out that in actual power systems, the types (e.g. false data injection attacks, replay attacks and/or bias injection attacks) and the features (e.g. occasionality, probability and/or intermittency) of the cyber-attacks are various, and it is difficult and even impossible to detect them correctly all the time. As a result, the smearing impacts caused by the undetected cyber-attacks [38] might seriously affect the performance of the secure state estimation algorithms developed within the threat-detection framework. On the other hand, it is difficult to extend the existing robust state estimation algorithms to cover the cyber-attacks with various types/features since the cyber-attacks are "coarsely" tread as complex disturbances (e.g. non-Gaussian disturbance) in these algorithms. To this end, a seemingly natural idea is to develop "active" schemes to prevent the cyber-attacks from occurring, thereby equipping the state estimation algorithm with desired security.

As a popular active security countermeasure, the cryptography-based technique has been widely applied in networked systems to ensure the security and protect privacy of data transmissions [10], [35], [39]. Accordingly, the encryption-decryption-based state estimation problem has attracted a rapidly growing research interest, see e.g. [40], [41]. For instance, in order to prevent eavesdropping in the remote state estimation, a linear encryption scheme has been adopted in [40] to promote the security of the transmitted data. In [41], a secure state estimation algorithm has been designed with the aid of multiplicative (and additive) homomorphic encryption techniques. Nevertheless, when it comes to the power grids, the secure state estimation problem under the cryptography framework has not yet received sufficient attention, despite its conspicuous engineering significance.

In view of the forgoing discussions, we conclude that there is a lack of secure state estimation algorithms for power grids with cryptographic measurement, and developing such kind of algorithms is highly desired given the increasing demand of secure monitoring in power grids. It is, therefore, the main purpose of this paper to shorten the gap by examining the secure state estimation problem with the following salient features.

- A particle-filter-based state estimation scheme is developed to cope with the strong nonlinearities and non-Gaussian noises of the power grids, and such a scheme is implemented in a decentralized manner with the aid of model decoupling technique of power grids, therefore facilitating online applications.
- The Paillier encryption-decryption mechanism is adopted to cater for the ever-increasing demand for preservation of data privacy of the power grids, thereby ensuring the security of the data transmission in the communication network.
- A new likelihood function is first put forward based on the decrypted measurement data, and a novel secure PF is then designed where the parameters of the encryption-decryption process are exploited in the calculation of the importance weights.

The rest of this paper is outlined as follows. Section II formulates the state estimation issue for a class of multi-machine power grids with non-Gaussian noises under the framework of the Paillier encryption-decryption mechanism. The basic steps

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TSG.2023.3271949, IEEE Transactions on Smart Grid

of the PF algorithm are reviewed in Section III. Section IV investigates the secure particle filter design problem based on the modified likelihood function. A practical application to the state estimation problem is provided in Section V for multi-machine power grids with cryptographic measurement data. Finally, some conclusion remarks are drawn in Section VI.

II. Problem Formulation

A. Power Grid Model

Consider a multi-machine power grid which contains L synchronous generators (SGs), where the discrete-time model of the l-th SG is of the following form [14]:

$$\delta_{l,k+1} = \delta_{l,k} + (\omega_{l,k} - \omega_s)\Delta t, \tag{1a}$$

$$\omega_{l,k+1} = \omega_{l,k} + \frac{\omega_s}{2H_l}\big[T_{m,l} - P_{l,k} - D_l(\omega_{l,k} - \omega_s)\big]\Delta t, \tag{1b}$$

$$E'_{q,l,k+1} = E'_{q,l,k} + \frac{1}{T'_{d0,l}}\big[-E'_{q,l,k} - (X_{d,l} - X'_{d,l})I_{d,l,k} + E_{fd,l,k}\big]\Delta t, \tag{1c}$$

$$E'_{d,l,k+1} = E'_{d,l,k} + \frac{1}{T'_{q0,l}}\big[-E'_{d,l,k} + (X_{q,l} - X'_{q,l})I_{q,l,k}\big]\Delta t \tag{1d}$$

with

$$I_{d,l,k} = \frac{1}{X'_{dl}}(E'_{q,l,k} - V_{q,l,k}),\ I_{q,l,k} = \frac{1}{X'_{ql}}(-E'_{d,l,k} + V_{d,l,k}),$$
$$V_{d,l,k} = V_{l,k}\sin(\delta_{l,k} - \theta_{l,k}),\ V_{q,l,k} = V_{l,k}\cos(\delta_{l,k} - \theta_{l,k}) \tag{2}$$

where the details of the parameters in (1) and (2) are given in Table I.

TABLE I: Parameters of the SG and its measurement

Parameter	Meaning
l	Index of the SG ($l = 1, 2, \ldots, L$)
Δt	Discretization period
k	Time instant
δ	Rotor angle of the SG
ω	Rotor speed of the SG
w_s	Nominal synchronous speed
$\frac{\omega_s}{2H_l}$	Inertia time constant of the SG
P	SG's terminal active power
T_m	Mechanical torque input of the SG
D	Damping factor of the SG
E_{fd}	Excitation field voltage of the SG
E'_d, E'_q	dq-axes transient voltages of the SG
X_d, X_q	dq-axes synchronous reactances of the SG
X'_d, X'_q	dq-axes transient synchronous reactances of the SG
T'_{d0}, T'_{q0}	dq-axes transient open-circuit time instants of the SG
I_d, I_q	dq-axes currents of the SG
V_d, V_q	dq-axes voltages of the SG
V	Terminal bus voltage magnitude of the SG
θ	Terminal bus phase angle of the SG
f	SG's terminal frequency
f_0	SG's nominal frequency
P	SG's terminal active power injection
Q	SG's terminal reactive power injection

Based on (1)-(2), the discretized state-space model of the l-th SG can be obtained as

$$x_{l,k+1} = f_l(x_{l,k}, u_{l,k}) + w_{l,k} \tag{3}$$

where the state vector and the known input vector are, respectively, defined by (for brevity, the time instant $k\Delta t$ is simply denoted by k)

$$x_{l,k} \triangleq \begin{bmatrix}\delta_{l,k} & \omega_{l,k} & E'_{q,l,k} & E'_{d,l,k}\end{bmatrix}^T \in \mathbb{R}^{n_x}$$

and

$$u_{l,k} \triangleq \begin{bmatrix}V_{l,k} & \theta_{l,k} & T_{m,l,k} & E_{fd,l,k}\end{bmatrix}^T \in \mathbb{R}^{n_u},$$

the nonlinear function $f_l(\cdot)$ is determined by (1)-(2), and $w_{l,k}$ represents the process noise satisfying the probability density function (PDF) $p_{w_{l,k}}$. Note that the mechanical torque input $T_{m,l,k}$ and the excitation field voltage $E_{fd,l,k}$ of the SG can be measured, respectively, in real-world application, and they are treated as known input in this paper.

B. PMU Measurement Model

For the purpose of implementing the state estimation algorithm in a decentralized manner, the model decoupling technique proposed in [14] is adopted in this paper to decouple each SG from the rest of the power grid. To be specific, by the model decoupling technique, the voltage phasor of the terminal bus is treated as model input and the current phasor of the terminal bus is treated as measured output. Note that the terminal active and reactive power injections (which can be obtained by using the voltage and current phasors) can better reflect the dynamics of the generators [14]. In this sense, the terminal frequency as well as the terminal active and reactive power injections of the l-th generator are selected as the PMU measurements, i.e.

$$f_{l,k} = f_0(w_{l,k} - w_s + 1), \tag{4a}$$

$$P_{l,k} = V_{d,l,k}I_{d,l,k} + V_{q,l,k}I_{q,l,k}, \tag{4b}$$

$$Q_{l,k} = -V_{d,l,k}I_{q,l,k} + V_{q,l,k}I_{d,l,k}, \tag{4c}$$

where the details of the parameters in (4) are shown in Table I, and the definitions of V_d, V_q, I_d and I_q are all given in (2).

A compact PMU measurement model of the l-th SG can be arranged as

$$\bar{z}_{l,k} = h_l(x_{l,k}, u_{l,k}) + v_{l,k} \tag{5}$$

where the measurement vector is denoted by

$$\bar{z}_{l,k} \triangleq \begin{bmatrix}f_{l,k} & P_{l,k} & Q_{l,k}\end{bmatrix}^T \in \mathbb{R}^{n_z},$$

the nonlinear function $h_i(\cdot)$ is determined by (4), and $v_{l,k}$ is the measurement noise obeying the PDF $p_{v_{l,k}}$.

C. Transmission Model

In order to enhance the transmission security of the measurement data over the communication network, the Paillier encryption-decryption scheme is adopted in this paper, which consists of four steps (i.e., quantization-encoding, encryption, decryption and decoding) given as follows.

Quantization-encoding: Note that, in practical systems, the measurement signal has to be quantized and then encoded before it is transmitted through communication networks. To be specific, the quantization procedure for the s-th element of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TSG.2023.3271949, IEEE Transactions on Smart Grid

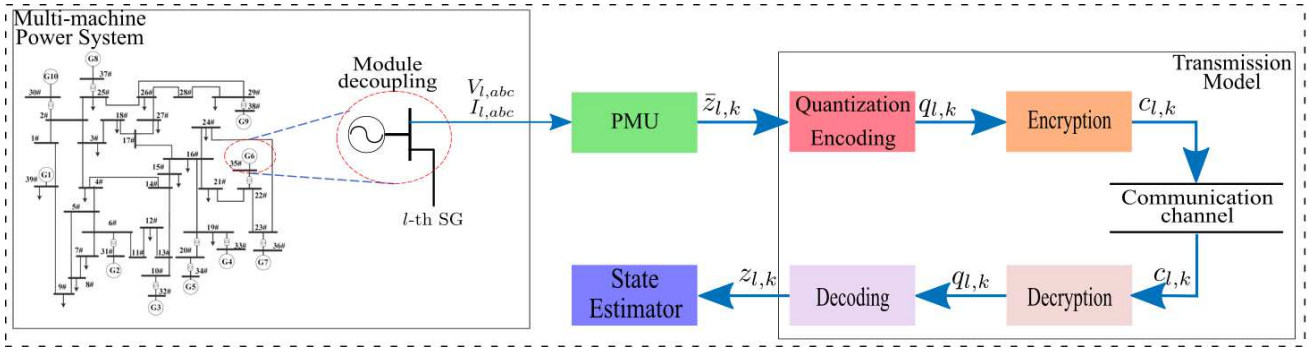


Fig. 1: Diagram of the secure state estimation for multi-machine power grids with encryption-decryption scheme.

the measurement vector, denoted as $\bar{z}_{l,k}^{[s]}$ $(s = 1, 2, \ldots, n_z)$, can be expressed as follows:

$$\bar{q}_{l,k}^{[s]} = Q(\bar{z}_{l,k}^{[s]}) = ar \quad \frac{(2a-1)r}{2} \leq \bar{z}_{l,k}^{[s]} < \frac{(2a+1)r}{2} \tag{6}$$

where $\bar{q}_{l,k}^{[s]}$ is the quantized output; $Q(\cdot)$ represents the quantization function; a is an integer which satisfies $a \in \{-\mathcal{A}, -\mathcal{A}+1, \cdots, 0, \cdots, \mathcal{A}-1, \mathcal{A}\}$ with $2\mathcal{A}+1$ being the number of quantization levels and $\mathcal{A}$ being positive integer; and r represents the length between two neighboring quantization levels.

After quantization, the coding process is adopted to convert the quantized value into codeword. In this paper, we assume that the corresponding codeword $q_{l,k}^{[s]}$ of the quantized value $\bar{q}_{l,k}^{[s]}$ $(s = 1, 2, \ldots, n_z)$ can be found in the finite non-negative integer set $\mathcal{M}$ (namely, the codeword space).

Encryption: After obtaining the codeword $q_{l,k}^{[s]}$ $(s = 1, 2, \ldots, n_z)$, we encrypt the plaintext by resorting to the Paillier encryption-decryption technique. The basic steps of the Paillier encryption are outlined as follows [41]:

- Generate public key $\mathcal{PK}$ and private key $\mathcal{SK}$.
  1) Select two large prime numbers p and q $(p \neq q)$ such that $\gcd\big(pq, (p-1)(q-1)\big) = 1$.
  2) Calculate $n = pq$ and $\lambda = \mathrm{lcm}(p-1, q-1)$.
  3) Select a positive integer g such that $g \in \mathbb{Z}_{n^2}^*$.
  4) Define a function $L(x)$ as $L(x) \triangleq \frac{x-1}{n}$.
  5) Calculate $\mu = \big(L(g^\lambda \bmod n^2)\big)^{-1} \bmod n$.
  6) Generate the public key $\mathcal{PK} = (n, g)$ and the private key $\mathcal{SK} = (\lambda, \mu)$.
- *Encrypt the plaintext*:
  1) Select a positive integer r such that $r \in \mathbb{Z}_n^*$.
  2) Based on the plaintext $q_{l,k}^{[s]}$ $(s = 1, 2, \ldots, n_z)$, calculate the ciphertext $c_{l,k}^{[s]}$ via

$$\begin{aligned} c_{l,k}^{[s]} &= \mathrm{Enc}(\mathcal{PK}, r) \\ &= g^{q_{l,k}^{[s]}} r^n \bmod n^2 \end{aligned} \tag{7}$$

  where $\mathrm{Enc}(\cdot)$ represents the Paillier encryption function.

Decryption: After receiving the ciphertext $c_{l,k}^{[s]}$ $(s = 1, 2, \ldots, n_z)$, the decryption procedure is performed to calculate the plaintext $q_{l,k}^{[s]}$ via

$$\begin{aligned} q_{l,k}^{[s]} &= \mathrm{Dec}(\mathcal{SK}, c_{l,k}^{[s]}) \\ &= L(c^\lambda \bmod n^2)\mu \bmod n \end{aligned} \tag{8}$$

where $\mathrm{Dec}(\cdot)$ is the Paillier decryption function.

Decoding: Denoting the output of the decoding process as $z_{l,k}^{[s]}$ $(s = 1, 2, \ldots, n_z)$, the value of $z_{l,k}^{[s]}$ can be recovered from the plaintext $q_{l,k}^{[s]}$ by resorting to the codeword space $\mathcal{M}$.

Before proceeding further, the following two assumptions are made.

Assumption 1: The initial state $x_{l,0}$ follows the prior distribution with $p_{x_{l,0}}$, i.e. $x_{l,0} \sim p_{x_{l,0}}$.

Assumption 2: The process noise $w_{l,k}$, the measurement noise $v_{l,k}$ and the initial state $x_{l,0}$ are mutually independent.

Remark 1: It is worth noting that most of the state estimation algorithms developed for power grids rely on a fundamental assumption that the initial states and the process/measurement noises follow *Gaussian* distributions with known PDFs (see e.g. [8], [10], [12] and the references therein). Compared with the existing results concerning the state estimation problem of power systems, the conservatism of this paper can be reduced to some extent since the PDFs of the initial state and the process/measurement noises are assumed to be Gaussian and/or non-Gaussian. In order to cater for engineering practice, recently, a novel adaptive state estimation algorithm has been designed in [42] for power system to tackle the unknown and time-varying PMU error statistics. However, such an algorithm is still essentially performed with the known noise statistics since the PDFs of the noises have been identified already by analyzing the historical data contained in a sliding window.

D. Problem Statement

The aim of this paper is to design a secure state estimation algorithm such that:

1) the nonlinearities and the non-Gaussian noises of the systems can be effectively handled;
2) the security of the transmitted measurement signal can be guaranteed by resorting to the Paillier encryption-decryption technique; and
3) the negative impacts from the decryption error can be mitigated by improving the particle filtering algorithm.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TSG.2023.3271949, IEEE Transactions on Smart Grid

III. Review Of Particle Filtering Method

As is well known, the nonlinearity and the non-Gaussian noise of the systems may seriously impair the estimation performances of the weighted-least-square-based filtering method and the conventional Kalman filtering method. As such, the PF technique is adopted in this paper to tackle the nonlinearity/non-Gaussianity. In this section, the fundamental steps of the sampling-importance-resampling (SIR) based PF are briefly reviewed.

Denote the sets of all available inputs and measurements up to time instant k, respectively, as

$$U_{l,k} \triangleq \{u_{l,1}, u_{l,2}, \ldots, u_{l,k}\}$$

and

$$Z_{l,k} \triangleq \{z_{l,1}, z_{l,2}, \ldots, z_{l,k}\}.$$

Then, the posterior PDF $p(x_{l,k}|U_{l,k}, Z_{l,k})$ of the state $x_{l,k}$ can be inferred recursively by the Bayes rule as follows:

$$\begin{aligned} &p(x_{l,k}|U_{l,k}, Z_{l,k}) \\ =&\frac{p(z_{l,k}|x_{l,k}, u_{l,k})p(x_{l,k}|U_{l,k-1}, Z_{l,k-1})}{\int p(z_{l,k}|x_{l,k}, u_{l,k})p(x_{l,k}|U_{l,k-1}, Z_{l,k-1})dx_{l,k}} \end{aligned} \tag{9}$$

where

$$\begin{aligned} &p(x_{l,k}|U_{l,k-1}, Z_{l,k-1}) \\ =&\int p(x_{l,k}|x_{l,k-1}, u_{l,k-1})p(x_{l,k-1}|U_{l,k-1}, Z_{l,k-1})dx_{l,k-1} \end{aligned}$$

is the predictive PDF of the state $x_{l,k}$.

Note that, in practice, it is intractable to obtain the close-form solution of the posterior PDF under the Bayesian framework. In this case, an alternative approach, namely, the PF technique, has been adopted to approximate the posterior PDF $p(x_{l,k}|U_{l,k}, Z_{l,k})$ with a set of weighted particles, i.e.,

$$p(x_{l,k}|U_{l,k}, Z_{l,k}) \approx \sum_{m=1}^{M} \omega_{l,k}^m \delta(x_{l,k} - x_{l,k}^m) \tag{10}$$

where M is the number of particles; $\delta(\cdot)$ denotes the Dirac delta function; $\{x_{l,k}^m\}_{m=1}^M$ represents a set of particles drawn from a proposal distribution $q(x_{l,k}|x_{l,k-1}^m, u_{l,k-1}, z_{l,k})$; and $\{\omega_{l,k}^m\}_{m=1}^M$ is a set of importance weights for the corresponding particles. In this paper, we follow the procedure of the SIR-based PF algorithm and select the state transition PDF $p(x_{l,k}|x_{l,k-1}, u_{l,k-1})$ as the proposal distribution [43].

The SIR-based PF algorithm is summarized as follows.

1) Initialization. The initial particles $\{x_{l,k}^m\}_{m=1}^M$ are generated from the known prior PDF $p_{x_{l,0}}$ where the associated weight for each initial particle is set as $1/M$.

2) Propagation. In this step, the posterior particle set $\{x_{l,k-1}^m\}_{m=1}^M$ at time instant $k-1$ is propagated one-step ahead via (1) to obtain the prior particle set $\{\bar{x}_{l,k}^m\}_{m=1}^M$, i.e.,

$$\bar{x}_{l,k}^m = f(x_{l,k-1}^m + u_{l,k-1}) + w_{l,k-1}^m. \tag{11}$$

3) Computation of the Importance Weights. After propagation, the associated importance weights for the prior particle set $\{\bar{x}_{l,k}^m\}_{m=1}^M$ is determined by

$$\bar{\omega}_{l,k}^m = \omega_{l,k-1}^m \frac{p(z_{l,k}|\bar{x}_{l,k}^m, u_{l,k})p(x_{l,k}|x_{l,k-1}^m, u_{l,k-1})}{q(x_{l,k}|x_{l,k-1}^m, u_{l,k-1}, z_{l,k})}. \tag{12}$$

Note that, in the SIR-based PF algorithm, the state transition PDF is usually selected as the proposal distribution, and we can rewrite (12) as

$$\bar{\omega}_{l,k}^m = \omega_{l,k-1}^m p(z_{l,k}|\bar{x}_{l,k}^m, u_{l,k}). \tag{13}$$

After normalization, we have

$$\omega_{l,k}^m = \frac{\bar{\omega}_{l,k}^m}{\sum_{m=1}^M \bar{\omega}_{l,k}^m}. \tag{14}$$

4) State Estimation. Based on the prior particle set $\{\bar{x}_{l,k}^m\}_{m=1}^M$ and the associated importance weights set $\{\omega_{l,k}^m\}_{m=1}^M$, the estimate of $x_{l,k}$ can be expressed as

$$\hat{x}_{l,k} = \sum_{i=1}^{M} \omega_{l,k}^j \bar{x}_{l,k}^j. \tag{15}$$

5) Particle Resample. As a common phenomenon, the particle degeneracy may occur after some iterations, which means that only a few particles have significant weights. For the purpose of mitigating the adverse effects on the estimation performance caused by the particle degeneration, in this paper, we follow the basic steps of the SIR-based PF algorithm and perform the resampling strategy at each iteration. To be specific, a new set of particles with equal weights are generated from $\sum_{m=1}^M \omega_{l,k}^m \delta(x_{l,k} - x_{l,k}^m)$. It should be noted that, even though we design the secure state estimation algorithm in the framework of the SIR-based PF, extensions to other resampling strategies (e.g. the adaptive resampling strategy) are fairly straightforward.

IV. Design of Secure Particle Filter

In general, the state estimation can be achieved directly with the aid of SIR-based PF algorithm. However, due to the adoption of the Paillier encryption-decryption scheme, the actual measurement data we receive would be totally different from the unencrypted one (i.e. $\bar{z}_{l,k}$ in (5)). In other words, the adverse effects caused by the encryption-decryption mechanisms have to be considered in the calculation of the likelihood function $p(z_{l,k}|\bar{x}_{l,k}^m, u_{l,k})$ evaluated at $\bar{x}_{l,k}^m$. The diagram of the secure state estimation for multi-machine power grids with encryption-decryption technique is shown in Fig. 1.

In this section, we aim to develop a secure state estimation algorithm for a class of multi-machine power grids with non-Gaussian noises by resorting to the Paillier encryption-decryption technique, where a modified likelihood function is constructed to compensate the effect of the decryption error. It should be pointed out that the expressions of the likelihood function $p(z_{l,k}|\bar{x}_{l,k}^m, u_{l,k})$ (evaluated at $\bar{x}_{l,k}^m$) are dependent on the properties of the measurement noises and, accordingly, we consider the following two cases.

Case 1: The measurement noise follows Gaussian distribution, i.e. $v_{l,k} \sim \mathcal{N}(\mu_{l,k}, \sigma_{l,k}^2)$.

For the s-th $(s = 1, 2, \ldots, n_z)$ element of the decoder output $z_{l,k}$, the likelihood function can be represented as

$$\begin{aligned} p(z_{l,k}^{[s]}|x_{l,k}, u_{l,k}) =&p_i\left(z_{l,k}^{[s]} - \frac{r}{2} \le z_{l,k}^{[s]} < z_{l,k}^{[s]} + \frac{r}{2}\right) \\ =&p\left(\underline{\varepsilon}_{l,k}^{[s]} \le v_{l,k}^{[s]} < \bar{\varepsilon}_{l,k}^{[s]}\right) \end{aligned}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TSG.2023.3271949, IEEE Transactions on Smart Grid

$$=\Phi\left(\frac{\bar{\varepsilon}_{l,k}^{[s]}-\mu_{l,k}^{[s]}}{\sigma_{l,k}^{[s]}}\right)-\Phi\left(\frac{\underline{\varepsilon}_{l,k}^{[s]}-\mu_{l,k}^{[s]}}{\sigma_{l,k}^{[s]}}\right) \tag{16}$$

where

$$\underline{\varepsilon}_{l,k}^{[s]} \triangleq z_{l,k}^{[s]}-h(x_{l,k},u_{l,k})-\frac{r}{2},$$
$$\bar{\varepsilon}_{l,k}^{[s]} \triangleq z_{l,k}^{[s]}-h(x_{l,k},u_{l,k})+\frac{r}{2},$$

and $\Phi(\cdot)$ denotes the cumulative distribution function of the standard normal distribution. Then, it follows from (16) that the likelihood function evaluated at $\bar{x}_{l,k}^m$ is described as

$$p(z_{l,k}|\bar{x}_{l,k}^m,u_{l,k})=\prod_{s=1}^{n_z}p(z_{l,k}^{[s]}|\bar{x}_{l,k}^m,u_{l,k}). \tag{17}$$

Case 2: The measurement noise follows non-Gaussian distribution.

Note that the analytical approach developed in Case 1 is no longer suitable for this case and, as such, we choose to adopt the Monte-Carlo method to approximate the likelihood function $p(z_{l,k}|x_{l,k},u_{l,k})$. To be specific, for each particle $\bar{x}_{l,k}^m$, N samples (denoted as $\{z_{l,k}^{m,n}\}_{n=1}^N$) are drawn from the measurement function (5) and the encryption-decryption process. Then, the likelihood function evaluated at $\bar{x}_{l,k}^m$ can be approximated as

$$p(z_{l,k}|\bar{x}_{l,k}^m,u_{l,k})=\prod_{s=1}^{n_z}\left(\frac{1}{N}\sum_{n=1}^{N}\mathbb{I}_{\{z_{l,k}^{[s],m,n}=z_{l,k}^{[s]}\}}\right), \tag{18}$$

where $\mathbb{I}_{\{z_{l,k}^{[s],m,n}\le z_{l,k}^{[s]}\}}$ is an indicator function and

$$\mathbb{I}_{\{z_{l,k}^{[s],m,n}\le z_{l,k}^{[s]}\}}=\begin{cases}1, & \text{if } z_{l,k}^{[s],m,n}\le z_{l,k}^{[s]},\\ \beta, & \text{otherwise}\end{cases} \tag{19}$$

with β being a positive scalar and $\beta \ll 1$.

Remark 2: The transmission model we adopted in this paper is actually a kind of nonlinear mapping and such a model would make the distribution of the actual measurement (i.e. $z_{l,k}$) different from the one of the original measurement (i.e. $\bar{z}_{l,k}$). As a consequence, the estimation performance may degrade severely if we use the actual measurement directly under the framework of the SIR-based PF algorithm. For the purpose of mitigating the influences on the estimation performance caused by the transmission model, a novel likelihood function is proposed to calculate the importance weights in which the parameters of the transmission model are fully considered.

Remark 3: For the computational complexities of the PF algorithm, there have been some scattered theoretical analysis results available in the literature, see e.g. [44], [45]. For example, in [44], the analytical expression of the computational complexities of the marginalized particle filter has been derived by calculating the number of floating-point operations. Note that in practice, the complicated factors (e.g. the nonlinear strength of the system, the various resampling strategies, the number of particles) involved in the PF algorithm make it difficult to follow the similar lines to conduct a rigorous analysis on the computational complexities. In order to assess the computational complexity of the PF algorithm in an easy-to-implement way, another widely used approach is to measure the time required in each step of iteration. For instance, in [46], a multi-scale based method has been proposed to accelerate the tracking computation of the particle filters, and the efficiency of the proposed algorithm has been verified by comparing the computational time with the one of the conventional PF algorithm. In this paper, the computational complexity of our proposed algorithm is assessed by measuring the execution time of each iteration.

For ease of illustration, the pseudocode of our proposed secure state estimation algorithm is outlined in Algorithm 1.

Algorithm 1 Secure particle filtering algorithm under the Paillier encryption-decryption scheme.

Initialization: Generate particles $\{x_{l,0}^m\}_{m=1}^M$ from the initial PDF $p_{x_{l,0}}$ and set the associated weights $\{\omega_{l,0}^m\}_{m=1}^M$ as $1/M$.

Recursion:

for $k=0,1,2,\ldots$ **do**
  Collect the measurement after decryption (i.e. $z_{l,k}$) at the current time instant.
  for $m=0,1,2,\ldots,M$ **do**
    Propagate the posterior particle $x_{l,k-1}^m$ one-step ahead through (11) to generate the prior particle $\bar{x}_{l,k}^m$.
    Case 1: Measurement noise follows Gaussian distribution. Compute the likelihood function $p(z_{l,k}|\bar{x}_{l,k}^m,u_{l,k})$ via (16) and (17).
    Case 2: Measurement noise follows non-Gaussian distribution.
    Compute the likelihood function $p(z_{l,k}|\bar{x}_{l,k}^m,u_{l,k})$ via (18) and (19).
    Calculate the corresponding unnormalized importance weight $\bar{\omega}_{l,k}^m$ via (13).
    Compute the normalized importance weights $\{\omega_{l,k}^m\}_{m=1}^M$ according to (14).
    Compute the estimate $\hat{x}_{l,k}$ by using (15).
    Resample to obtain the new particle set $\{x_{l,k}^m\}_{m=1}^M$.
  end for
end for

V. Simulation Example

To verify the effectiveness of our proposed secure state estimation algorithm, the model IEEE 39-bus system has been use for the simulation examples and the Matlab/Simulink has been adopted for its modeling. The detailed parameters of each SG described in (1), (2) and (4) can be found in [47]. For the sake of saving space, only the states of SG 3 are taken for illustration. The system is initialized with steady state values obtained from the pre-disturbance system condition, i.e. $x_{3,0}\sim\mathcal{N}([0.9\ 0.5\ 0.1\ 0.45]^T,\mathrm{diag}_4\{0.01^2\})$. The number of particles is selected as $M=200$. The initial particles of SG 3 are generated from the initial PDF of the states, i.e. $x_{3,0}^m\sim\mathcal{N}([0.9\ 0.5\ 0.1\ 0.45]^T,\mathrm{diag}_4\{0.01^2\})$ where $m\in\{1,2,\ldots,M\}$. The associated weights of the initial particles are all set to be $1/M$.

The notion mean square error (MSE) is adopted to evaluate the estimation accuracy where MSE_j denotes MSE for the estimate of the j-th state over H_{MC} independent Monte Carlo runs, i.e.,

$$\mathrm{MSE}_j=\frac{1}{H_{MC}}\sum_{h=1}^{H_{MC}}\left(x_{l,k}^{[j,h]}-\hat{x}_{l,k}^{[j,h]}\right)^2,$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TSG.2023.3271949, IEEE Transactions on Smart Grid

with $x_{l,k}^{[j,h]}$ and $\hat{x}_{l,k}^{[j,h]}$ being the actual and estimated values of $x_{l,k}^{[j]}$ (i.e. the j-th state of the l-th synchronous generator) in the h-th run. In addition, we set the public key and the private key as $\mathcal{PK} = (20687, 53)$ and $\mathcal{SK} = (10200, 14141)$, respectively. To simplify the notation, the estimation results of the conventional SIR-based particle filter under the original measurement (i.e. $\bar{z}_{l,k}$) is labeled as SIR-PF-O, the estimation results of the conventional SIR-based particle filter, extend Kalman filter (EKF), unscented Kalman filter (UKF) and our proposed algorithm under the actual measurement $z_{l,k}$ (i.e. measurement after encryption-decryption) are labeled as SIR-PF-A, EKF-A, UKF-A and Enc-Dec-PF-A, respectively.

A. Scenario 1: Gaussian Noise

In this scenario, both the process and measurement noises follow the Gaussian distributions. To be specific, the Gaussian white sequences with zero means and covariance matrices $5 \times 10^{-6}I$ and $10^{-4}I$ are used to characterize the process noise and measurement noise, respectively. The length between the neighboring quantization levels is selected as $r = 0.1$.

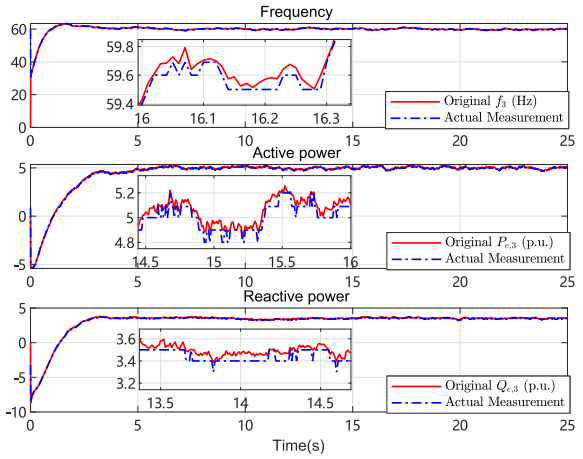
In order to assess the state estimation performance, comparisons between the SIR-PF-O, SIR-PF-A and Enc-Dec-PF-A are carried out. The simulation results are plotted in Fig. 2. Specifically, the original measurement curves and the corresponding curves after decryption are given in Fig. 2(a). The trajectories of the states and the corresponding estimates of SG 3 with the SIR-PF-O, SIR-PF-A and Enc-Dec-PF-A are shown in Fig. 2(b). Fig. 2(c) shows the log(MSE) of each state of the SIR-PF-O, SIR-PF-A and Enc-Dec-PF-A with 20 Monte Carlo runs.

From Fig. 2, it can be found that under Gaussian noises: 1) the measurement after encryption-decryption (i.e. the actual measurement) derivatives significantly from the original measurement; 2) the revised likelihood function is effective since our proposed algorithm (i.e. Enc-Dec-PF-A) is capable of tracking the state effectively with the cryptographic measurement; 3) our proposed algorithm performs better than the conventional SIR-based PF (i.e. SIR-PF-A) under the cryptographic measurement; and 4) the estimation accuracy of our proposed algorithm under the cryptographic measurement is close to the one of the conventional SIR-based PF under the original measurement (i.e. SIR-PF-O).

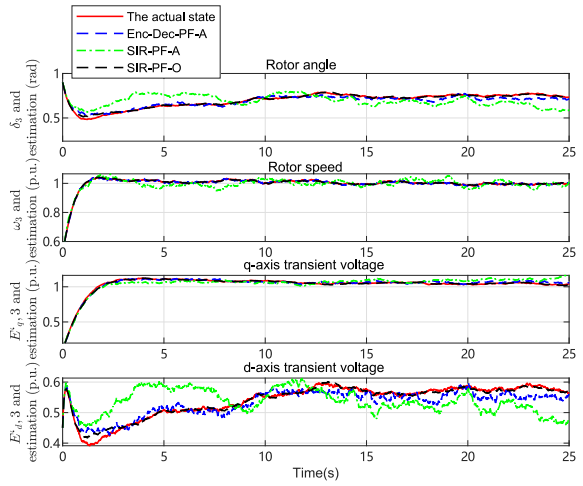
B. Scenario 2: Non-Gaussian Noise

In this scenario, the GMM-based non-Gaussian sequences are used to simulate the process and measurement noises, i.e. $w_{3,k} \sim 0.8\mathcal{N}_1(0, 5 \times 10^{-6}I) + 0.2\mathcal{N}_2(0, 10^{-4}I)$ and $v_{3,k} \sim 0.9\mathcal{N}_1(0, 10^{-4}I) + 0.1\mathcal{N}_2(0, 10^{-2}I)$. The length of the quantization level is still selected as $r = 0.1$.

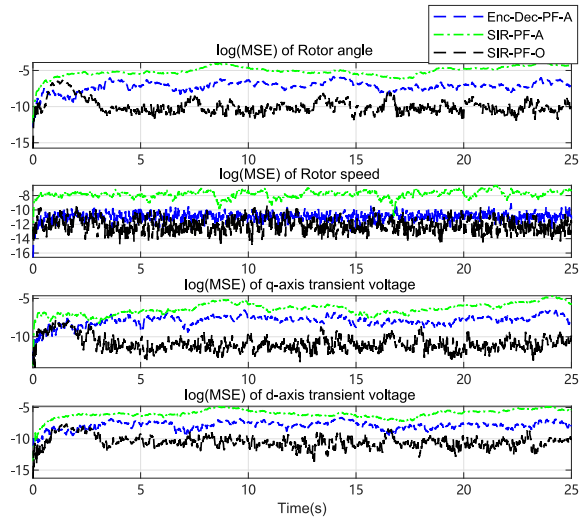
The simulation results under Scenario 2 are plotted in Fig. 3. The effects of the encryption-decryption on the measurements are clearly reflected in Fig. 3(a). The states and the corresponding estimates obtained with the SIR-PF-O, SIR-PF-A and Enc-Dec-PF-A are plotted in Fig. 3(b). Fig. 3(c) shows the log(MSE) of each state of the SIR-PF-O, SIR-PF-A and Enc-Dec-PF-A with 20 Monte Carlo runs.



(a)



(b)

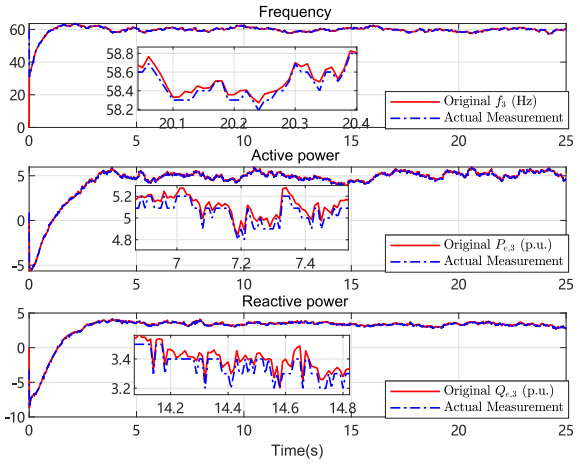


(c)

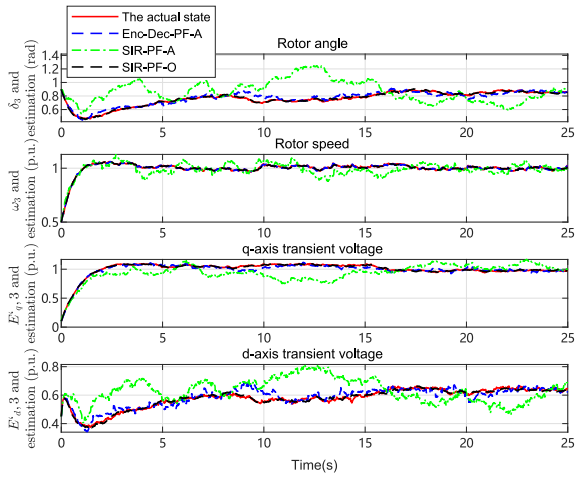
Fig. 2: Scenario 1: Simulation results of SG 3 (a) Measurement curves. (b) Estimated states. (c) Log(MSE) of each estimate.

It can be observed from Fig. 3 that under non-Gaussian noises: 1) the measurement after encryption-decryption is totally different from its original value; 2) the Enc-Dec-PF-A

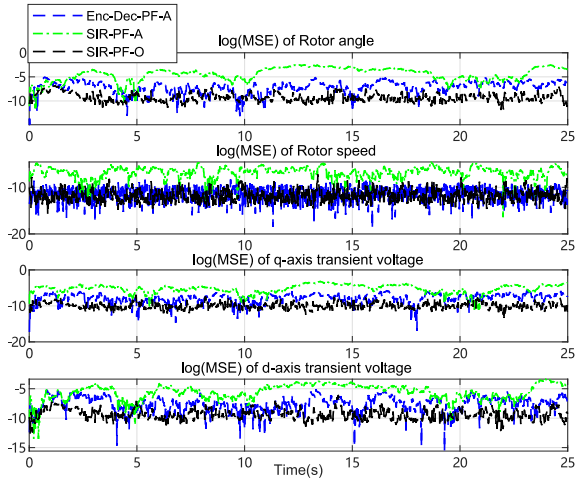
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TSG.2023.3271949, IEEE Transactions on Smart Grid



(a)



(b)



(c)

Fig. 3: Scenario 2: Simulation results of SG 3 (a) Measurement curves. (b) Estimated states. (c) Log(MSE) of each estimate.

performs well in the presence of information loss caused by the encryption-decryption process; 3) under the cryptographic measurement, the estimation performance of the Enc-Dec-PF-A outperforms the one of the SIR-PF-A due to the revised likelihood function; and 4) the estimation accuracy of our proposed algorithm under the cryptographic measurement is close to the one of the conventional SIR-based PF under the original measurement (i.e. SIR-PF-O).

C. Computational Efficiency

In this subsection, the computational efficiency of each algorithm under the cryptographic measurement is discussed. All the test cases are implemented on a PC with Intel Core CPU i7-7700HQ, 2.80GHz and 16 GB RAM. The average computing time (ACT) of each algorithm is presented in Table II. From Table II, we can conclude that: 1) the ACT of the encryption-decryption process is about 10 ms which is less than the PMU scan rate (20 ms/sample); and 2) the ATC of the Enc-Dec-PF-A is longer than the one of the SIR-PF-A due to the computation of the modified likelihood function; and 3) the total ATC of Enc-Dec-PF-A is less than the PMU scan rate, which means that our proposed state estimation algorithm is able to implement online.

TABLE II: Average Computing Time At Each PMU Scan (ms)

Algorithm	Encryption Decryption	State Estimation	Total
Enc-Dec-PF-A	8.87	8.15	17.02
SIR-PF-A	9.81	4.84	14.65

D. Discussions

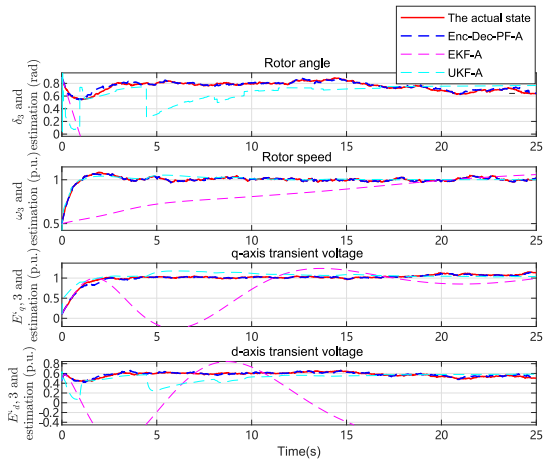
In this subsection: 1) the comparisons between our proposed algorithm, EKF and UKF are all performed under the cryptographic measurement; and 2) the effects of the number of particles on the estimation accuracy and computation time of our proposed algorithm are discussed. The simulation conditions remain the same as they are shown in Scenario 2. To be specific: 1) the curves of the states and the corresponding estimates under the cryptographic measurement of SG 3 with the Enc-Dec-PF-A, EKF-A and UKF-A are shown in Fig. 4(a); 2) Fig. 4(b) shows the log(MSE) of each state of the Enc-Dec-PF-A, EKF-A and UKF-A with 20 Monte Carlo runs; and 3) Fig. 5 and Table III reveal the effects of the number of particles (i.e. M=100,200 and 300) on the estimation performance and computation time, respectively.

TABLE III: Average Computing Time Of Each Iteration For The Enc-Dec-PF-A With Different Number Of Particles (ms)

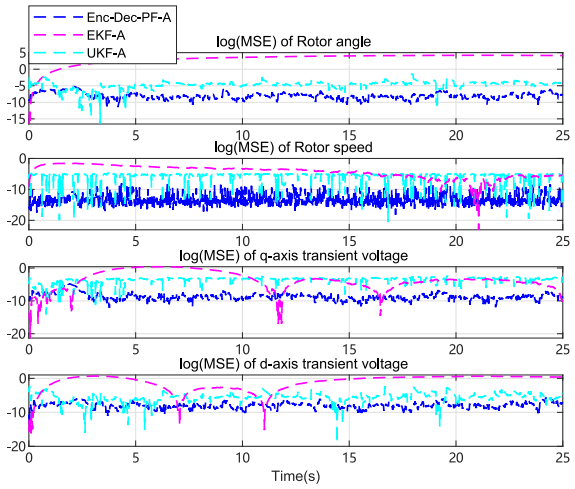
Number of Particles	State Estimation
100	3.85
200	8.06
300	12.37

From Fig. 4, it can be found that under non-Gaussian noises: 1) the estimation results of the EKF-A and UKF-A deviate significantly from their true values; and 2) our proposed algorithm outperforms the EKF-A and UKF-A. Moreover, it can be concluded from Fig. 5 and Table III that the estimation accuracy and computation time of the proposed algorithm all increase along with the growing number of particles.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TSG.2023.3271949, IEEE Transactions on Smart Grid



(a)



(b)

Fig. 4: Comparison studies of SG 3 (a) Estimated states. (b) Log(MSE) of each estimate.

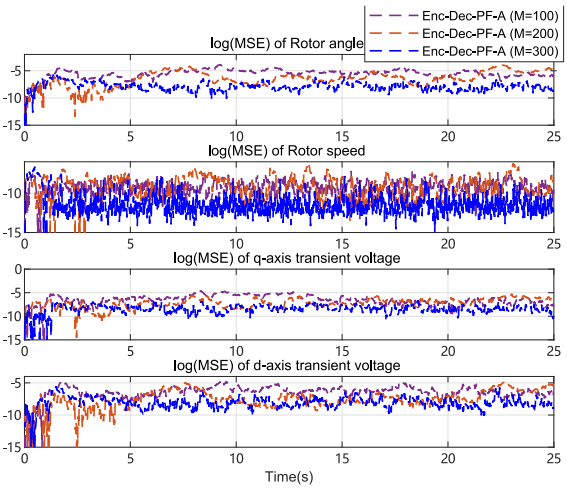


Fig. 5: Log(MSE) of each state of SG 3 with different number of particles.

VI. Conclusion

In this paper, the secure state estimation problem has been investigated for a class of multi-machine power grids. For the purpose of enhancing the transmission security and preserving the data privacy, the Paillier encryption-decryption scheme has been adopted. A novel state estimation algorithm has been proposed to mitigate the influences caused by the nonlinearities and non-Gaussian noises as well as the encryption-decryption process on the estimation performance. Specifically, the PF technique has been adopted to tackle the nonlinearity/non-Gaussianity of the systems and the modified likelihood function has been developed by fully taking the encryption-decryption process of the measurement data. Finally, based on the IEEE 39-bus system, three test scenarios have been considered in the simulation experiment to validate the effectiveness of the proposed secure state estimation scheme.

References

[1] Y. Liang, Z. Ding, T. Ding and W.-J. Lee, Mobility-aware charging scheduling for shared on-demand electric vehicle fleet using deep reinforcement learning, *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1380–1393, 2021.

[2] X. Wan, F. Wei, C.-K. Zhang and M. Wu, Hybrid variables-dependent event-triggered model predictive control subject to polytopic uncertainties, *International Journal of Systems Science*, vol. 53, no. 14, pp. 3042-3055, 2022.

[3] D. Ding, Q.-L. Han, X. Ge and J. Wang, Secure state estimation and control of cyber-physical systems: A survey, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 1, pp. 176–190, 2021.

[4] X. Wang, Y. Sun and D. Ding, Adaptive dynamic programming for networked control systems under communication constraints: a survey of trends and techniques, *International Journal of Network Dynamics and Intelligence*, vol. 1, no. 1, pp. 85-98, 2022.

[5] F. Qu, X. Zhao, X. Wang and E. Tian, Probabilistic-constrained distributed fusion filtering for a class of time-varying systems over sensor networks: A torus-event-triggering mechanism, *International Journal of Systems Science*, vol. 53, no. 6, pp. 1288-1297, 2022.

[6] Z. Fang, Y. Lin, S. Song, C. Li, X. Lin and Y. Chen, State estimation for situational awareness of active distribution system with photovoltaic power plants, *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 239–250, 2021.

[7] S. Das and B. K. Panigrahi, A PMU-based data-driven approach for enhancing situational awareness in building a resilient power systems, *IEEE Transactions on Industrial Informatics*, vol. 18, no. 7, pp. 4773–4784, 2022.

[8] Y. Chakhchoukh, H. Lei and B. K. Johnson, Diagnosis of outliers and cyber attacks in dynamic PMU-based power state estimation, *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1188–1197, 2020.

[9] N. Zhou, D. Meng, Z. Huang and G. Welch, Dynamic state estimation of a synchronous machine using PMU data: A comparative study, *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 450–460, 2015

[10] M. N. Kurt, Y. Yılmaz and X. Wang, Secure distributed dynamic state estimation in wide-area smart grids, *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 800–815, 2020.

[11] A. F. Taha, J. Qi, J. Wang and J. H. Panchal, Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs, *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 886–899, 2018.

[12] J. Yang, W.-A. Zhang and F. Guo, Dynamic state estimation for power networks by distributed unscented information filter, *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2162–2171, 2020.

[13] K. Emami, T. Fernando, H. H.-C. Iu, H. Trinh and K. P. Wong, Particle filter approach to dynamic state estimation of generators in power systems, *IEEE Transactions on Power Systems*, vol. 30, no. 5, pp. 2665–2675, 2015.

[14] J. Zhao and L. Mili, Power system robust decentralized dynamic state estimation based on multiple hypothesis testing, *IEEE Transactions on Power Systems*, vol. 33, no. 4, pp. 4553–4562, 2018.

[15] R. Caballero-Águila, A. Hermoso-Carazo and J. Linares-Pérez, Networked fusion estimation with multiple uncertainties and time-correlated channel noise, *Information Fusion*, vol. 54, pp. 161–171, 2020.
[16] Y. Su, H. Cai and J. Huang, The cooperative output regulation by the distributed observer approach, *International Journal of Network Dynamics and Intelligence*, vol. 1, no. 1, pp. 20-35, 2022.
[17] X. Li, S. Feng, N. Hou, R. Wang, H. Li, M. Gao and S. Li, Surface microseismic data denoising based on sparse autoencoder and Kalman filter, *Systems Science & Control Engineering*, vol. 10, no. 1, pp. 616-628, 2022.
[18] D. Ciuonzo, A. Aubry, and V. Carotenuto, Rician MIMO channel- and jamming-aware decision fusion, *IEEE Transactions on Signal Processing*, vol. 65, no. 15, pp. 3866–3880, 2017.
[19] G. Bao, L. Ma and X. Yi, Recent advances on cooperative control of heterogeneous multi-agent systems subject to constraints: A survey, *Systems Science & Control Engineering*, vol. 10, no. 1, pp. 539-551, 2022.
[20] W. Li, Y. Niu and Z. Cao, Event-triggered sliding mode control for multi-agent systems subject to channel fading, *International Journal of Systems Science*, vol. 53, no. 6, pp. 1233–1244, 2022.
[21] Y. H. Liu, F. H. Huang and H. Yang, A fair dynamic content store-based congestion control strategy for named data networking, *Systems Science & Control Engineering*, vol. 10, no. 1, pp. 73-78, 2022.
[22] M. Cai, X. He and D. Zhou, Performance-improved finite-time fault-tolerant control for linear uncertain systems with intermittent faults: an overshoot suppression strategy, *International Journal of Systems Science*, vol. 53, no. 16, pp. 3408–3425, 2022.
[23] P. Wen, X. Li, N. Hou and S. Mu, Distributed recursive fault estimation with binary encoding schemes over sensor networks, *Systems Science & Control Engineering*, vol. 10, no. 1, pp. 417–427, 2022.
[24] H. Zhang, D. Yue, C. Dou, X. Xie, K. Li and G. P. Hancke, Resilient optimal defensive strategy of TSK fuzzy-model-based microgrids' system via a novel reinforcement learning approach, *IEEE Transactions on Neural Networks and Learning Systems*, vol. 34, no. 4, pp. 1921–1931, 2023.
[25] F. M. Shakiba, M. Shojaee, S. M. Azizi and M. Zhou, Real-time sensing and fault diagnosis for transmission lines, *International Journal of Network Dynamics and Intelligence*, vol. 1, no. 1, pp. 36-47, 2022.
[26] X. Chen, S. Hu, Y. Li, D. Yue, C. Dou and L. Ding, Co-estimation of state and FDI attacks and attack compensation control for multi-area load frequency control systems under FDI and DoS attacks, *IEEE Transactions on Smart Grid*, vol. 13, no. 3, pp. 2357-2368, 2022.
[27] Y. Cui and R. Kavasseri, A particle filter for dynamic state estimation in multi-machine systems with detailed models, *IEEE Transactions on Power Systems*, vol. 30, no. 6, pp. 3377–3385, 2015.
[28] T. Ahmad and N. Senroy, Statistical characterization of PMU error for robust WAMS based analytics, *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 920–928, 2020.
[29] S. Wang, J. Zhao, Z. Huang and R. Diao, Assessing Gaussian assumption of PMU measurement error using field data, *IEEE Transactions on Power Delivery*, vol. 33, no. 6, pp. 3233–3236, 2018.
[30] Q. Zhang and Y. Zhou, Recent advances in non-Gaussian stochastic systems control theory and its applications, *International Journal of Network Dynamics and Intelligence*, vol. 1, no. 1, pp. 111-119, 2022.
[31] Q. Zhou, M. Shahidehpour, A. Alabdulwahab and A. Abusorrah, Privacy-preserving distributed control strategy for optimal economic operation in islanded reconfigurable microgrids, *IEEE Transactions on Power Systems*, vol. 35, no. 5, pp. 3847–3856, 2020.
[32] M. M. Hossain, C. Peng, H.-T. Sun and S. Xie, Bandwidth allocation-based distributed event-triggered LFC for smart grids under hybrid attacks, *IEEE Transactions on Smart Grid*, vol. 13, no. 1, pp. 820–830, 2022.
[33] T. T. Kim and H. V. Poor, Strategic protection against data injection attacks on power grids, *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326–333, 2011.
[34] S. Siamak, M. Dehghani and M. Mohammadi, Dynamic GPS spoofing attack detection, localization, and measurement correction exploiting PMU and SCADA, *IEEE Systems Journal*, vol. 15, no. 2, pp. 2531–2540, 2021.
[35] Z. Wu, E. Tian and H. Chen, Covert attack detection for LFC systems of electric vehicles: A dual time-varying coding method, *IEEE/ASME Transactions on Mechatronics*, vol. 28, no. 2, pp. 681–691, 2023.
[36] J. A. D. Massignan, J. B. A. London and V. Miranda, Tracking power system state evolution with maximum-correntropy-based extended Kalman filter, *Journal of Modern Power Systems and Clean Energy*, vol. 8, no. 4, pp. 616–626, 2020.
[37] L. Dang, B. Chen, S. Wang, W. Ma and P. Ren, Robust power system state estimation with minimum error entropy unscented Kalman filter, *IEEE Transactions on Instrumentation and Measurement*, vol. 69, no. 11, pp. 8797–8808, 2020.
[38] H. Wang, X. Wen, Y. Xu, B. Zhou, J. Peng and W. Liu, Operating state reconstruction in cyber physical smart grid for automatic attack filtering, *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 2909–2922, 2022.
[39] W. Chen, L. Liu and G.-P. Liu, Privacy-preserving distributed economic dispatch of microgrids: A dynamic quantization based consensus scheme with homomorphic encryption, *IEEE Transactions on Smart Grid*, vol. 14, no. 1, pp. 701–713, 2023.
[40] J. Shang and T. Chen, Linear encryption against eavesdropping on remote state estimation, *IEEE Transactions on Automatic Control*, in press, DOI: 10.1109/TAC.2022.3205548.
[41] Z. Zhang, P. Cheng, J. Wu and J. Chen, Secure state estimation using hybrid homomorphic encryption scheme, *IEEE Transactions on Control System Technology*, vol. 29, no. 4, pp. 1704–1720, 2021.
[42] G. Cheng, Y. Lin, Y. Chen and T. Bi, Adaptive state estimation for power systems measured by PMUs with unknown and time-varying error statistics,*IEEE Transactions on Power Systems*, vol. 36, no. 5, pp. 4882–4491, 2021.
[43] 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.
[44] R. Karlsson, T. Schon and F. Gustafsson, Complexity analysis of the marginalized particle filter, *IEEE Transactions on Signal Processing*, vol. 53, no. 11, pp. 4408–4411, 2005.
[45] F. Daum and J. Huang, Mysterious computational complexity of particle filters, in *Proceedings of SPIE*, vol. 4728, pp. 418–426, 2002.
[46] G. Shabat, Y. Shmueli, A. Bermanis and A. Averbuch, Accelerating particle filter using randomized multiscale and fast multipole type methods, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 37, no. 7, pp. 1396—1407, 2015.
[47] IEEE PES TF on Benchmark System for Stability Controls, Benchmark systems for small-signal stability analysis and control, IEEE Power Energy Society, Piscataway, New Jersey, USA, Technical Report, PES-TR18, 2015.

Bogang Qu received the B.Eng. degree in electrical engineering and automation and the M.Eng. degree in electrical engineering from University of Shanghai for Science and Technology, Shanghai, China, in 2014 and 2017, respectively, and the Ph.D. degree in control science and engineering from Donghua University, Shanghai, China, in 2022.

He is currently a Lecturer with the College of Automation Engineering, Shanghai University of Electric Power, Shanghai. From November 2021 to October 2022, he was a visiting Ph.D. Student with the Department of Computer Science, Brunel University London, Uxbridge, U.K. His current research interests include state estimation and information perception and their applications in smart grids. He is a very active reviewer for many international journals.

Zidong Wang (Fellow, IEEE) received the B.Sc. degree in mathematics in 1986 from Suzhou University, Suzhou, China, and the M.Sc. degree in applied mathematics in 1990 and the Ph.D. degree in electrical engineering in 1994, both from Nanjing University of Science and Technology, Nanjing, China.

He is currently Professor of Dynamical Systems and Computing in the Department of Computer Science, Brunel University London, U.K. From 1990 to 2002, he held teaching and research appointments in universities in China, Germany and the UK. Prof. Wang's research interests include dynamical systems, signal processing, bioinformatics, control theory and applications. He has published more than 700 papers in international journals. He is a holder of the Alexander von Humboldt Research Fellowship of Germany, the JSPS Research Fellowship of Japan, William Mong Visiting Research Fellowship of Hong Kong.

Prof. Wang serves (or has served) as the Editor-in-Chief for *International Journal of Systems Science*, the Editor-in-Chief for *Neurocomputing*, the Editor-in-Chief for *Systems Science & Control Engineering*, and an Associate Editor for 12 international journals including IEEE Transactions on Automatic Control, IEEE Transactions on Control Systems Technology, IEEE Transactions on Neural Networks, IEEE Transactions on Signal Processing, and IEEE Transactions on Systems, Man, and Cybernetics-Part C. He is a Member of the Academia Europaea, a Member of the European Academy of Sciences and Arts, an Academician of the International Academy for Systems and Cybernetic Sciences, a Fellow of the IEEE, a Fellow of the Royal Statistical Society and a member of program committee for many international conferences.

Bo Shen (Senior Member, IEEE) received the B.Sc. degree in mathematics from Northwestern Polytechnical University, Xi'an, China, in 2003, and the Ph.D. degree in control theory and control engineering from Donghua University, Shanghai, China, in 2011.

He is currently a Professor with the School of Information Science and Technology, Donghua University. From 2009 to 2010, he was a Research Assistant with the Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong. From 2010 to 2011, he was a Visiting Ph.D. Student with the Department of Information Systems and Computing, Brunel University London, London, U.K. From 2011 to 2013, he was a Research Fellow (Scientific Co-Worker) with the Institute for Automatic Control and Complex Systems, University of Duisburg-Essen, Duisburg, Germany. He has published around 80 articles in refereed international journals. His research interests include nonlinear control and filtering, stochastic control and filtering, as well as complex networks and neural networks.

Prof. Shen serves (or has served) as an Associate Editor or Editorial Board Member for eight international journals, including *Systems Science and Control Engineering*, *Journal of The Franklin Institute*, *Asian Journal of Control*, *Circuits, Systems, and Signal Processing*, *Neurocomputing*, *Assembly Automation*, *Neural Processing Letters*, and *Mathematical Problems in Engineering*. He is a program committee member for many international conferences.

Hongli Dong (Senior Member, IEEE) received the Ph.D. degree in control science and engineering from the Harbin Institute of Technology, Harbin, China, in 2012.

From 2009 to 2010, she was a Research Assistant with the Department of Applied Mathematics, City University of Hong Kong, Hong Kong. From 2010 to 2011, she was a Research Assistant with the Department of Mechanical Engineering, The University of Hong Kong, Hong Kong. From 2011 to 2012, she was a Visiting Scholar with the Department of Information Systems and Computing, Brunel University London, Uxbridge, U.K. From 2012 to 2014, she was an Alexander von Humboldt Research Fellow with the University of Duisburg-Essen, Duisburg, Germany. She is currently a Professor with the Artificial Intelligence Energy Research Institute, Northeast Petroleum University, Daqing, China. She is also the Director of the Heilongjiang Provincial Key Laboratory of Networking and Intelligent Control, Daqing. Her current research interests include robust control and networked control systems.

Dr. Dong is a very active reviewer for many international journals.

Xin Zhang (Senior Member, IEEE) is currently a Professor of Control and Power Systems with University of Sheffield, U.K. Previously he was a Senior Lecturer in electronic and electrical engineering with Brunel University London, U.K. He was with National Grid U.K. for real-time power system operation and control in the Electricity National Control Centre. His research interests include power system control, planning and operation, cyber-physical power systems modelling and co-simulation, and grid-integrated transport electrification.

Prof. Zhang received the B.Eng. degree in automation and control systems from Shandong University, China, in 2007, the M.Sc. and Ph.D. degrees in electrical power engineering from The University of Manchester, U.K., in 2007 and 2010, respectively.

Prof. Zhang is a member of the IEEE P2988 Virtual Synchronous Machines working group, a member of the CIGRE SC B5 Protection and Automation working group. He is a Chartered Engineer with the U.K. Engineering Council.