Deep learning enhanced situation awareness for high renewable-penetrated power systems with multiple data corruptions

Qi Wang[1]*, Siqi Bu*[1] ✉

[1]*Department of Electrical Engineering, The Hong Kong Polytechnic University, Kowloon, Hong Kong*

✉ *E-mail: siqi.bu@polyu.edu.hk*

Abstract: High renewable penetration and inevitable data corruptions can prominently jeopardise the security of power systems and greatly challenge the conventional situation awareness (SA). This study proposes an enhanced SA model that solves two major difficulties faced by the conventional SA. The first difficulty is to accurately detect anomalies, especially the imperceptible variation of renewable power output. This is addressed by a novel aggregation of random matrix and long short-term memory network. The model's high accuracy and alertness in real-time anomaly detection are achieved by a newly proposed perceptual indicator. The second difficulty is to be robust against multiple data corruptions. In this connection, a dedicated workflow is designed to mitigate the impact of data corruptions from two stages, which ensures the robustness of the enhanced SA model. By comparing with several existing conventional SA models, the proposed enhanced SA model has shown its prominent superiority in several practical scenarios. In addition, a fast security check is also achieved by the enhanced SA model to indicate the security margin of the system on different renewable penetration levels. The enhanced SA model can reinforce the system operators' observability on insecure risks and hedge them against potential data manipulations or cyber attacks.

1 Introduction

The power industry is experiencing an unprecedented evolution towards decarbonisation and digitisation currently. On the one hand, different types of renewable energy sources (RESs) such as wind and solar power are being integrated into power systems at a markedly increasing pace. Nevertheless, the high penetration of power electronics-based RESs has greatly reduced system's inertia, which can prominently jeopardise the security of power systems [1]. Take the power cut in UK in August 2019 as an example, the final technical report has shown that one of the major causes of this event was an unexpected power output reduction of an off-shore wind farm [2]. On the other hand, profiting from the rapidly developed information and communication technology (ICT), power systems have reached a certain level of digitisation. Modern power systems are hence being treated as comprehensive cyber physical systems (CPS) in a large number of recent research studies. However, the complicated communication and cyber environment not only brings about intractable data quality issues, but also makes power systems more vulnerable to cyber attacks. For instance, the Ukraine blackout in December 2015 is attributed to synchronised and coordinated cyber attacks [3], and the US government even passed a legislation to isolate power equipment from grid operators' digital control systems to prevent the similar blackout accident [4].

One of the common causes of above incidents is that the system operators failed to be fully cognisant of what they need to know, especially the security status of the system. To tackle this issue, situation awareness (SA) can be served as a viable solution. SA endows the system operators with the ability of panoramic perception in wide area, in order to efficaciously ensure a secure, stable and smooth operation of power systems [5]. Since first explored from the area of military and aviation, SA has attracted extensive attentions in the power industry over the past few years [6]. In power systems, SA is considered as the operators' temporal and spatial perception of dynamic changes in the current system and environment, as well as appropriate comprehension and associated measures taken, to implement actions on the projection of system's future status [7]. Although certain efforts have been devoted to SA to some extent [5–8], the performance of the conventional SA is too limited to reach a satisfactory level when coping with today's data-oriented power systems.

The development of wide area measurement system has promoted wide deployments of phasor measurement units (PMUs) on critical points of the system, to offer essential measurement data in a real-time manner [1]. This creates great opportunities for SA to acquire substantial data in order to reveal the actual status of power systems [5]. However, enormous challenges are also produced for the conventional SA along with the great opportunities. Widely dispersed PMUs require massive ICT auxiliaries, which lead to tight interactions between the cyber part and the physical part of the CPS [9, 10]. The interactions tend to expose the measurement data in a vulnerable cyber environment, which can result in multiple data corruptions. These data corruptions include: (i) data quality problems such as *data loss* and *time delay* [11, 12]; (ii) malicious data attacks such as *replay attack*, *false anomaly injection* and *denial of service attack* [13, 14]; (iii) *insufficient measurements* or *incomplete data sets* [15].

The above challenges have opened up data-driven solutions rather than establish a full understanding of the physical model. Recently, many studies of data-driven approaches have sought help from the machine learning or even deep learning algorithms such as decision tree (DT) [16, 17], *k*-nearest neighbour (*k*NN) [18] and long short-term memory (LSTM) network [19, 20]. Among these algorithms, the LSTM network has shown its promising prediction ability which can be utilised to detect anomalies from sequential data. Moreover, some other pioneering studies have explored a new SA possibility for power systems based on big data techniques such as random matrix [8, 21]. As a data pre-processing tool, the random matrix has shown certain feasibility under noisy and bad data environment. However, the enhanced SA has claimed a much higher goal to cope with the challenge of multiple data corruptions in the complex spatiotemporal presence, especially for high renewable-penetrated power systems. It is a challenging task to distinguish implicit anomalies (e.g. abnormal wind power output variation) from multiple data corruptions, and the performance of individual LSTM network or random matrix algorithms can be awfully limited. In this connection, an aggregation of these algorithms is worth trying to improve their respective performances and hence to enhance the conventional SA to a great extent.

The aim of this paper is to facilitate an enhanced SA for high renewable-penetrated power systems with multiple data corruptions. A pure data-driven approach is proposed by applying deep learning technique and random matrix theory in the enhanced SA model. The novel idea is to aggregate the LSTM network with random matrix, where the deep LSTM network is responsible for processing, memorising and predicting the sequential data, while the random matrix is utilised as the pre-processor to implement data cleansing, feature selection and dimensionality reduction. The contributions of this paper can be summarised as follows.

(i) The enhanced SA model achieves high accuracy and alertness in the real-time anomaly detection, by a novel aggregation of random matrix and LSTM network. Based on a newly proposed perceptual indicator, the detectability of the enhanced SA model prominently outperforms many existing conventional SA models. It reinforces the system operators' observability on any suspicious variation of the system, in order to implement appropriate recovery controls opportunely and promptly.
(ii) A dedicated workflow is presented to endow the enhanced SA model with salient robustness against multiple data corruptions. A two-stage mitigation process is designed in the workflow to greatly mitigate the impact of data corruptions, and hence arms SA with vital immunity under an increasingly vulnerable cyber environment. It hedges the system operators against potential data manipulations or cyber attacks, in order to provide appropriate perceptions and hence facilitate proper decisions for system control.
(iii) The enhanced SA can also realise fast security check on different renewable penetration levels, which explicitly indicate the security margin of a given system. It is not only helpful for the assignment of appropriate renewable proportion in the planning stage, but also efficacious to reveal the system tolerance for the system operators in order to take hedging action from insecure risks in the operation stage.

The remainder of this paper is organised as follows. Section 2 gives the proposed methodology, including the theoretical foundations of random matrix and LSTM network, as well as the proposed perceptual indicator and designed workflow. Section 3 is the case study which shows a wide range of application scenarios of the enhanced SA model and the comparative study with other benchmarks in the literature. Section 4 finally concludes this paper.

2 Proposed methodology

2.1 Random matrix and single ring theorem

A matrix is called random matrix when every entry of it is a random variable. In the probability space $(\Omega, \mathbb{F}, \Pr)$ with a sample space Ω, a set of events $\mathbb{F}$ and the probability measure Pr, an $n \times m$ random matrix with random variables $\{X_{ij}\}_{1 \le i \le n, 1 \le j \le m}$ are denoted as $\boldsymbol{X}$. In order to study the statistic properties of a random matrix, the theorem of spectral analysis is developed by reinterpreting a random measure of the empirical process [22]. In the theorem of spectral analysis, empirical spectral distribution (ESD) and limiting spectral distribution (LSD) are two crucial metrics that describe the eigenvalue distribution of the random matrix. For an arbitrary $n \times n$ complex random matrix $\boldsymbol{A}$ with complex eigenvalues $\lambda_i^{\boldsymbol{A}}$, $i = 1, 2, \ldots, n$, the two-dimensional ESD function of $\boldsymbol{A}$ is given by

$$F^{\boldsymbol{A}}(x, y) = \frac{1}{n} \sum_{i=1}^{n} \delta_{\mathrm{Re}(\lambda_i^{\boldsymbol{A}})}(\mathbb{M}_x) \cdot \delta_{\mathrm{Im}(\lambda_i^{\boldsymbol{A}})}(\mathbb{M}_y) \tag{1}$$

where $\delta_{\mathrm{Re}(\lambda_i^{\boldsymbol{A}})}(\mathbb{M}_x)$ and $\delta_{\mathrm{Im}(\lambda_i^{\boldsymbol{A}})}(\mathbb{M}_y)$ are the Dirac measures defined on measurable sets $\mathbb{M}_x \triangleq (-\infty, x] \subseteq \mathbb{F}$ and $\mathbb{M}_y \triangleq (-\infty, y] \subseteq \mathbb{F}$, respectively, $\mathrm{Re}(\lambda_i^{\boldsymbol{A}})$ and $\mathrm{Im}(\lambda_i^{\boldsymbol{A}})$ are the corresponding real and imaginary parts of the ith eigenvalue.

Based on ESD, more attentions are drawn on the convergence problem of the sequence of ESDs for a series of random matrices. Let $\{\boldsymbol{A}_k\}_{k=1}^{(L)}$ concisely denotes the random matrices sequence $\{\boldsymbol{A}_1, \boldsymbol{A}_2, \ldots, \boldsymbol{A}_L\}$. If the ESD sequence $\{F^{\boldsymbol{A}_k}\}_{k=1}^{(L)}$ converges to F^{∞} as the sequence length $L \to \infty$, F^{∞} is called the LSD of $\{\boldsymbol{A}_k\}_{k=1}^{(L)}$. LSD is generally non-random while ESDs are random metrics of various random matrices. The significance of ESD and LSD is that many essential statistics in multivariate spectral analysis can be reinterpreted by ESD and LSD of random matrices. When big data issues involved i.e. the dimensions (number of rows and columns) of random matrices are tending to infinity, LSD shows salient spectral signatures of random matrices described by the single ring theorem [8, 21].

Considering an $n \times m$ non-Hermitian random matrix $\boldsymbol{X}$ with raw data entries, the following normalisation formula is applied to get a standard Gaussian random matrix $\tilde{\boldsymbol{X}}$ from $\boldsymbol{X}$:

$$\tilde{x}_{ij} = (x_{ij} - \mu(\boldsymbol{x}_i)) \cdot \frac{\sigma(\tilde{\boldsymbol{x}}_i)}{\sigma(\boldsymbol{x}_i)} + \mu(\tilde{\boldsymbol{x}}_i) \tag{2}$$

where $\boldsymbol{x}_i = (x_{i1}, x_{i2}, \ldots, x_{im})$, $\tilde{\boldsymbol{x}}_i = (\tilde{x}_{i1}, \tilde{x}_{i2}, \ldots, \tilde{x}_{im})$, $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, m$, $\mu(\boldsymbol{x}_i)$, $\sigma(\boldsymbol{x}_i)$, $\mu(\tilde{\boldsymbol{x}}_i)$ and $\sigma(\tilde{\boldsymbol{x}}_i)$ are the respective expectations and standard deviations of row vectors $\boldsymbol{x}_i$ and $\tilde{\boldsymbol{x}}_i$, $\mu(\tilde{\boldsymbol{x}}_i) = 0$ and $\sigma(\tilde{\boldsymbol{x}}_i) = 1$.

As the singular value decomposition of $\tilde{\boldsymbol{X}}$ exists, one can obtain an $n \times n$ singular value equivalent matrix $\check{\boldsymbol{X}}$ of $\tilde{\boldsymbol{X}}$ as

$$\check{\boldsymbol{X}} = \sqrt{\tilde{\boldsymbol{X}}\tilde{\boldsymbol{X}}^{\dagger}}\boldsymbol{U} \tag{3}$$

where $\tilde{\boldsymbol{X}}^{\dagger}$ denotes the conjugate transpose of $\tilde{\boldsymbol{X}}$ and $\boldsymbol{U}$ is a Haar distributed unitary random matrix which satisfies the following lemma.

Lemma 1: For every Borel subset $\mathbb{H}$ of the set of all unitary matrices $\mathbb{U}$, the following probability holds as

$$\Pr\{\boldsymbol{U} \in \mathbb{H} \subset \mathbb{U}\} = \Xi(\mathbb{H})$$

where $\Xi(\mathbb{H})$ is the normalised Haar measure defined on $\mathbb{H}$.

In the sequence of several random matrices, the product matrix is defined as

$$\boldsymbol{Z} = \prod_{k=1}^{L} \check{\boldsymbol{X}}_k \tag{4}$$

Then the normalised form of the product matrix, which is denoted as $\tilde{\boldsymbol{Z}}$, is obtained by a row-by-row operation as

$$\tilde{z}_i = \frac{z_i}{\sqrt{n}\sigma(z_i)} \tag{5}$$

where $z_i = (z_{i1}, z_{i2}, \ldots, z_{in})$, $\tilde{z}_i = (\tilde{z}_{i1}, \tilde{z}_{i2}, \ldots, \tilde{z}_{in})$ for $i = 1, 2, \ldots, n$ and $\sigma(z_i)$ is the standard deviation of row vector z_i.

After (2)–(5), the sequence of rectangular $n \times m$ random matrices $\{\boldsymbol{X}_k\}_{k=1}^{(L)}$ is characterised by an $n \times n$ square normalised product matrix $\tilde{\boldsymbol{Z}}$ with the same spectral signature. From the accumulation of tremendous PMU measurements data, both $\boldsymbol{X}$ and $\tilde{\boldsymbol{Z}}$ will grow into large dimensional random matrices, whose spectral convergence is described by the following theorem.

Theorem 1 (Single ring theorem): Let the entries of $n \times m$ random matrix $\boldsymbol{X}$ be independent and identically distributed random variables. A sequence of $\boldsymbol{X}$ has a normalised product matrix $\tilde{\boldsymbol{Z}}$ with zero mean and variance $1/n$. Then the ESD of $\tilde{\boldsymbol{Z}}$ converges almost surely to the same density function given by

$$f(\lambda^{\tilde{\boldsymbol{Z}}}) = \begin{cases} \dfrac{1}{\pi\eta L} \| \lambda^{\tilde{\boldsymbol{Z}}} \|^{\frac{2}{L} - 2}, & (1 - \eta)^{\frac{L}{2}} \le \| \lambda^{\tilde{\boldsymbol{Z}}} \| \le 1 \\ 0 & \text{elsewhere} \end{cases}$$

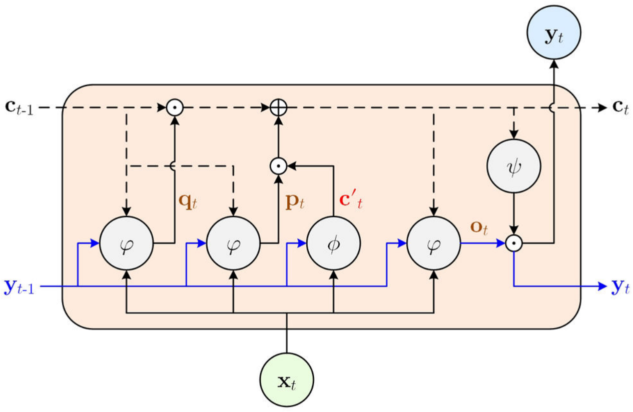


Fig. 1 *Schematic of the LSTM cell within the hidden layers of RNN*

as $n, m \to \infty$ with ratio $\eta = n/m \in (0, 1]$, where $\lambda^{\tilde{\boldsymbol{Z}}}$ is each eigenvalue of $\tilde{\boldsymbol{Z}}$.

2.2 Mean spectral radius

For a random matrix, its statistical properties cannot be revealed by a single eigenvalue, which is an unobservable random variable. The spectral analysis of random matrix mainly focuses on the asymptotic eigenvalues distribution when the dimension of a random matrix becomes very large. Therefore, a natural statistic known as linear eigenvalue statistic (LES) is given via the following definition [23].

Definition 1 (LES): For random matrix $\boldsymbol{A}$ with a sequence of ascending ordered n eigenvalues $\{\lambda_i^{\boldsymbol{A}}\}_{i=1}^{(n)}$, by a given test function $\varepsilon(\cdot)$, the LES of $\boldsymbol{A}$ is defined as

$$\mathcal{N}_n(\varepsilon) = \sum_{i=1}^{n} \varepsilon(\lambda_i^{\boldsymbol{A}})$$

There are various choices of test functions, leading to different forms of LES. A particular form among those LESs, which is called mean spectral radius (MSR), is expressed by

$$r_{\text{MSR}} = \frac{1}{n} \sum_{i=1}^{n} \| \lambda_i^{\boldsymbol{A}} \| \tag{6}$$

MSR can be intuitively interpreted as the average distance of all eigenvalues of random matrix to the centre on the complex plane. MSR appropriately describes the spectral signature of random matrix, whose trace is reflected by LES in general. Together with the single ring theorem, a quick perception of power system's status can be realised according to a relative position between MSR and the single ring. This will be further illustrated in Section 3. On the other hand, the spectral signature expressed by MSR is promising to extract features from random data matrices with large dimensions. In other words, MSR is an essential tool to perform the dimensionality reduction for massive measurement data as well as to excavate innermost features from big data streaming, in order to dramatically enhance the performance of the following deep learning model.

2.3 LSTM network

Recurrent neural network (RNN) is a special deep learning model which is originally designed for processing sequential data. Evolved from RNN, the LSTM network was firstly proposed in [24] and has been improved and popularised by many scholars in a wide range of modern applications [25]. In comparison with regular RNN, the LSTM network is characterised by its memory cell, and hence can memorise information in much longer sequences [26]. Basically, the LSTM cell is composed by several gate units with the functionality to add or remove information over the flow. Although there are a variety of choices on cell mechanisms, this paper uses one of the most popular variants originally proposed in [27]. The detailed mechanism of the LSTM cell is illustrated in Fig. 1.

Three principal gate units, with gate activation function $\varphi(\cdot)$, are designed for the LSTM cell. A forget gate with outputs $\boldsymbol{q}_t$ decides how many memories to keep from previous time step. An input gate with outputs $\boldsymbol{p}_t$ gives the exact value to be updated to the current time step. An output gate with outputs $\boldsymbol{o}_t$ filters out the desired output vector for the current time step. On this basis, the forward propagation of LSTM network is modelled as

$$\boldsymbol{q}_t = \varphi(\overrightarrow{\boldsymbol{W}}_q \boldsymbol{x}_t + \overleftarrow{\boldsymbol{W}}_q \boldsymbol{y}_{t-1} + \widehat{\boldsymbol{W}}_q \boldsymbol{c}_{t-1} + \boldsymbol{b}_q) \tag{7}$$

$$\boldsymbol{p}_t = \varphi(\overrightarrow{\boldsymbol{W}}_p \boldsymbol{x}_t + \overleftarrow{\boldsymbol{W}}_p \boldsymbol{y}_{t-1} + \widehat{\boldsymbol{W}}_p \boldsymbol{c}_{t-1} + \boldsymbol{b}_p) \tag{8}$$

$$\boldsymbol{o}_t = \varphi(\overrightarrow{\boldsymbol{W}}_o \boldsymbol{x}_t + \overleftarrow{\boldsymbol{W}}_o \boldsymbol{y}_{t-1} + \widehat{\boldsymbol{W}}_o \boldsymbol{c}_t + \boldsymbol{b}_o) \tag{9}$$

$$\boldsymbol{c}'_t = \phi(\overrightarrow{\boldsymbol{W}}_c \boldsymbol{x}_t + \overleftarrow{\boldsymbol{W}}_c \boldsymbol{y}_{t-1} + \boldsymbol{b}_c) \tag{10}$$

$$\boldsymbol{c}_t = \boldsymbol{q}_t \odot \boldsymbol{c}_{t-1} + \boldsymbol{p}_t \odot \boldsymbol{c}'_t \tag{11}$$

$$\boldsymbol{y}_t = \psi(\boldsymbol{c}_t) \odot \boldsymbol{o}_t \tag{12}$$

In (7)–(12), notations of $\boldsymbol{W}$ with distinct hats and subscripts denote different weights matrices as: $\overrightarrow{\boldsymbol{W}}$, $\overleftarrow{\boldsymbol{W}}$ and $\widehat{\boldsymbol{W}}$ for the input weights, recurrent weights and peephole weights, while $\boldsymbol{W}_q$, $\boldsymbol{W}_p$, $\boldsymbol{W}_o$ and $\boldsymbol{W}_c$ are the corresponding weights to compute $\boldsymbol{q}$, $\boldsymbol{p}$, $\boldsymbol{o}$ and $\boldsymbol{c}'$, respectively. $\boldsymbol{b}_q$, $\boldsymbol{b}_p$, $\boldsymbol{b}_o$ and $\boldsymbol{b}_c$ are bias vectors. By looking at both current input and previous output, the LSTM cell selects a memory candidate $\boldsymbol{c}'_t$ through an input activation function $\phi(\cdot)$, as shown in (10). Then the current memory $\boldsymbol{c}_t$ is updated based on both the previous one and the candidate, according to (11), in which $\odot$ is the pointwise multiplication operator. Finally, the current output is raised by (12) with an output activation function $\psi(\cdot)$ passed through, and transmitted (recurred) to the next time step.

2.4 Perceptual indicator

The SA model, in practice, is an aggregated LSTM network with random matrix as its pre-processor. After generating the measurement random matrices, the spectral analysis, which has been presented in Sections 2.1 and 2.2, is processed to obtain MSRs of the corresponding normalised product matrices in a sequential manner. By the spectral analysis, all measurement data are compressed and projected into a unified representation of MSR, to feed into the LSTM network. After proper training, the LSTM network can present a predicted MSR value, given a sequence of previous ones, step by step. With an appropriate metric, the accuracy of the prediction can be measured by comparing deviations between the predicted values (from the LSTM network) and the true values (from the measurements) of MSR.

In order to set the metric as well as to evaluate the prediction performance of the SA model, a new perceptual indicator named as gradient of the cumulative squared error (GCSE) is proposed by the following definition.

Definition 2 (GCSE): At time step t, given the output of the LSTM network $y(t)$ (i.e. the predicted value) and the true value $y^*(t)$, the GCSE of the LSTM network at time T is defined as

$$e_{\text{GCSE}}(T) = \nabla \int_0^T (y^*(t) - y(t))^2 \, \mathrm{d}t$$

As the perceptual indicator, the GCSE endows the enhanced SA model with powerful ability of anomaly detection. This detectability is ensured by both the effectiveness of MSR and the predictability of the LSTM network. When anomalies occur, the MSR of the system will experience a drop at this time point. However, this drop can be sometimes too slight to be distinguished from possible data corruptions. Fortunately, after applying the

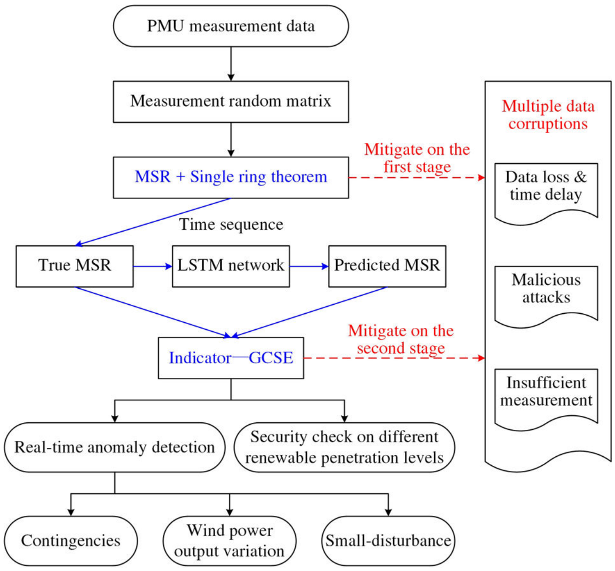

PMU measurement data
Measurement random matrix
MSR + Single ring theorem
Mitigate on the first stage
Multiple data corruptions
Data loss & time delay
Time sequence
True MSR
LSTM network
Predicted MSR
Malicious attacks
Mitigate on the second stage
Indicator—GCSE
Insufficient measurement
Real-time anomaly detection
Security check on different renewable penetration levels
Contingencies
Wind power output variation
Small-disturbance

Fig. 2 *Workflow of the proposed enhanced SA model*

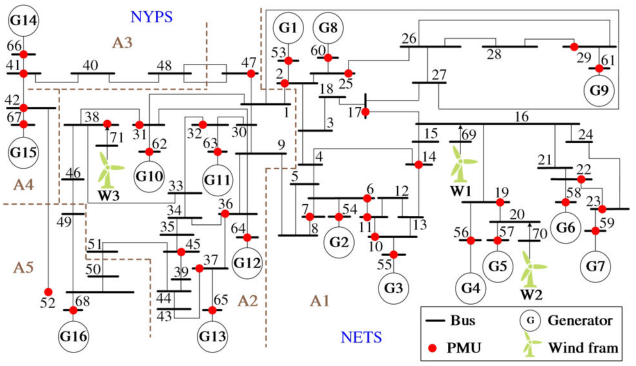


Fig. 3 *NETS-NYPS test system with PMU deployment*

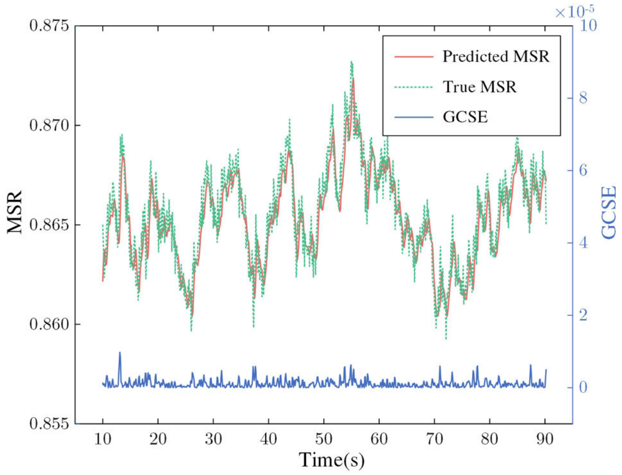


Fig. 4 *Prediction performance of the SA model with the perceptual indicator*

LSTM network, a predicted value of MSR can be obtained and compared with the true value of MSR. The GCSE indicator is designed to handle this comparison and magnify the quantitative distance between the predicted MSR and the true MSR. As a result, the GCSE can be of great activity and alertness in detecting anomalies, which can significantly improve the accuracy of the enhanced SA model.

A workflow of the enhanced SA model is designed and illustrated in Fig. 2. This workflow shows not only the implementation of anomaly detection but also the mitigation of data corruptions, achieved by both MSR and GCSE indicators. Multiple data corruptions are mitigated from two stages by the enhanced SA model. On the first stage, the MSR acts as a unified index of the system's status which is concentrated from all measurements. The redundancy of these measurements guarantees the robustness of MSR to some extent even though a portion of measurement data is corrupted. On the second stage, due to the predictability of the LSTM network, the predicted MSR can tightly track the true MSR. This creates the advantages of GCSE to keep almost stable in the presence of data corruptions but to produce dramatic changes with detected anomalies. Consequently, the robustness of the enhanced SA model is guaranteed by these two mitigation stages.

3 Case study

The New England Test System and the New York Power System (NETS-NYPS) is used as the test system in the case study. The NETS-NYPS consists of five areas and contains 16 generators and 68 buses, with network parameters given in [28]. Furthermore, three wind farms are integrated to the system with three additional buses, and the penetration level of the wind power is configured at 30%. A limited number of 38 PMUs are installed in the system as shown in Fig. 3, as an expanded version of one benchmark deployment given in [29]. This expanded version has supplemented extra 16 PMUs on every PV buses and the slack bus, on top of those 22 PMUs in the original version, to step closer to the actual field scene of PMU placement.

3.1 Model setup

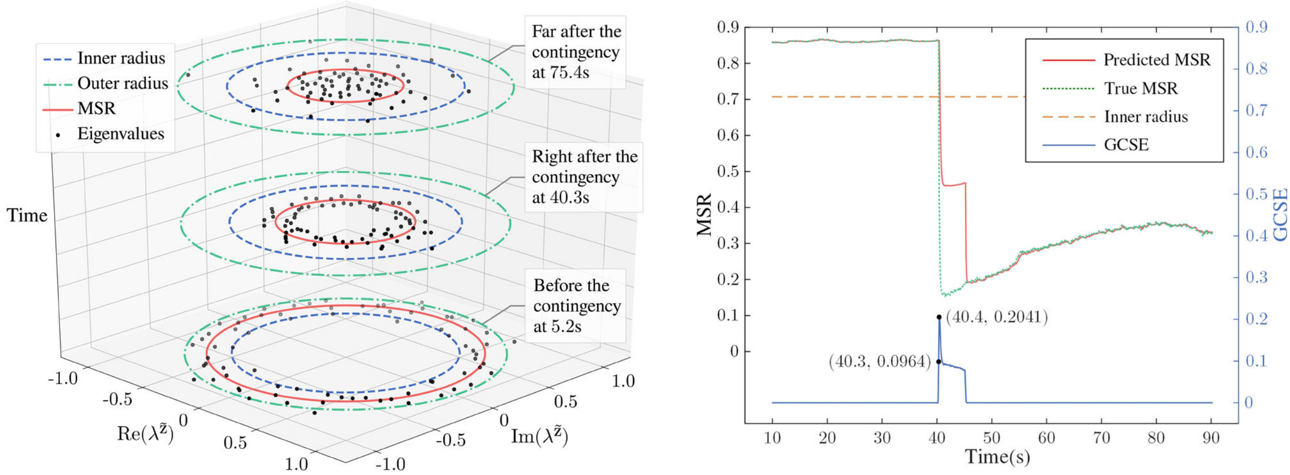
At the first stage, it is sufficient to assume that all 38 PMUs in Fig. 3 can be accessed without any data corruption. By obtaining measurements of both voltage amplitude and phase angle from every PMU (with 1% Gaussian bias), together with a chosen window size which satisfies $\eta = 0.5$, the measurement random matrix $\boldsymbol{X}$ is built with rows $n = 76$ (measurements number) and columns $m = 152$ (window size). As the window slides, a random matrices sequence $\{\boldsymbol{X}\}^{\{T\}}$ is generated in the form of time series. After implementing the spectral analysis, the corresponding MSRs sequence of the normalised product matrices is generated.

Meanwhile, a deep LSTM network is built with three LSTM layers, two dropout layers and one fully connected layer. Each LSTM layer equips with 50 neurons, by choosing the sigmoid function as the gate activation functions and hyperbolic tangent function as both the input and output activation functions. The dropout layers with 20% dropout rate are used to prevent the network from overfitting problems. After the fully connected layer comprising 20 neurons, outputs are raised through a final activation function with the form of exponential linear unit.

When the test system operates in the normal scenario without any anomalies, the measurements data with a total length of 90s are used to generate the MSRs sequence, for training of the deep LSTM network. The mean squared error (MSE) is chosen as a loss function and the Adam algorithm [30] is adopted as an optimiser in the training process. After 100 epochs of training, another 90s data of normal scenario are utilised to test the LSTM network. The test results are shown in Fig. 4 together with the changing values of the perceptual indicator GCSE. It can be revealed that GCSE keeps almost constant along with merely acceptable random bias at a negligible 10^{-5} magnitude. It shows the fact that the LSTM network can present accurate predictions of the system's future status which is described by MSR, given the current and certain historical measurements. This result indicates an excellent performance of the SA model on status perception of the test system in a noisy data environment.

3.2 Application in contingency detection

The first application of the enhanced SA model lies in detecting contingencies. In this application the NETS-NYPS is assumed to suffer from various contingency events such as earth faults, line breaks, wind farm disconnections and load losses. The first scenario is a single persistent line break at the branch between Bus-16 and Bus-17, which occurs at 40.3 s. By applying the



a

b

Fig. 5 *Detection of a single persistent line break*

(a) Degeneration of the MSR, ***(b)*** Performance of the SA model

Table 1 Arrangement of the sequential contingencies scenario in the presence of data corruptions

Contingencies			
No.	Event	Spot	Time, s
1	earth fault	Bus-43	80.1–80.2
2	wind farm offline	W3	280.1–280.3
3	load loss	Bus-8	480.1–481.0
		Data corruptions	
No.	Type	PMU no.	Details
1	data loss	37,45,65	lost first 1 s data in every 10 s
2	time delay	41,66	delayed by 2 s entirely
3	replay attack	6,7,11,54	replayed first 10 s data

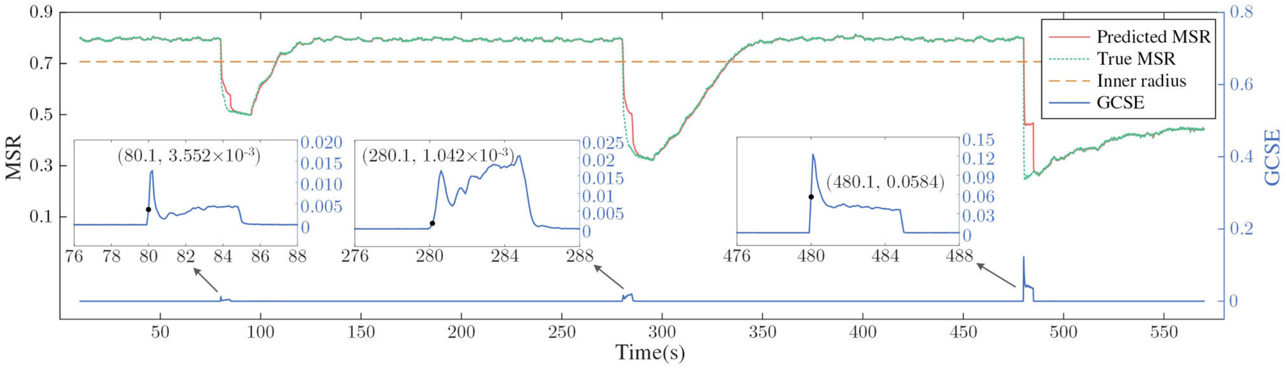


Fig. 6 *Detection of the sequential contingencies in the presence of data corruptions*

proposed SA model, the detection results are illustrated in Fig. 5. Fig. 5*a* shows the intuitive degeneration of MSR in accordance with the single ring theorem. One can find that the single ring theorem holds, i.e. the MSR and nearly all eigenvalues of the normalised product matrix are constrained by the single ring, before the contingency took place. However, right after the line break, the MSR and most of the eigenvalues collapse into the inner radius and the single ring constraint is broken. Furthermore, the MSR and those eigenvalues keep inside the inner radius and the single ring constraint no longer holds far after the contingency, which indicates a sustained insecure (unstable) state (i.e. voltage collapse or pole slips) of the test system.

It can be seen from Fig. 5*b* that the GCSE shoots up instantaneously right after the line break at 40.3 s, and then reaches a peak at next moment at 40.4s. This shows the model's ability to detect line break contingency in real time based on the perceptual indicator GCSE. It is also observed that the predicted values can tightly track the true values of MSR at most of of other moments, maintaining GCSE at around zero. This indicates an accurate prediction performance of the SA model, even in some post-contingency dynamics.

Next a more complicated scenario is arranged to extend this application. In this scenario a chain of transient contingencies take place sequentially, meanwhile PMU measurements are obtained in the presence of data corruptions. The events chain of the contingencies as well as a series of data corruptions are configured according to Table 1. From the detection results shown in Fig. 6, it is found that all three contingencies can be detected based on GCSE in real time, even though the measurement data are corrupted to a certain extent. This is a distinct verification of the model's robustness in the presence of data corruptions.

3.3 Application in wind power output variation perception

On top of contingencies, variations or fluctuations of wind power output can also potentially hazard the system's security. Therefore, the perception of variant wind power output should be another crucial application of the enhanced SA model. In this application,

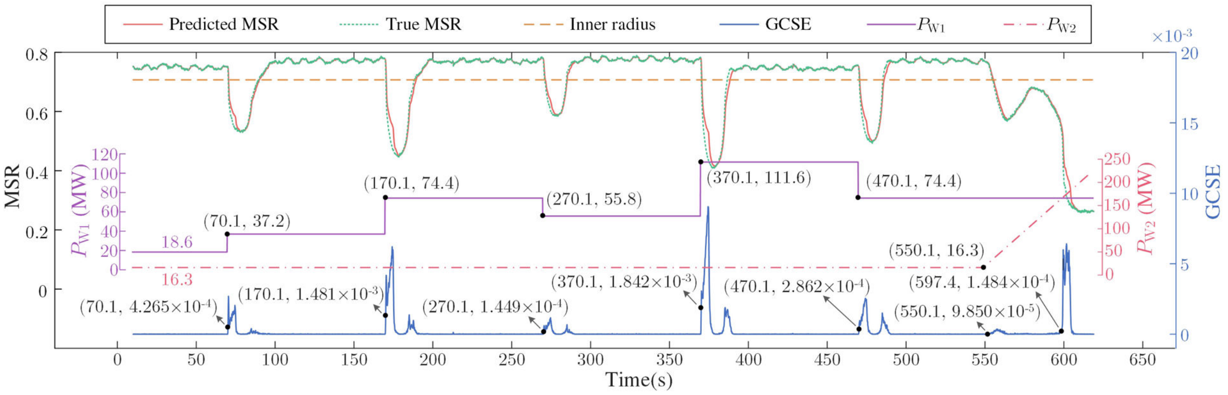


Fig. 7 *Perception of the wind power output variation*

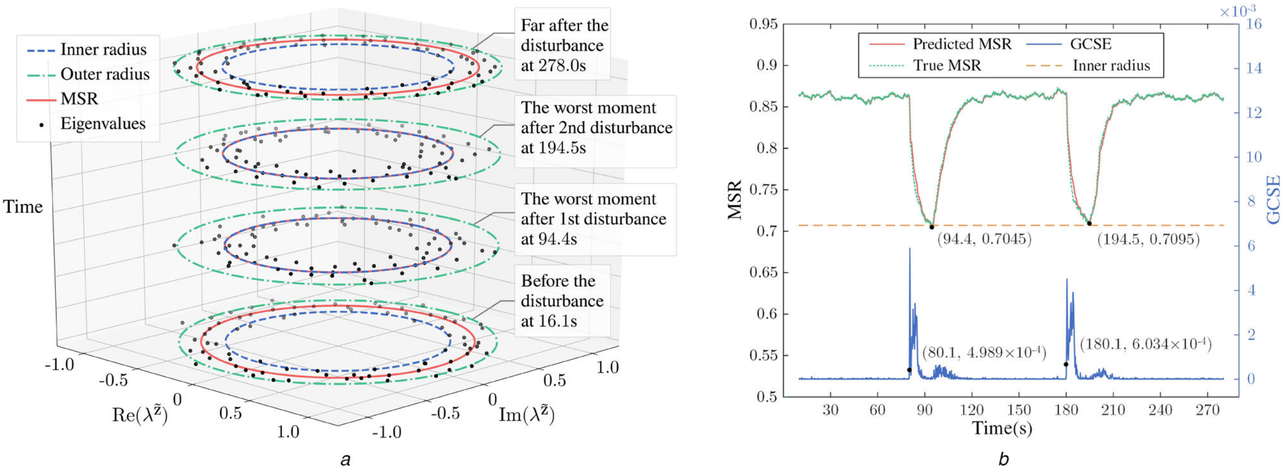


Fig. 8 *Awareness of the small disturbances*
(a) Degeneration of the MSR, ***(b)*** Performance of the SA model

the model is tested under a scenario including both a series of step fluctuations and a progressively linear increase of the wind power output. The former is a rough reflection of the stochastic wind power output behaviour, while the latter approximately simulates the switch-in process of wind farms. As shown in Fig. 7, the active power output of W1 (which is denoted as P_{W1}) has experienced several jumps or drops in a step manner at 70.1, 170.1, 270.1, 370.1 and 470.1 s, followed by a monotonically increasing active power output of W2 (which is denoted as P_{W2}) starting from 550.1 s.

On the other hand, the presence of data corruption is also arranged in this scenario. Firstly, comparing with the sequential contingencies scenario, a more serious case of data loss and time delay is present as: the measurements from PMUs at Bus-14, 17 (nearest to W1) have lost first 2 s data in every 10 s; the measurements from PMUs at Bus-31, 38 (nearest to W3) have delayed by 3 s entirely. Moreover, it is assumed that the attacker has had full access of the PMUs at Bus-19, 56, 57 (nearest to W2) and launched attacks in the following two stages:

- *First attack*: A false anomaly injection from 210.1 to 410.1 s, to deceive the system by a false contingency.
- *Second attack*: A replay attack starting at 520.1 s, replacing anomalous data with a period of pre-recorded normal data, to mask the power output increase of W2.

For an intuitive view, the perception results are plotted in Fig. 7, together with the wind power output variation exhibition under the same time axis. It can be discovered that the SA model is able to perceive every step variation of wind power output of W1, despite data loss and time delay in presence. Furthermore, the progressively linear increase of wind power output of W2 can be also perceived no matter whether neighbouring PMUs are subjected to replay attacks. In this case two successive climbs of GCSE are observed as: the slight one labelling at 550.1 s indicates the starting point of the wind power output increase, and the steep one labelling at 597.4 s is actually an evidence of the system's insecure (unstable) state from then. This is another proof of the SA model's perceptual performance, to raise timely and accurate early warnings on forthcoming insecure state of the system. In addition, the approximate plateaus of GCSE at both 210.1 s and 410.1 s shows that the model has successfully overcome the deception by false anomaly injection.

3.4 Application in small-disturbance awareness

Although only marginal magnitudes are involved, a particular type of anomalies known as small disturbance may also play a dominant role to jeopardise the dynamic stability of the high renewable-penetrated system. Moreover, such signals of small disturbances are prone to be concealed in the noisy and data-corrupted environment. Accordingly, the enhanced SA model is also expected to apply its perceptual ability in small-disturbance awareness. Hence, a scenario that contains two disturbances under data attacks is designed as follows:

- *First disturbance*: On wind farm W3 from 80.1 to 82 s, with replay attacks launched nearby at Bus-31, 38 (by recording first 10 s data and replaying them constantly).
- *Second disturbance*: On load at inter-area nearby Bus-8 from 180.1 to 186 s, with replay attacks launched nearby at Bus-6, 7 (by recording first 10 s data and replaying them constantly).

Fig. 8 illustrates the test results of this scenario. Obviously, the model can recognise these two disturbances by two corresponding leaps of GCSE, even in the presence of data attacks, as shown in Fig. 8*b*. The closely tracked MSR (which keeps GCSE below a magnitude of 10^{-3}) is also a marked demonstration of the SA

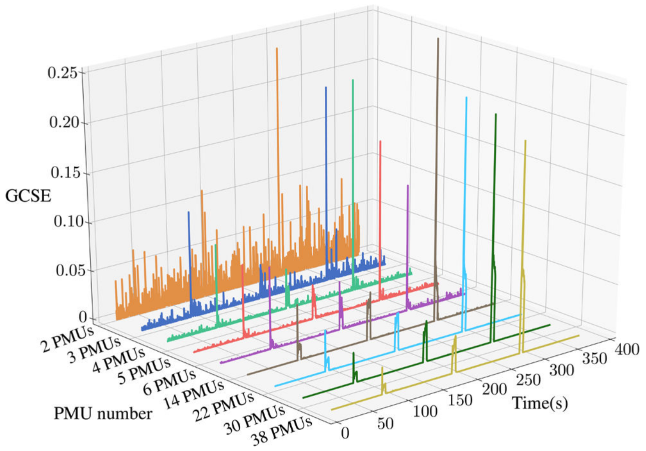


Fig. 9 *Perceptual performance on insufficient measurements*

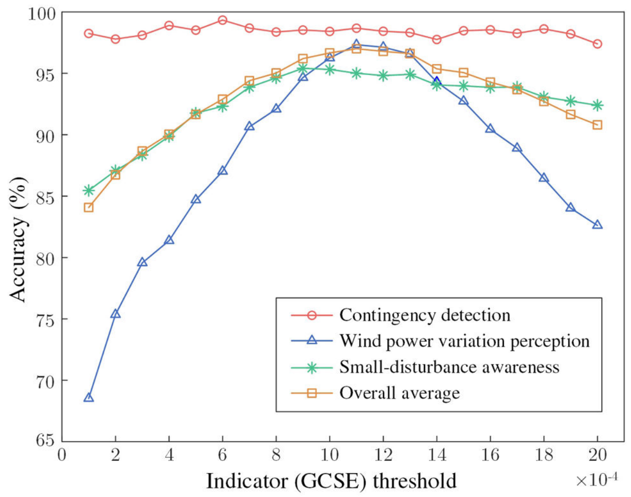


Fig. 10 *Influence of different indicator thresholds on the accuracy of the model*

model's prediction performance, even during the dynamic period after the disturbance. In addition, it is interesting to note that the MSR gets very close to the inner radius of the ring (almost coincides) at the worst moments of those two disturbances, which is exhibited in Fig. 8*a*. This is an indication of approaching the limit point of the system's stability and it can be used as an indicator for future study on asymptotic stability under small disturbances.

3.5 Performance on insufficient measurements

From the presence of above data corruptions with mild or moderate extents, the model still works well by utilising all accessible measurements (PMUs) even with bad data. However, in some worse cases when data corruptions are too critical to be handled any more, the system supposed to abandon the whole PMUs which have already been contaminated by those bad data. Besides, another negative case is the lack of measurements due to no installation, restricted access or denial of service attacks etc. These cases force the system run on insufficient measurements and thus the enhanced SA model should be tested under this scenario.

To show distinct results in this scenario, the same sequence of contingencies as given in Table 1 is arranged except for some shortened intervals (100 s rather than 200 s) between the occurrence of each event. In addition, all accessible PMUs in this scenario are arranged without any contamination of data corruptions. The number of PMUs is reduced by one at a time, based on a random selection criteria, from a initial number of 38. The test results over typical PMU numbers are illustrated in Fig. 9. One can find that there is almost no harm on the model's perceptual performance during incipient reductions of PMU number from 38 to 6. Threats begin to arise when PMU number continues to reduce from 6. However, a certain perceptual ability is still maintained by the model, until it is nearly lost on two PMUs merely. These results show the robustness of the SA model considering insufficient measurements or incomplete data sets. By choosing the appropriate PMU placement, it is feasible to achieve sufficient SA which relies on the minimum size of measurements in power systems. This inspires future study on an extensive application of GCSE as the data adequacy indicator.

3.6 Analysis on the indicator threshold

Different thresholds of the GCSE indicator create different criteria in the applications of real-time anomaly detection, leading to different levels of accuracy of the enhanced SA model. A low threshold can make confusion between anomalies and normal fluctuations by data corruptions (e.g. those minor jumps after first major ones in Fig. 7 or 8*b*), which may cause misjudgement. Alternately, a high threshold is probably out of the range of anomalies and hence incurs missing detection. Therefore, an appropriately selected indicator threshold is crucial to ensure high accuracy of the SA model. This subsection analyses the impact of the indicator threshold on the model's accuracy based on Monte Carlo simulation.

The Monte Carlo simulation is implemented to generate random operating points of the test system, including stochastic load conditions, wind power outputs, anomalies and data corruptions. More specifically, the active power load of each bus is assumed to be uniformly distributed within an interval $[0.75, 1.25]$ of the base value, and the reactive power load is determined by the corresponding active power load by multiplying a power factor which follows a uniform distribution from $[0.25, 0.55]$. For the stochastic wind power outputs, we add a forecast error which follows a normal distribution with zero mean and a standard deviation of 0.05. Three previously mentioned scenarios, i.e. contingency detection (in Section 3.2), wind power variation perception (in Section 3.3) and small-disturbance awareness (in Section 3.4), are reused in the analysis. All the anomalies (including contingencies, wind power output variations and small-disturbances) are also configured randomly in both temporal and spatial aspects, with the similar extent as described in Sections 3.2–3.4

By changing the range of indicator threshold from 1×10^{-4} to 2×10^{-3}, the model's accuracy on the above three scenarios as well as the overall average accuracy are analysed. Fig. 10 illustrates the analysis results based on 10^4 times Monte Carlo simulation. The accuracy reflects the model's ability in both correctly detecting the anomalies and successfully avoiding misjudgement by data corruptions. It is observed that the model can reach the highest accuracy with the threshold chosen as 1.1×10^{-3}, for both wind power variation perception and the overall average. For small-disturbance awareness, a plateau is reached after 9×10^{-4} of threshold and only slightly drops afterwards. For contingency detection, the accuracy almost remains constant with the changing thresholds. Consequently, it is plausible to choose 1.1×10^{-3} as the most appropriate indicator threshold for the enhanced SA model.

3.7 Comparative study

In order to validate the superiority of the enhanced SA model, a comparative study is carried out in this subsection. The same Monte Carlo simulation as in Section 3.6 is implemented to generate random operating points of the test system. Then the accuracy of the proposed model is investigated and compared with other four benchmarks in the literature: pure LSTM [19], pure random matrix (RM) [21], *k*NN [18] and DT [16].

After 10^4 times Monte Carlo simulation, the accuracy comparison results are listed in Table 2. The results show a distinct superiority of the proposed SA model over the other four benchmarks in all three scenarios. Without the aggregation, the robustness of either pure LSTM or pure RM against data corruptions is greatly reduced. As a result, neither of them can reach a satisfactory accuracy. Furthermore, neither pure LSTM nor pure RM is applicable in small-disturbance awareness due to a

Table 2 Accuracy comparison with other models

Model	Accuracy		
	Contingency detection, %	Wind power variation perception	Small-disturbance awareness
proposed model	98.68	97.33%	95.41%
pure LSTM	87.32	83.78%	×
pure RM	91.59	87.40%	×
*k*NN	74.11	×	×
DT	62.95	×	×

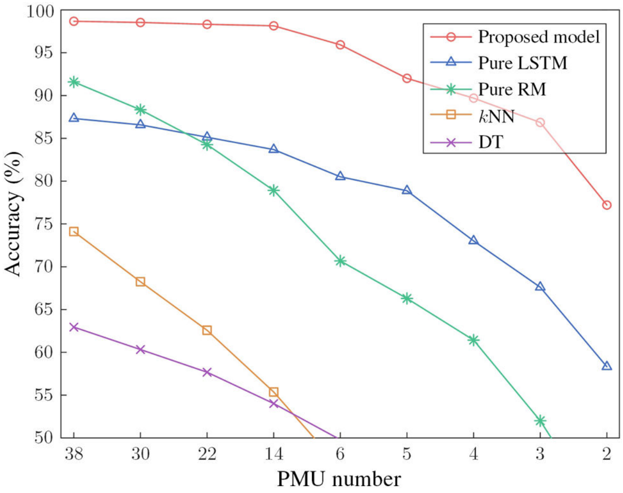


Fig. 11 *Model comparison under insufficient measurement*

Table 3 Security status under typical scenarios of power systems with different wind power penetration levels

Penetration level, %	Scenario 1	Scenario 2	Scenario 3	Scenario 4
0	secure	secure	secure	secure
30	secure	secure	secure	secure
50	secure	secure	insecure	secure
70	secure	insecure	insecure	secure
90	insecure	insecure	insecure	secure

missing appropriate indicator. This just validates that GCSE is a powerful indicator for the proposed SA model. For conventional machine learning models like *k*NN and DT, lower levels of accuracy are observed in contingency detection, and they even cannot be used for wind power variation perception. This is a proof that these conventional machine learning models are not applicable under such high renewable-penetrated and data-corrupted operating environment.

Another comparative study is implemented to investigate and compare the accuracy of these models under insufficient measurement. The same 10^4 times Monte Carlo simulation is executed and the contingencies are also configured randomly. The reduction of PMU number is as similar as Section 3.5. Fig. 11 shows the comparative results on the accuracy of the proposed model and the other four models, with a decreasing PMU number. One can find that the proposed SA model consistently outperforms other models even if only two PMUs are available. The pure LSTM model shows a similar downward trend but with lower levels of accuracy, while the pure RM model experiences a plunge in accuracy with the decreasing PMU number. The *k*NN and DT models show much lower levels of accuracy which even drop below 50% with six or less PMUs. These results also validate the superiority and robustness of the proposed SA model over other benchmark models, especially under insufficient measurement conditions.

3.8 Security check on different renewable penetration levels

Power systems in different countries or regions may have significant diversity in the penetration level of renewable energy. It is imperative to investigate the SA model's ability to check the security status of power systems with different renewable penetration levels. In this case, the same NETS-NYPS test system is studied except for a series of different penetration levels of wind power configured. The system is tested starting from no wind power integrated (0%) to a very high wind penetration level as much as 90%. Almost the same typical scenarios in the previous sections of case study, with just slight adjustments, are reused in this case. In order to make a clear exhibition, these scenarios are listed as follows.

- *Scenario 1*: The same scenario where wind power output performs step fluctuations, as arranged in Section 3.3.
- *Scenario 2*: Almost the same scenario where wind power output performs a progressively linear climb, as arranged in Section 3.3, except that the climbing time is shortened to 10 s.
- *Scenario 3*: The same scenario of sequential contingencies in Section 3.2, as shown in Table 1.
- *Scenario 4*: The same scenario of small disturbance as configured in Section 3.4.

It should be noted that any variation value of wind power output (i.e. scenarios 1 and 2) does not change with the wind penetration level in these scenarios. The security status of the system under each of these scenarios is checked by the degeneration ring plot of the predicted MSR, and the results are demonstrated in Table 3. It is observed that a higher wind power penetration level leads to a greater insecure risk of the system, undergoing the first three scenarios. More serious anomalies (from scenario 1 to scenario 3) are more likely to jeopardise the system security with the rise of penetration level. Moreover, the horizontal comparison among these four scenarios shows the fact that scenario 3 (i.e. contingencies) is more harmful to the system's security than scenarios 1 and 2 (i.e. variations of renewable output). In the field operation, more efforts should be made to avoid such contingencies which have worse impacts on the transient stability margin of the system. In addition, it can be also found that the system maintains a secure status regardless of the penetration levels in scenario 4. This is because the power flow of the system remains the same and the full-converter wind turbines are decoupled from the power grid by power electronics devices, the dynamics of which do not have a major impact on small-disturbance stability of the systems.

The results of the security check on different renewable penetration levels indicate a promising field applications of the SA model, in both the planning and operation stages. The security margin of the system is explicit by giving the maximum acceptable penetration levels, for example 30% in Table 3, which ensures the exact secure status of the system from the typical anomalies. This is helpful to design appropriate proportion of renewable and conventional energy sources in the planning stage. On the other hand, the system operators are working towards a better mastery of the system tolerance when the growing renewable energy switched in. Based on the security check of the SA model, the system operators can implement targeted dispatching control, to hedge the system from any possible insecure risks of those critical anomalies, in the operation stage.

4 Conclusion

In this paper, an enhanced version of SA has been proposed to provide panoramic perception for high renewable-penetrated power systems with multiple data corruptions. By applying a novel aggregation of random matrix and LSTM network, an enhanced SA model is developed. Owing to the newly defined perceptual indicator, the model's high accuracy and alertness have been illustrated in the application of real-time anomaly detection, which outperforms many existing benchmarks in the literature. Furthermore, a dedicated workflow is designed to mitigate the impact of data corruptions from two stages. As a result, the SA model has been verified with salient robustness against multiple complex data corruptions. In addition, a fast security check on different renewable penetration levels has been realised by the enhanced SA to explicitly indicate the security margin of the system.

The proposed enhanced SA can reinforce the system operators' observability on any suspicious variation, and hedge the system operators against potential data manipulations or cyber attacks. It will not only help to assign appropriate renewable proportion in the planning stage, but also reveal the system tolerance for the system operators in the operation stage. Accordingly, the system operators can make accurate dispatching decisions and implement appropriate recovery controls opportunely and promptly, in order to ensure a secure, stable and smooth operation, for the increasingly decarbonised and digitised power systems.

5 Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under grant 51807171, in part by the Sichuan Science and Technology Program under grant 2018RZ0075, in part by the Hong Kong Research Grant Council for the Research Project under grants 25203917, 15200418 and in part by the Hong Kong Polytechnic University for the Start-up Fund Research Project under grant 1-ZE68. The authors would like to sincerely appreciate for the attentions, comments and suggestions from the editors and anonymous reviewers.

6 References

[1] Lin, Z., Wen, F., Ding, Y., *et al.*: 'WAMS-based coherency detection for situational awareness in power systems with renewables', *IEEE Trans. Power Syst.*, 2018, **33**, (5), pp. 5410–5426

[2] NGESO: 'Technical Report on the Events of 9 August 2019', National Grid ESO, 2019

[3] NCCIC/ICS.CERT: 'Cyber-attack against Ukrainian critical infrastructure'. Available at https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01, 2016

[4] IEEESpectrum: 'Unplugging from digital controls to safeguard power grids'. Available at https://spectrum.ieee.org/energywise/energy/the-smarter-grid/unplugging -digital-networks-to-safeguard-power-grids, 2019

[5] Sodhi, R., Sharieff, M.I.: 'Phasor measurement unit placement framework for enhanced wide-area situational awareness', *IET Gener. Transm. Distrib.*, 2015, **9**, (2), pp. 172–182

[6] Panteli, M., Kirschen, D.S.: 'Situation awareness in power systems: theory, challenges and applications', *Electr. Power Syst. Res.*, 2015, **122**, (1), pp. 140–151

[7] Panteli, M., Crossley, P.A., Kirschen, D.S., *et al.*: 'Assessing the impact of insufficient situation awareness on power system operation', *IEEE Trans. Power Syst.*, 2013, **28**, (3), pp. 2967–2977

[8] He, X., Chu, L., Qiu, R.C., *et al.*: 'A novel data-driven situation awareness approach for future grids-using large random matrices for big data modeling', *IEEE Access*, 2018, **6**, pp. 13855–13865

[9] Vellaithurai, C., Srivastava, A., Zonouz, S., *et al.*: 'CPIndex: cyber-physical vulnerability assessment for power-grid infrastructures', *IEEE Trans. Smart Grid*, 2015, **6**, (2), pp. 566–575

[10] Eissa, M.: 'Challenges and novel solution for wide-area protection due to renewable sources integration into smart grid: an extensive review', *IET Renew. Power Gener.*, 2018, **12**, (16), pp. 1843–1853

[11] Morshedizadeh, M., Kordestani, M., Carriveau, R., *et al.*: 'Power production prediction of wind turbines using a fusion of MLP and ANFIS networks', *IET Renew. Power Gener.*, 2018, **12**, (9), pp. 1025–1033

[12] Lackner, C., Wilches Bernal, F., Pierre, B.J., *et al.*: 'A tool to characterize delays and packet losses in power systems with synchrophasor data', *IEEE Power Energy Technol. Syst. J.*, 2018, **5**, (4), pp. 117–128

[13] Khalid, H.M., Peng, J.C.H.: 'A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks', *IEEE Trans. Smart Grid*, 2016, **7**, (4), pp. 2026–2037

[14] Pasqualetti, F., Dörfler, F., Bullo, F.: 'Attack detection and identification in cyber-physical systems', *IEEE Trans. Autom. Control*, 2013, **58**, (11), pp. 2715–2729

[15] He, M., Vittal, V., Zhang, J.: 'Online dynamic security assessment with missing PMU measurements: a data mining approach', *IEEE Trans. Power Syst.*, 2013, **28**, (2), pp. 1969–1977

[16] Ma, J., Makarov, Y.V., Diao, R., *et al.*: 'The characteristic ellipsoid methodology and its application in power systems', *IEEE Trans. Power Syst.*, 2012, **27**, (4), pp. 2206–2214

[17] Guo, T., Milanovic, J.V.: 'Online identification of power system dynamic signature using PMU measurements and data mining', *IEEE Trans. Power Syst.*, 2016, **31**, (3), pp. 1760–1768

[18] Cai, L., Thornhill, N.F., Kuenzel, S., *et al.*: 'Real-time detection of power system disturbances based on *k*-nearest neighbor analysis', *IEEE Access*, 2017, **5**, pp. 5631–5639

[19] Zhang, S., Wang, Y., Liu, M., *et al.*: 'Data-based line trip fault prediction in power systems using LSTM networks and SVM', *IEEE Access*, 2017, **6**, pp. 7675–7686

[20] Ospina, J., Newaz, A., Faruque, M.O.: 'Forecasting of PV plant output using hybrid wavelet-based LSTM-DNN structure model', *IET Renew. Power Gener.*, 2019, **13**, (7), pp. 1087–1095

[21] He, X., Ai, Q., Qiu, R.C., *et al.*: 'A big data architecture design for smart grids based on random matrix theory', *IEEE Trans. Smart Grid*, 2017, **8**, (2), pp. 674–686

[22] Chan, T.: 'The wigner semi-circle law and eigenvalues of matrix-valued diffusions', *Probab. Theory Relat. Fields*, 1992, **93**, (2), pp. 249–272

[23] Lytova, A., Pastur, L.: 'Central limit theorem for linear eigenvalue statistics of random matrices with independent entries', *Ann. Probab.*, 2009, **37**, (5), pp. 1778–1840

[24] Hochreiter, S., Schmidhuber, J.: 'Long short-term memory', *Neural Comput.*, 1997, **9**, (8), pp. 1735–1780

[25] Greff, K., Srivastava, R.K., Koutník, J., *et al.*: 'LSTM: a search space odyssey', *IEEE Trans. Neural Netw. Learn Syst.*, 2017, **28**, (10), pp. 2222–2232

[26] Pascanu, R., Mikolov, T., Bengio, Y: 'On the difficulty of training recurrent neural networks'. Int. Conf. on Machine Learning, Atlanta, GA, USA, 2013, pp. 1310–1318

[27] Gers, F.A., Schmidhuber, J: 'Recurrent nets that time and count'. Proc. of the IEEE-INNS-ENNS Int. Joint Conf. on Neural Networks (IJCNN 2000) Neural Computing: New Challenges and Perspectives for the New Millennium, Como, Italy, 2000, pp. 189–194

[28] Rogers, G.: '*Power system oscillations*' (Springer Science & Business Media, New York City, NY, USA, 2000)

[29] Peppanen, J., Alquthami, T., Molina, D., *et al.*: 'Optimal PMU placement with binary PSO'. 2012 IEEE Energy Conversion Congress and Exposition (ECCE), Raleigh, NC, USA, 2012, pp. 1475–1482

[30] Kingma, D.P., Ba, J: 'ADAM: a method for stochastic optimization'. The 3rd Int. Conf. for Learning Representations, San Diego, CA, USA, 2015, pp. 1–15