Sustainable Energy, Grids and Networks 34 (2023) 101009

Contents lists available at ScienceDirect

Sustainable Energy, Grids and Networks

journal homepage: www.elsevier.com/locate/segan

Wide area monitoring system operations in modern power grids: A median regression function-based state estimation approach towards cyber attacks

Haris M. Khalid [a,b,c], Farid Flitti [a], Magdi S. Mahmoud [d], Mutaz M. Hamdan [e], S.M. Muyeen [f,*], Zhao Yang Dong [g]

[a] Department of Electrical and Electronics Engineering, Higher Colleges of Technology 7947, United Arab Emirates
[b] Department of Electrical and Electronic Engineering Science, University of Johannesburg, Auckland Park 2006, South Africa
[c] Department of Electrical Engineering, University of Santiago, Avenida Libertador, 3363, Santiago, RM, Chile
[d] Control and Instrumentation Engineering Department, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia
[e] Department of Mechanical Engineering, National University College of Technology, Amman, 11592, Jordan
[f] Department of Electrical Engineering, Qatar University 2713, Doha, Qatar
[g] School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore

ARTICLE INFO

Article history:
Received 6 December 2021
Received in revised form 3 January 2023
Accepted 14 January 2023
Available online 23 January 2023

Keywords:
Bad-data injection attacks
Cyber–physical systems
Cyber security
Dynamic vulnerability assessments (DVA)
Exogenous
Generation mix
Median filter
Model prediction
Phasor measurement unit (PMU)
Regression
Renewable energy integration (REI)
Situational awareness
State estimation
Synchrophasor
Variable renewable energy resources (VRES)
Wide area monitoring system (WAMS)

ABSTRACT

Modern power grid is a generation mix of conventional generation facilities and variable renewable energy resources (VRES). The complexity of such a power grid with generation mix has routed the utilization of infrastructures involving phasor measurement units (PMUs). This is to have access to real-time grid information. However, the traffic of digital information and communication is potentially vulnerable to data-injection and cyber attacks. To address this issue, a median regression function (MRF)-based state estimation is presented in this paper. The algorithm was stationed at each monitoring node using interacting multiple model (IMM)-based fusion architecture. An exogenous variable-driven representation of the state is considered for the system. A mapping function-based initial regression analysis is made to depict the margins of state estimate in the presence of data-injection. A median regression function is built on top of it while generating and evaluating the residuals. The tests were conducted on a revisited New England 39-Bus system with large scale photovoltaic (PV) power plant. The system was affected with multiple system disturbances and severe data-injection attacks. The results show the effectiveness of the proposed MRF method against the mainstream and regression methods. The proposed scheme can accurately estimate the states and evaluate the contaminated measurements while improving the situation awareness of wide area monitoring systems (WAMS) operations in modern power grids

1. Introduction

1.1. Power grids – A complex network

Power grids represent a complex interconnected network of generating stations, electrical substations, high voltage distribution lines, and loads. This is due to: (1) an increase in demand of power, and (2) an interface to renewable energy integration (REI). These factors promote to expand the grid size. This would eventually result to increase the distribution and network which further increases the dimensionality of information. As the dimensionality increases, the number of model parameters increase which require a higher number of manpower to monitor the power flow. Due to this complexity of information and structure, modern power grids could possibly deploy phasor measurements units (PMUs) and wide-area monitoring systems (WAMS) to better manage these resources and have more access towards the observability of the power system [1–4].

[*] Corresponding author.
E-mail addresses: harism.khalid@ieee.org (H.M. Khalid), fflitti@hct.ac.ae (F. Flitti), magdisadekmahmoud@gmail.com (M.S. Mahmoud), mutaz.hamdan82@gmail.com (M.M. Hamdan), sm.muyeen@qu.edu.qa (S.M. Muyeen), zy.dong@ntu.edu.sg (Z.Y. Dong).

https://doi.org/10.1016/j.segan.2023.101009

Nomenclature

Notations: In this paper, notations are represented according to a structure. $\mathbf{E}_{\mu_{1/2}}$ is the median-based expectation operator. The notation $\tilde{\ }$ denotes the estimate error, e.g. $\tilde{\mathcal{P}}$ is the estimate error of $\mathcal{P}$. A hat $\hat{\ }$ over a variable expresses an estimate, e.g. $\hat{\mathcal{P}}$ is an estimate of $\mathcal{P}$. The individual entries of a variable like $\mathcal{P}$ are denoted by $\mathcal{P}(.)$. Note when these variables are represented as function of time. Here the time index t appears as a subscript e.g. $\mathcal{P}_t$. The notation $\mathcal{P}_0^T$ represents the time-sequence (e.g. $\mathcal{P}_0$, $\mathcal{P}_1$, …., $\mathcal{P}_T$).

Acronyms

ABB	ASEA Brown Boveri
BAT	bagged trees
BOT	boosted trees
DSE	dynamic state estimation
DVA	dynamic vulnerability assessment
EnKF	ensemble Kalman filter
GP	Gaussian Processes
GPS	global positioning system
IMM	interacting multiple model
IP	internet protocol
KF	Kalman filter
LR	linear regression
MRF	median regression function
MSE	mean square error
NN	neural network
PCC	point of common coupling
PDC	phasor data concentrator
PF	particle filter
PMU	phasor measurement unit
PV	photovoltaic
SSE	static state estimation
REI	renewable energy integration
SVM	support vector machine
TCP	transmission control protocol
UKF	unscented Kalman filter
VRES	variable renewable energy resources
VSC	voltage source converter
WAMS	wide area monitoring system

Symbols

$\mathcal{P}$	power grid state
$\mathcal{P}_0$	initial condition of frequency oscillation state transition model
t	time-instant
$\mathcal{U},\mathcal{V},...,\mathcal{Z}$	PMU nodes
n	state vector size
$\mathbf{R}$	subspace
r	size of noise transition matrix
ε	exogenous variable
G	noise transition matrix
$p(G)$	probability vector
w	random process noise
$\mathcal{Y}$	observation output
m	number of observations
$\mathcal{H}$	observation matrix
v	observation noise
$d(a)$	function of attack vector
p, q	instants
R	covariance matrix
δ	Kronecker delta function
Q	process noise correlation factor
$f(\mathcal{P}_\varepsilon)$	non-linear mapping function
$g(.), h(.)$	non-linear vector functions
$\mathcal{C}$	set size of $\mathcal{A}$
ξ^+	positive mapping variable
ξ^-	negative mapping variable
ζ	distance from actual value
$\mathcal{T}$	actual value
α	mapping variable
A, B	random variables
$f(a)$	probability mass function
Θ	vector of all involved parameters
$\mathbf{E}_{\mu_{1/2}}$	median-based expectation operator
Ω	possible realization of $\mathcal{P}$
$b\mathcal{P}$	realization of observation matrix
J	positive energy function
γ	positive parameter
e_{res}	error matrix
$\mathcal{F}$	modal matrix of exogenous function
R_e	covariance of observation noise
ξ, ξ_f	fault-injection dependent parameters.
$\mathcal{N}$	zero-mean multivariate normal distribution
ρ	positive definite matrix minimize variable
Γ_{stat}	cross-spectral density function
S	cross-spectral density of data-injection free parameters
S_f	cross-spectral density of data-injected parameters
η_{th}	computed threshold value

1.2. WAMS and focus of this work

WAMS readily managed the high interconnectivity, measurement of physical quantities on the grid and their interdependency by data acquisition technology of PMUs through its applications [5–13]. The optimal installation of PMUs from the perspective of location could provide additional features of visibility and monitoring towards situational awareness, where they can extract information about frequency quantities like phase angles and magnitudes. This information is synchronized after an allocated sampling time with global positioning system (GPS). The phasor data concentrator (PDC) is somehow a central hub where all this information is gathered, thereby status of regional variations and instabilities can be monitored and detected. This is followed by an adequate and timely action to enhance the regulation of power flow. However, this whole modern network of timely monitoring with rigorous transfer of information and communication is dependent on the communication network. At some occasions, this communication network bridges with the commercial internet providers for an integrated network. The internet protocol suite, Transmission Control Protocol and the Internet Protocol (TCP/IP) which communicates between networks and devices is prone and vulnerable to deliberate injections and actions. This could raise concerns on the power grid infrastructure and security protocols [14–21]. Tales of such a breach are: (1) 2015 Ukranian power grid attack [22], and (2) cluster of attacks reported by ASEA Brown Boveri (ABB) [23,24], which exposed the tenderness of WAMS and its applications towards networking technology and world wide web. The focus of this paper is towards the cyber-security of network-based digital infrastructure of WAMS applications.

1.3. State estimation and main motivation of this work

Among the significant growth of WAMS applications, a mature and widely used function installed by the power transmission utilities is state estimation [9–13]. This is because of the variable behavior of modern power grids, which do operate on system-level in three possible states. These are (1) normal, (2) emergency, and restorative states [25]. Normal state of a power system defines that all the system state variables are operating within their operating limits. A violation of these operating limits could lead to situations of vulnerability. This vulnerability could generate instability and make the power grid prone to intrusion. When such contingencies take place, the state is considered to be an emergency state. Power system can be brought from an emergency state to a normal state. The transient phase of such a power system where control procedures and actions are employed to reinstate the system to its original normal state is called as the restorative state. The system in this state requires restoration to the initial state while being balanced and operating with no system violations. Apart from system-level classification, state estimation is further divided into two basic paradigms of: (1) static state estimation (SSE), and (2) dynamic state estimation (DSE) methods [26]. The prominent ones are the conventional, distributed, and sequential forms of state estimation [27,28]. All these methods have to match the fast digital dynamics of PMUs. This is to capture the smallest of the variations happening in the whole network, which could be due to the rise of generation and load demands. However, a accurate execution of state estimation in such situations becomes challenging while capturing the full stretch of dynamics, which is the main motivation of this paper.

1.4. DSE methods, cyber attacks, and need for new scheme

The DSE methods have been dominated by recursive techniques built on *a–priori* knowledge. The most widely used are based on Kalman filter (KF) framework. This also involves the variants techniques of KF, such as: (1) the unscented KF (UKF), (2) robust H-infinity UKF, (3) the ensemble KF (EnKF), and (4) the particle filter (PF) [10–13]. The non-recursive forms of estimators can also be adopted for the state as well as parameter estimation. These could be the infinite impulse and finite versions of impulse response filter, etc. [29]. From the perspective of cyber attacks, cases of KF have also been discussed in situations with bad-data injection attacks [30–35]. However, with the expansion of modern power grids with REI and its awareness to the hackers, the adversary can model the attack vector as well as make a sensible choice on site of the attack. This can lead to more devastating impacts while affecting the safety and consumer economy. To the best of author's knowledge, such a situation has not been investigated in power systems dynamic state estimation, where these variations and deviations could be modeled as an exogenous variable to boost the state estimation approach towards cyber attacks and its variants. A negligence to detect these variations by system-level identification tools could result in amplifying the surged instabilities of a modern power grid.

1.5. Main contribution of this work

The main contribution of this paper is towards the state estimation enhancement of the WAMS applications with REI in the presence of data-injection attacks. This is achieved by proposing a signal processing-based solution involving dynamic state estimation approach. A novel median regression function-based dynamic state estimation method is derived for estimating the contaminated frequency oscillations. The aim is to maintain the accuracy of state estimation while identifying and detecting the deliberately injected variations. In order to accurately estimate such dynamic states, it is assumed that the hacker can access the whole network of PMUs which are deployed as an integral units of WAMS operation. The mapping function-based initial regression analysis also helped to depict the margins of state estimation in the presence of injections. This would allow to propose a post-contingency step to analyze associated risks and impacts towards dynamic vulnerability assessments (DVA). These assessments are interfaced to coordinate for corrective control actions in cyber security situational awareness. The effectiveness of the proposed scheme was measured by the comparative analysis against mainstream technique and regression methods.

1.6. Formation of the remaining paper

The remaining work in this paper is organized as follows. Section 2 expresses the problem formulation of power grid under attack. Section 3 illustrates the methodology and derivation of the proposed scheme made on median regression function. Section 4 describes pseudo code for the proposed scheme implementation. In Section 5, the validation is made using implementation and evaluation of the proposed approach. Finally, the conclusion and future work is drawn in Section 6.

2. Problem formulation: Power grid under attack

The problem formulation of a power grid infected with attack is acquired in this section. An assumption is made that attacker could have accessed the digital information of sensor-nodes of the power grid. An overview of the formulation can be seen in Fig. 1. Consider a modern power grid with $\mathcal{X}$ number sensor nodes are deployed on the PMUs for the digital information. The problem formulation begins with the state representation of a power grid in (1). This is followed by its observation model in (2). The correlation of noise is defined in (3)–(6). The exogenous function is expressed in (7)–(9). The attack vector is stated in (10)–(11).

2.1. State representation of a power grid

A state of power grid $\mathcal{P}_t$ is represented as:

$$\mathcal{P}^{\mathcal{X}}_{t+1} = f(\mathcal{P}^{\mathcal{X}}_{\varepsilon,t}) + G^{\mathcal{X}}_t w^{\mathcal{X}}_t \tag{1}$$

where $\mathcal{P}^{\mathcal{X}}_0 \in \mathbf{R}^{n\times 1}$ represents an initial condition of frequency oscillation state transition model at time-instant t, such that $t = 1, 2, \ldots\ldots, T$ with $\mathcal{X} = [\mathcal{P}^{\mathcal{U}}_t, \mathcal{P}^{\mathcal{V}}_t, \ldots \mathcal{P}^{\mathcal{Z}}_t]$. Here $\mathcal{U}$, $\mathcal{V}$, ..., $\mathcal{Z}$ represent the PMU nodes in the plant. The superscript n represents the state vector size in subspace $\mathbf{R}$. The subscript ε represents the exogenous variable. $G^{\mathcal{X}}_t \in \mathbf{R}^{r\times r}$ is the noise transition matrix. The superscript r represents the size of the noise transition matrix. It is the probability vector $p(G_{k,t})$ such that $\sum_{k=1}^{n} p(G_{k,t}) = 1$. In this probability vector, each individual component shall have the following properties:

- *Property 1:* It is a non-negative real number,
- *Property 2:* It must have a probability between 0 and 1, such that $0 \leq |p(G_{k,t})| \leq 1$,

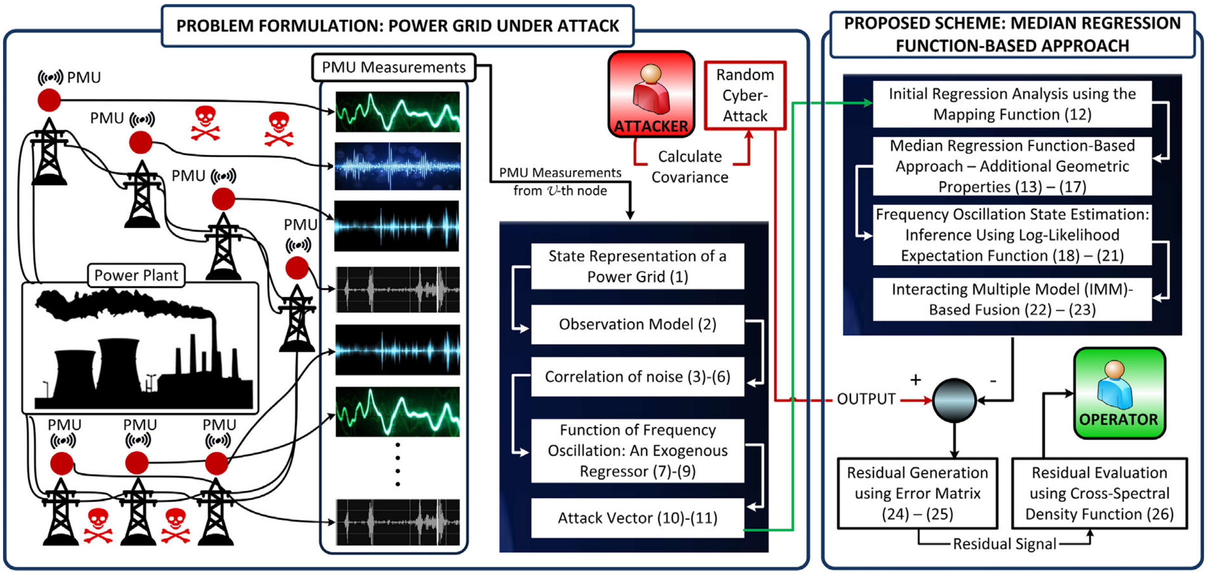
PROBLEM FORMULATION: POWER GRID UNDER ATTACK
PMU
PMU
PMU
PMU
PMU Measurements
Power Plant
PMU
PMU
PMU
PMU Measurements from $\mathcal{U}$-th node
ATTACKER
Random Cyber-Attack
Calculate Covariance
State Representation of a Power Grid (1)
Observation Model (2)
Correlation of noise (3)-(6)
Function of Frequency Oscillation: An Exogenous Regressor (7)-(9)
Attack Vector (10)-(11)
PROPOSED SCHEME: MEDIAN REGRESSION FUNCTION-BASED APPROACH
Initial Regression Analysis using the Mapping Function (12)
Median Regression Function-Based Approach – Additional Geometric Properties (13) – (17)
Frequency Oscillation State Estimation: Inference Using Log-Likelihood Expectation Function (18) – (21)
Interacting Multiple Model (IMM)-Based Fusion (22) – (23)
OUTPUT
+
-
OPERATOR
Residual Generation using Error Matrix (24) – (25)
Residual Evaluation using Cross-Spectral Density Function (26)
Residual Signal

Fig. 1. Formulation framework of the proposed scheme.

- *Property 3:* It has sum of all numbers equal to 1.

Also, $w_t^{\mathcal{X}} \in \mathbf{R}^r$ is the random process noise.

Once the state representation is made, the observation model is stated.

2.2. Observation model

Let the observation model for the oscillation state expressed in (1). It can be stated at time-instant t as:

$$\mathcal{Y}_t^{\mathcal{U}} = \mathcal{H}_t^{\mathcal{U}} \mathcal{P}_t^{\mathcal{X}} + d(a_t)\mathcal{P}_t^{\mathcal{X}} + v_t^{\mathcal{U}} \tag{2}$$

where $\mathcal{Y}_t^{\mathcal{U}} \in \mathbf{R}^{m\times 1}$ denotes the observation output of frequency oscillation state, m defines the number of observations made simultaneously by $\mathcal{U}$ PMUs at time-instant t. $\mathcal{H}_t^{\mathcal{U}} \in \mathbf{R}^{m\times r}$ and $v_t^{\mathcal{X}} \in \mathbf{R}^m$ are the observation matrix and the observation noise respectively. $d(a_t) \in \mathbf{R}^{\bar{o}\times 1}$ is the function of attack vector. Here the superscript $\bar{o}$ belongs to the set $\mathcal{A} \subseteq \{1, 2, \dots .\bar{o}\}$.

Once the observation model is formulated, the correlation between process noise and observation model is defined.

2.3. Correlation of noise

The noises w_t and v_t are initially uncorrelated. Moreover, they are zero-median white Gaussian such that:

$$\mathbf{E}_{\mu_{1/2}}[w_t] = \mathbf{E}_{\mu_{1/2}}[v_t] = 0, \ \forall\, t, \tag{3}$$

Also,

$$\mathbf{E}_{\mu_{1/2}}[w_p v_q'] = 0 \tag{4}$$

Here (4) is defined for two instants p and q. Also,

$$\mathbf{E}_{\mu_{1/2}}[w_p w_q'] = R_t \delta_{pq} \tag{5}$$

where noise processes are considered to be serially uncorrelated. Also, they have zero-mean, a finite variance process with constant value. Note the variable R_t denotes the covariance matrix. δ_{pq} is a Kronecker delta function. This function is deployed for shifting the integer variable after the presence or absence of noise. Similarly,

$$\mathbf{E}_{\mu_{1/2}}[v_p v_q'] = Q_t \delta_{pq} \tag{6}$$

with Q_t is the process noise correlation factor.

Once the correlation of noises are defined, function of oscillation state is modeled.

2.4. Function of frequency oscillation state: An exogenous regressor

The function of frequency oscillation state is represented in the oscillation state model. It is represented as an exogenous regressor variable, such that $f(\mathcal{P}_{\varepsilon,t}^{\mathcal{X}}) \in \mathbf{R}^r$. $f(\mathcal{P}_{\varepsilon,t}^{\mathcal{X}})$ represents a non-linear mapping function, such that: $\mathbf{E}_{\mu_{1/2}}\left[f(\mathcal{P}_{\varepsilon,t}^{\mathcal{X}})|\mathcal{P}_{t+1}^{\mathcal{X}}\right] = 0$.

Let $f(\mathcal{P}, \mathcal{Y}, \varepsilon) = g(\mathcal{P}, \varepsilon) - h(\mathcal{P}, \mathcal{Y})$. Here $g(.)$ and $h(.)$ are the non-linear vector functions. The exogenous property satisfies:

$$f(\mathcal{P}_{\varepsilon,t}^{\mathcal{X}}) = \arg \max_{\mathcal{P}_{\varepsilon,t}^{\mathcal{X}} \in \{0,1\}} \mathbf{E}_{\mu_{1/2}}[f(\mathcal{P}, \mathcal{Y}, \varepsilon)|\mathcal{H}, \mathcal{Y}] \tag{7}$$

$$= \arg \max_{\mathcal{P}_{\varepsilon,t}^{\mathcal{X}} \in \{0,1\}} \left[\mathbf{E}_{\mu_{1/2}}[g(\mathcal{P}, \varepsilon)|\mathcal{H}, \mathcal{Y}] - h(\mathcal{P}, \mathcal{Y})\right] \tag{8}$$

$$= \begin{cases} 1 & \text{if } \mathbf{E}_{\mu_{1/2}}[g(\mathcal{P}, \varepsilon)|\mathcal{H}, \mathcal{Y}] - h(1, \mathcal{Y}) \geq \\ & \mathbf{E}_{\mu_{1/2}}[g(0, \varepsilon)|\mathcal{H}, \mathcal{Y}] - h(0, \mathcal{Y}) \\ 0 & \text{, Otherwise} \end{cases} \tag{9}$$

Once the exogenous function of oscillation state is modeled on extracted measurements, the generalized form of an attack vector is defined.

2.5. Attack vector – A generalized form

A generalized form[1] of an attack vector is defined by the hacker as a pathway to access or penetrate the target system. In the observation model (2), the attack vector function is represented as $d(a_t) \in \mathbf{R}^{\bar{o}\times 1}$. The superscript $\bar{o}$ belongs to the set $\mathcal{A} \subseteq \{1, 2, \dots .\bar{o}\}$. It contains PMU sensor-nodes installed in the plant which are infected with attack. The attack vector is thus expressed for any $\mathcal{U}$th and $\mathcal{V}$th sensor-node as:

$$d(a_t^{\mathcal{U}\mathcal{V}}) = 0 \tag{10}$$

where $\mathcal{U} \in \mathcal{A}^{\mathcal{C}}$, and $\mathcal{V} \geq 0$. Here the superscript $\mathcal{C}$ denotes the set size of $\mathcal{A}$, such that:

$$\mathcal{A}^{\mathcal{C}} = \frac{S}{\mathcal{A}} \tag{11}$$

[1] Note a generalized form an attack is assumed here in the form of vector. The occurrence of cyber attacks, data-injections, and security breach in industry could be in various forms and types, such as scalar values, vectors, matrices, arrays, packets, nested loops, etc.

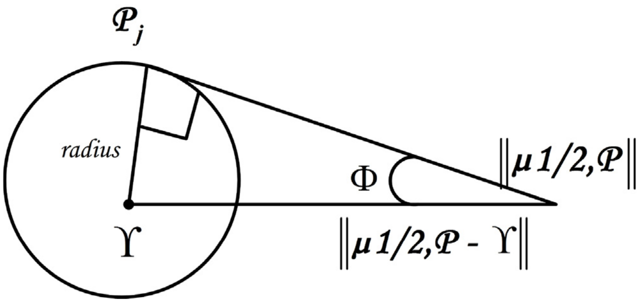
$\mathcal{P}_j$
radius
Φ
Υ
$\|\mu 1/2,\mathcal{P}\|$
$\|\mu 1/2,\mathcal{P} - \Upsilon\|$

Fig. 2. Median gradient-based convergence diagram.

$\sup(a_t^{\mathcal{V}}) \subseteq \mathcal{A}$ for all $\mathcal{V} \geq 0$. Here the function $d(a_t)$ itself represents the stochastic nonlinearity, such that: $\mathbf{E}\big[d(a_t)|\mathcal{P}_t^x\big] = 0$, also $\mathbf{E}\big[d(a_t^x)d'(a_t^{\mathcal{U}})\big] = 0$, $\mathcal{U} \neq \mathcal{V}$. '′' denotes here the transpose operator.

Once the modeling of attack vector is made on the measurements extract, the proposed scheme is represented.

3. Proposed scheme: Median regression function-based approach

The proposed scheme is built on the problem formulation. An overview of the framework can be viewed in Fig. 1. The initial regression analysis is expressed in (12). The additional geometric properties of median regression function-based approach is made in (13)–(17). The log-likelihood expectation function-based state estimation is derived in (18)–(21). The IMM-based fusion is represented in (22)–(23). The generation of residual and threshold based evaluation of residual is determined at (24)–(25) and (26) respectively.

3.1. Initial regression analysis using the mapping function

The initial regression analysis towards the data-injection attacks can be achieved by demonstrating a mapping function. This mapping function is defined here by determining a mapping function for predicting the initial observation. It can be expressed as:

$$\begin{aligned}\mathcal{M}(\mathcal{P}_{\varepsilon,t})={}&\mathcal{C}\sum_{k=1}^{\mathcal{M}}(\xi_k^+ + \xi_k^-)+\frac{1}{2}\|w\|^2-\sum_{k=1}^{\mathcal{M}}(\mu_k^+\xi_k^+ + \mu_k^-\xi_k^-)\\ &-\sum_{k=1}^{\mathcal{M}}\alpha_k^+(\zeta+\xi_k^+ + y_k-\mathcal{T}_k)-\sum_{k=1}^{\mathcal{M}}\alpha_k^-(\zeta+\xi_k^+ - y_k+\mathcal{T}_k)\end{aligned} \tag{12}$$

where $\mathcal{C}$ is the variable controlling the trade-off between the variables defined for mapping and size of the margin, ξ_k^+ and ξ_k^- are positive and negative mapping variables, w is normal to the mapping, $\mu \geq 0$, ζ is the distance from the actual value, $\mathcal{T}$ is the actual value, and α is the mapping variable.

Once the initial regression analysis using the mapping function is made, the additional properties of median regression function-based approach is defined.

3.2. Median regression function-based approach — additional geometric properties

The median regression function-based approach is built on the update the probability for a hypothesis on the available information. This requires some additional properties to derive the median-based expectation operator. These properties can be built on [36]. Some additional properties are defined as follows.

Property 1. *Let A and B be two random variables. The variables have a Gaussian distribution. If* $A, B \in \mathbf{R}^n$, *then* $\lim_{A\to B} \mathbf{E}_{\mu_{1/2}}[|A-B|^2] = 0$.

$$\begin{aligned}p\big(A, B \leq \mu_{1/2}\big) &= p\big(A, B \geq \mu_{1/2}\big)\\ &= \mathbf{E}_{\mu_{1/2}}\big[(A)^2+(B)^2-2(A)(B)\big]\\ &= \Big(\sum_{-\infty}^{\mu_{1/2}} af(a)\Big)^2+\Big(\sum_{-\infty}^{\mu_{1/2}} bf(b)\Big)^2\end{aligned} \tag{13}$$

where $f(a)$ is the probability mass function of A. It further simplifies as:

$$\begin{aligned}p\big(A, B \leq \mu_{1/2}\big) &= -2\Big(\sum_{-\infty}^{\mu_{1/2}} af(a)\Big)\Big(\sum_{-\infty}^{\mu_{1/2}} bf(b)\Big)\\ &= \Big(\frac{1}{2}\Big)^2+\Big(\frac{1}{2}\Big)^2-2\Big(\frac{1}{2}\Big)\Big(\frac{1}{2}\Big)=0\end{aligned} \tag{14}$$

Note for A, B, the whole process is called a median-square continuous such that for all $A, B \in \mathbf{R}^n$.

Property 2. *A Gaussian process-based function f is said to be median-based differentiable on* $\mathbf{R}^r$. *This is possible if for every sequence* $\{A_n\}$ *for* $i = 1, \ldots., n$ *converges* $\|A_n - A\| \to 0$.

Considering the gradient property in [36] and as shown in Fig. 2, let $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \ldots.., \mathcal{P}_n \in H$. Also $\Upsilon \in H$. $\|\mu_{1/2} - \Upsilon\| > \Phi radius$, and $\gamma > 0$. A derivative is considered to be obtained in the direction of $\Upsilon - \mu_{1/2}$ for $\dot{f}(A_n)$, such that:

$$\partial f(\mu_{1/2,n,\Upsilon}-\mu_{1/2,n})=\lim_{t\to 0}\frac{f(\mu_{1/2,n}+t(\Upsilon-\mu_{1/2,n}))-f(\mu_{1/2,n})}{t} \tag{15}$$

Similarly for the derivative in the direction of $\Upsilon - \mu_{1/2}$ for $\dot{f}(X)$ gives:

$$\partial f(\mu_{1/2,\Upsilon}-\mu_{1/2})=\lim_{t\to 0}\frac{f(\mu_{1/2}+t(\Upsilon-\mu_{1/2}))-f(\mu_{1/2})}{t} \tag{16}$$

$\mu_{1/2}$ is designed to minimize the function f. This employs that:

$$\partial f(\mu_{1/2,n,\Upsilon}-\mu_{1/2,n}),\ \partial f(\mu_{1/2,\Upsilon}-\mu_{1/2}) \geq 0 \tag{17}$$

Based on (15)–(17), $\mathbf{E}_{\mu_{1/2}}[(\dot{f}_i(A_n)-\dot{f}_i(A))^2] = 0$ holds.

Note the additional properties remain the same for symmetric error distributions as well. Once the additional geometric properties are defined, the variations are further derived. This is a challenging task because of the following: (1) deriving a median regression function-based property, and its structural transformation from a conventionally utilized tool for data analysis, forecasting and computer vision to an inference system where updates are generated using probability for a hypothesis on the available information, (2) derivation of the regression structure. Here a median-based expectation is considered over the classic weighted average-based expectation.

3.3. Frequency oscillation state estimation: Inference using log-likelihood expectation function

The frequency oscillation state estimation is made by using the inference system which is calculated and built by the log-likelihood function. This is to get an estimate of the latent variations of the oscillation state as:

$$\begin{aligned}\mathcal{L}(\Theta)&=\log p\big(\mathcal{P}_t^x, f(\mathcal{P}_{\varepsilon,t}^x)\big)\\ &= \mathbf{E}_{\mu_{1/2},\mathcal{H}_t|\mathcal{P}'_{0,t},\mathcal{Y}_t}\log p\big(\mathcal{P}_t^x, f(\mathcal{P}_{\varepsilon,t}^x)\big)\\ &+ \mathbf{E}_{\mu_{1/2}}\log p\big(f(\mathcal{P}_{\varepsilon,t}^x)|\mathcal{P}_t^x\big)\end{aligned} \tag{18}$$

where Θ is the vector of all involved parameters.

The computation of the $\mathcal{L}$ derivatives with respect to each of the parameters is stated as:

$$
\begin{aligned}
\frac{\partial \mathcal{L}(\Theta)}{\partial \Theta_{\mathcal{P}_t^x, f(\mathcal{P}_{\varepsilon,t}^x)}} &= \arg\max_{\mathcal{P}_t} \mathbf{E}_{\mu_{1/2}, \mathcal{H}_t | \mathcal{P}'_{0,t}, \mathcal{Y}_t} \log p(\mathcal{Y}_t, \mathcal{H}_t | \mathcal{P}_t) p(\mathcal{P}_t) \\
&\quad + \arg\min_{\mathcal{P}_t^{var}} \left(\mathcal{P}_{t-1}^{var} - \mu_{1,2.t-1} \right) \\
&= \arg\max_{\mathcal{P}_t} \mathbf{E}_{\mu_{1/2}, \mathcal{H}_t | \mathcal{P}_{0,t}^T, \mathcal{Y}_t} \sum_{\mathcal{H}_t \in \Omega} \left(\mathcal{Y}_t \log b_t \mathcal{P}_t^x \right) \\
&\quad - \gamma J(\mathcal{P}_t) + \arg\min_{\mathcal{P}_t^{var}} (\mathcal{P}_{t-1}^{var} - \mu_{1/2}, t-1) \\
&= \arg\min_{\mathcal{P}_t} \sum_{\mathcal{H}_t \in \Omega} b_t \mathcal{P}_t^x - \mathbf{E}_{\mu_{1/2}, \mathcal{H}_t | \mathcal{P}'_{0,t}, \mathcal{Y}_t} \mathcal{H}_t \log b_t \mathcal{P}_t^x \\
&\quad + \gamma J(\mathcal{P}_t^x) + \arg\min_{\mathcal{P}_t^{var}} (\mathcal{P}_{t-1}^{var} - \mu_{1/2,t-1}) \qquad (19)
\end{aligned}
$$

where $\mathbf{E}_{\mu_{1/2}}$ is the median-based expectation operator, Ω denotes the possible realization of $\mathcal{P}_t^x$. The realization of the observation matrix $\mathcal{H}_t^x$ is denoted by $b_t \mathcal{P}_t^x$. J is a positive energy function and γ is a positive parameter.

Taking the difference between (1) and (19) gives the covariance matrix, such that $\mathcal{P}_t^x - \hat{\mathcal{P}}_{t|t-1}^x = P_{t|t-1}^x$. It is presented as:

$$
\begin{aligned}
P_{t|t-1}^x &= f(\mathcal{P}_{\varepsilon,t}^x) + G_t^x w_t^x - \arg\min_{P_t^x} \sum_{\mathcal{H}_t^x \in \Omega} (b_t \mathcal{P}_t^x) \\
&\quad + \mathbf{E}_{\mu_{1/2}, \mathcal{H}_t | \mathcal{P}_{0,t}^T, \mathcal{Y}_t} \mathcal{H}_t \log(b_t \mathcal{P}_t^x) - \gamma J(\mathcal{P}_t^x) \\
&\quad - \arg\min_{\mathcal{P}_t^{var}} \left(\mathcal{P}_{t-1}^{var} - \mu_{1/2,t-1} \right) \qquad (20)
\end{aligned}
$$

Further simplifying (20) gives:

$$
\begin{aligned}
P_{t|t-1}^x &= -\arg\min_{P_t^x} \sum_{\mathcal{H}_t^x \in \Omega} (b_t \mathcal{P}_t^x) + \mathbf{E}_{\mu_{1/2}, \mathcal{H}_t | \mathcal{P}'_{0,t}, \mathcal{Y}_t} \mathcal{H}_t \log(b_t \mathcal{P}_t^x) \\
&\quad - \gamma J(\mathcal{P}_t^x) - \arg\min_{\mathcal{P}_t^{var}} (\mathcal{P}_{t-1}^{var} - \mu_{1/2,t-1}) + G_t^x w_t^x \qquad (21)
\end{aligned}
$$

The state estimation and covariance matrix will now incorporate in information fusion architecture using the interacting multiple model (IMM) algorithm. Due to the property of state hypothesis of multiple models with time-varying dynamics, IMM is given preference on other fusion techniques.

3.4. Interacting multiple model (IMM)-based fusion

The processing of IMM-based fusion takes place by blending the information of estimated parameters from each installed sensor-node. The information extracted from $\mathcal{U}$th sensor-node $\mathcal{P}_t^{\mathcal{U}}$ is merged as:

$$
\hat{\mathcal{P}}_{t|t}^{\text{IMM}} = \sum_{\chi=\mathcal{U}}^{z} \text{Pr}_{\mathcal{U}\mathcal{V}}(\mathcal{P}_t^{\mathcal{U}}) \hat{\mathcal{P}}_{t|t}^{\mathcal{U}} \qquad (22)
$$

$$
cov_{t|t}^{\text{IMM}} = \sum_{\chi=\mathcal{U}}^{z} \text{Pr}_{\mathcal{U}\mathcal{V}}(\mathcal{P}_t^{\mathcal{U}})(cov_{t|t}^{\mathcal{U}} + [\hat{\mathcal{P}}_{t|t}^{\mathcal{U}} - \hat{\mathcal{P}}_{t|t}][\hat{\mathcal{P}}_{t|t}^{\mathcal{U}} - \hat{\mathcal{P}}_{t|t}]') \qquad (23)
$$

Here the superscript IMM denotes the variable processed based on IMM fusion. $\text{Pr}_{\mathcal{U}\mathcal{V}}$ is the probability of model to switch from sensor-node $\mathcal{P}_t^{\mathcal{U}}$ to $\mathcal{P}_t^{\mathcal{V}}$, given the probability of $\mathcal{P}_t^{\mathcal{U}}$ at time-instant t. Once the IMM-based fusion is made, this will determine the generation of residual.

3.5. Residual generation using error matrix

The generated residual is made here using the error matrix. The error matrix e_{res} is usually calculated to detect any: (1) unusual dynamic variations, (2) data-injections, (3) biased signatures, and (4) system-faults. For oscillation state, these variations can be detected as:

$$
\begin{aligned}
e_{\text{res},\mathcal{Y},t}^x &= \mathcal{H}_t^x e_{\mathcal{P},t+1}^x \mathcal{H}_t^x \left(\mathcal{F}_t^x - [\mathbf{E}_{\mu_{1/2}} \mathcal{P}_{t+1}^x (\mathcal{Y}_t^x - v_t)'] R_{e,t}^{-1} \mathcal{H}_t^x \right) \\
&\quad (\mathcal{P}_t^x - \hat{\mathcal{P}}_t^x) + \Xi [\xi_t f(\mathcal{Y}_t^x, \mathcal{P}_t^x) - \xi_{f,t} f(\mathcal{Y}_t^x, \mathcal{P}_t^x)] \qquad (24)
\end{aligned}
$$

where $\mathcal{F}_t^{c1} \in \mathbf{R}^{r \times r}$ is the modal matrix of the exogenous function, $R_{e,t}$ is the covariance of observation noise v_t. This covariance matrix has a zero-mean multivariate normal distribution $\mathcal{N}$ such that $R_{e,t}$: $v_t \sim \mathcal{N}(0, R_{e,t})$, $f(\mathcal{Y}_t^x . \mathcal{P}_t^x) \in \mathbf{R}^r$ is a non-linear vector function of $\mathcal{Y}_t^X$ and $\mathcal{P}_x$. Note $\xi_t, \xi_{f,t} \in \mathbf{R}$ are the fault-injection f-based change dependent parameters.

Note the generated residual is asymptotically convergent when the parameters show no change due to the fault injection. This is represented such that ξ_t, $\xi_{f,t}$, $\lim_{t\to\infty} e_{\text{res},\mathcal{Y},t}^x = 0$. Here the difference between residual generation and the estimated state can be represented by a Lyapunov variable $\mathcal{V}$. This is represented as:

$$
\begin{aligned}
\Delta \mathcal{V} &= \mathbf{E}_{\mu_{1/2}} \left[\mathcal{V}(e_{\mathcal{P},t+1} | e_{\mathcal{P},t}, \mathcal{P}_t^x - \hat{\mathcal{P}}_t^x) \right] \\
&\leq -e_{\text{res},\mathcal{Y},t}^x \aleph_t e_{\mathcal{P},t}^x + 2 \| e_{\text{res},\mathcal{Y},t}^x \| | R_{e,t} \xi_{f,t} | \mathcal{V} \| e_{\mathcal{P},t}^x \| \\
&\leq -\rho \| e_{\text{res},\mathcal{Y},t}^x \|^2 - \mathcal{V}(e_{\text{res},\mathcal{Y},t}^x) \\
&< 0 \qquad (25)
\end{aligned}
$$

Here ρ is defined to minimize the positive definite matrix $\aleph_t$.

Once the error matrix determines the residual, the evaluation of residual is made.

3.6. Residual evaluation using cross-spectral density function

The residual evaluation is determined using a threshold. This threshold determines the false data injection and unusual variations. This is achieved here using the cross-spectral density function using test statistic Γ_{stat}. This can be stated as:

$$
\Gamma_{\text{stat}} = f(S_t, S_{f,t}), \begin{cases} \leq \eta_{th} & noattack \\ > \eta_{th} & attack \end{cases} \qquad (26)
$$

where the cross-spectral density function can be stated as:

$$
f(S_t, S_{f,t}) = \frac{|S_t S_{f,t}|^2}{S_t^2 S_{f,t}^2} \qquad (27)
$$

Here S_t and $S_{f,t}$ are the cross-spectral densities of data-injection free and data-injected parameters respectively. η_{th} is a computed threshold value. The value of the computed threshold is chosen and determined to ensure a low false alarm probability. This is during the course of an accurate residual evaluation.

4. Pseudo code for proposed scheme implementation

The pseudo code of the implementation of proposed scheme is shown in Algorithm 1. Referring to the steps of the state representation of a power grid, observation model, correlation of noise, function of frequency oscillation state, initial regression analysis, Median regression function, frequency oscillation, interacting multiple model, error matrix, and cross-spectral density function. It can be observed that the implementation of the proposed scheme correspond to steps in Lines 12 to 23, 13 to 17, 18 to 22, and 24 to 27 respectively. The main motivation is to enhance the grid resilience by the proposed state estimation scheme. The objective here is to tackle the data-injection attacks and its effects on the neighboring nodes and following time windows. This is a challenging task as the proposed scheme utilizes a interacting multiple model architecture. The error matrix-based residual generation and cross spectra density function-based residual evaluation were utilized in the end of the proposed scheme to generate residual and isolate the injected fault and its effect.

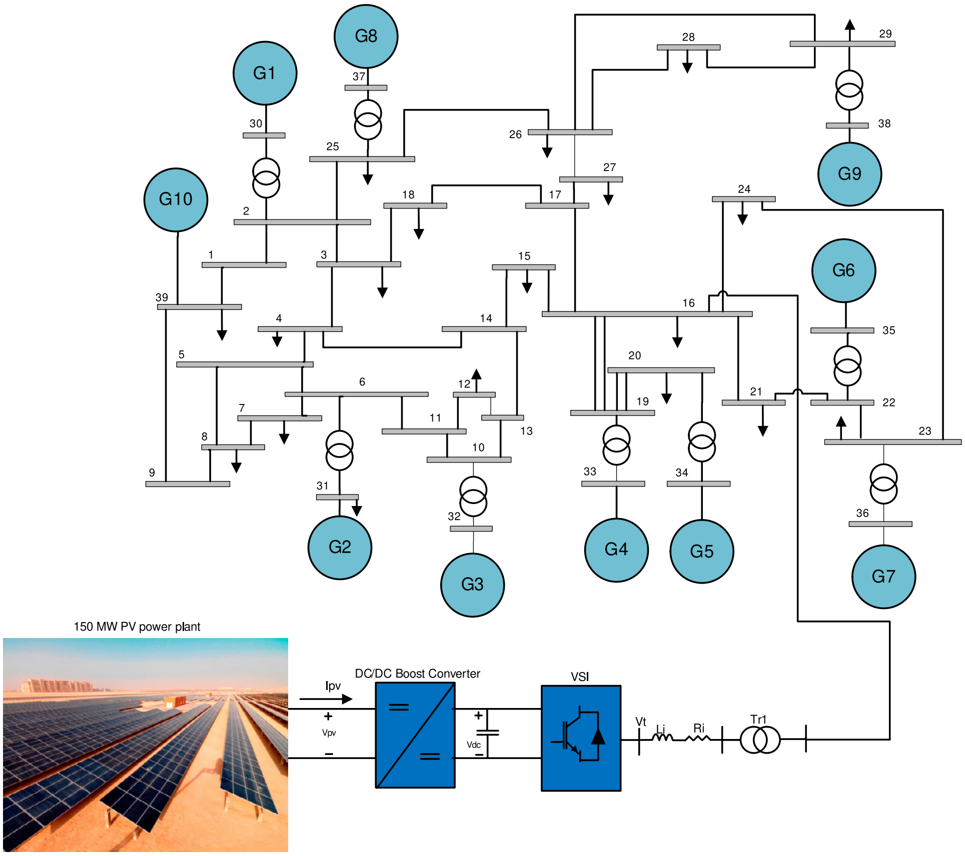

Fig. 3. Model of revised New-England 39-Bus system with large scale PV power plant.

Algorithm 1 Pseudo code for proposed scheme implementation

```
$N \rightarrow$ number of measurements
$SR \rightarrow$ state representation of power grid
$OM \rightarrow$ observation model
$CN \rightarrow$ correlation of noise
$FFOS \rightarrow$ function of frequency oscillation state
$IRA \rightarrow$ initial regression analysis
$MRF \rightarrow$ median regression function
$FO \rightarrow$ frequency oscillation
$IMM \rightarrow$ interacting multiple model
$EM \rightarrow$ error matrix
$CSDF \rightarrow$ cross-spectral density function
for $i$=1 to $T$//including IMM
    $\boldsymbol{SR}_i \leftarrow$ measurements ($\boldsymbol{N}_i$);
    $\boldsymbol{OM}_i \leftarrow$measurements ($\boldsymbol{SR}_i$);
    $\boldsymbol{CN}_i \leftarrow$measurements($\boldsymbol{OM}_i$);
    $\boldsymbol{FFOS}_i \leftarrow$measurements ($\boldsymbol{CN}_i$);
end for
for $i$=1 to $N$
    $\boldsymbol{IRA}_i \leftarrow$measurements($\boldsymbol{FFOS}_i$);
    $\boldsymbol{MRF}_i \leftarrow$measurements ($\boldsymbol{IRA}_i$);
    $\boldsymbol{FO}_i \leftarrow$measurements ($\boldsymbol{MRF}_i$);
end for
end for
for $i$=1 to $N$
    $\boldsymbol{EM}_i \leftarrow$Residual-Generation($\boldsymbol{IMM} - \boldsymbol{OUTPUT}_i$);
    $\boldsymbol{CSDF}_i \leftarrow$Residual-Evaluation($\boldsymbol{EM}_i$);
end for
```

5. Implementation and evaluation of the proposed scheme

5.1. Validation system and modeling details

The proposed scheme is validated on the simulated synchrophasor measurements. These measurements are collected from the revised New England, 39-Bus, 10-machines system with large scale PV power plant of 150 MW as shown in Fig. 3. Modeling details are based on [37,38]. Measurements are collected from generators G30, G35, G37, G38 and G39, loads 4, 15, and 29, Buses 16–18. Note the frequency mode of 0.69 Hz is an inter-area oscillation. All loads are subjected to random small magnitude fluctuations. These fluctuations are on continuous basis up to 10 MW/s. The DIgSILENT PowerFactory Ver. 15.1 was utilized for all the simulation performances [39]. From the collected measurements, the averaged oscillatory parameters were updated using the monitoring schemes every 5 s.

5.2. System disturbances

Over a period of 60 s, the system is excited by five large-signal disturbances as follows:

- *First Disturbance:* A three-phase-to-ground fault occurred at Bus 24 at 5 s. It was cleared after 0.1 s.
- *Second Disturbance:* Uncertainty of PV power generation due to changes in solar radiation. A ramp down in solar irradiance from 1000 W/m^2 to 200 W/m^2 at 25 s. A ramped up in solar irradiance from 200 W/m^2 to 1100 W/m^2 at 50 s.
- *Third Disturbance:* The active and reactive power demands load connected at Bus 21. These power demands of load are ramped up by 30% and 10% respectively over 10 s.

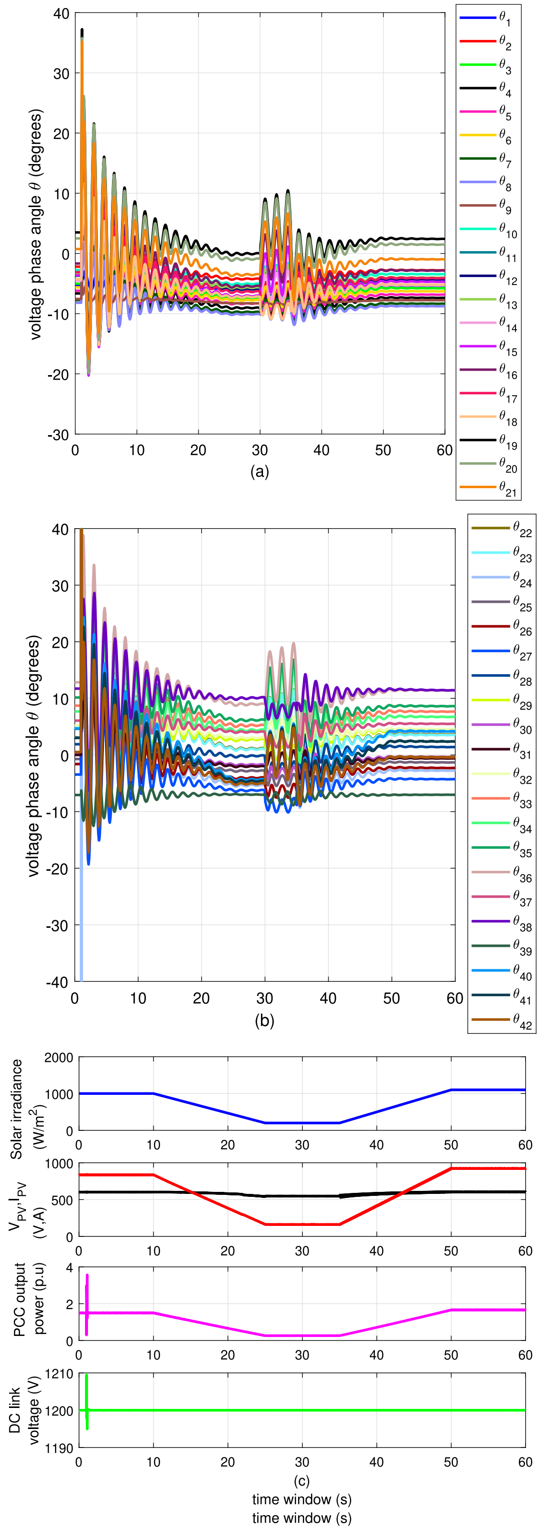

Fig. 4. Dynamic response of phase voltage angles to the: (a) prescribed disturbances ($\theta_1 - \theta 21$), (b) prescribed disturbances ($\theta_{22} - \theta 42$), and (c) PV power plant.

- *Fourth Disturbance:* Line connecting Bus 16 and 17 is disconnected at 25 s. This was reconnected after 5 s.
- *Fifth Disturbance:* The power demand loads (active and reactive) at Bus 4 are ramped up by 20% and 10%, respectively over 5 s.

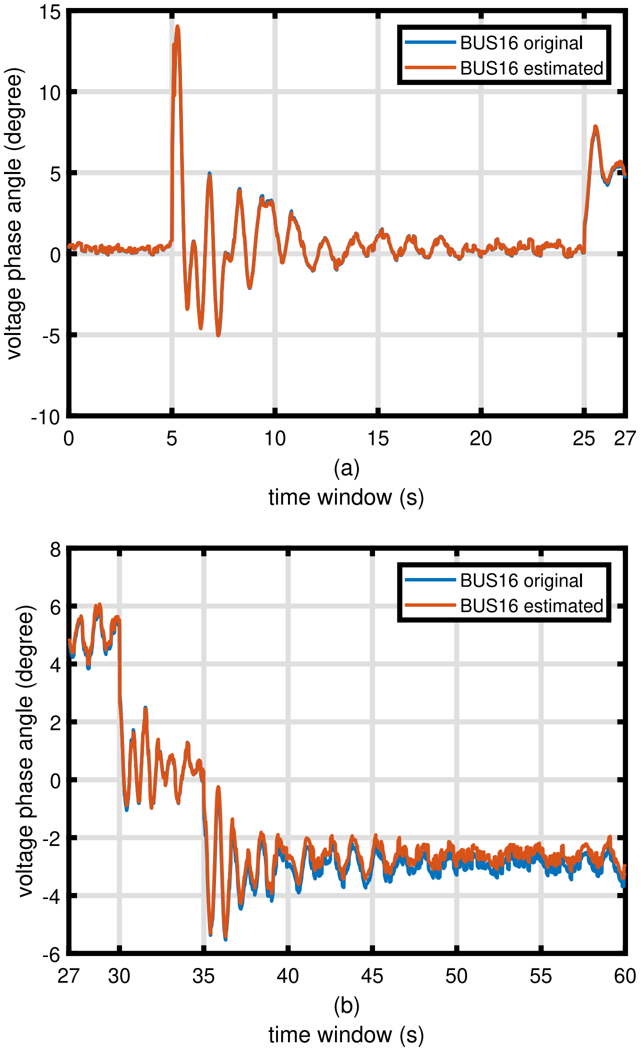

Fig. 5. Estimation performance of (a–b) Bus 16.

5.3. Performance metrics, dynamic response, and REI operation

(1) Performance Metrics for Evaluation: In this paper, the proposed scheme is evaluated using the following performance metrics: (1) estimation performance with no attack injection, (2) training and testing error no attack injection, (3) estimation performance with injection attacks, (4) residual evaluation with injection attacks, (5) mean square error (MSE)-based estimation comparative analysis. Note for MSE-driven comparative analysis, firstly, the evaluation of proposed scheme is made against the track fusion technique of [18]. Secondly, it is referenced comprehensively with other regression methods [40–42]: (1) linear regressions, (2) standard Gaussian processes, (3) support vector machine (SVM), (4) neural networks (NN), (5) regression trees, (6) boosted trees, and (7) bagged trees. Note the later are regression methods and are not originally designed to estimate the frequency oscillations in WAMS operations in the presence of data-injection attacks.

(2) Dynamic Response — Disturbances and PV Power Plant: Fig. 4(a)–(b) shows the dynamic response of the phasor voltage angles to the prescribed set of disturbances. In addition, Fig. 4(c) shows the dynamic response of the PV power plant. It is noticed that the output power at the point of common coupling (PCC) follows the variations of solar irradiance. Meanwhile, a constant DC

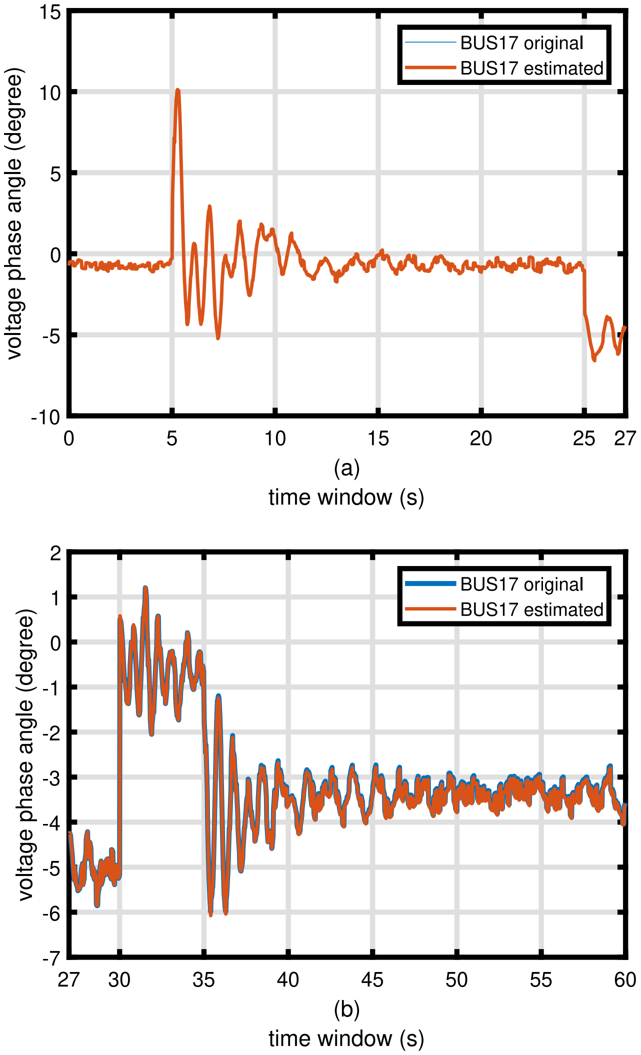

Fig. 6. Estimation performance of (a–b) Bus 17.

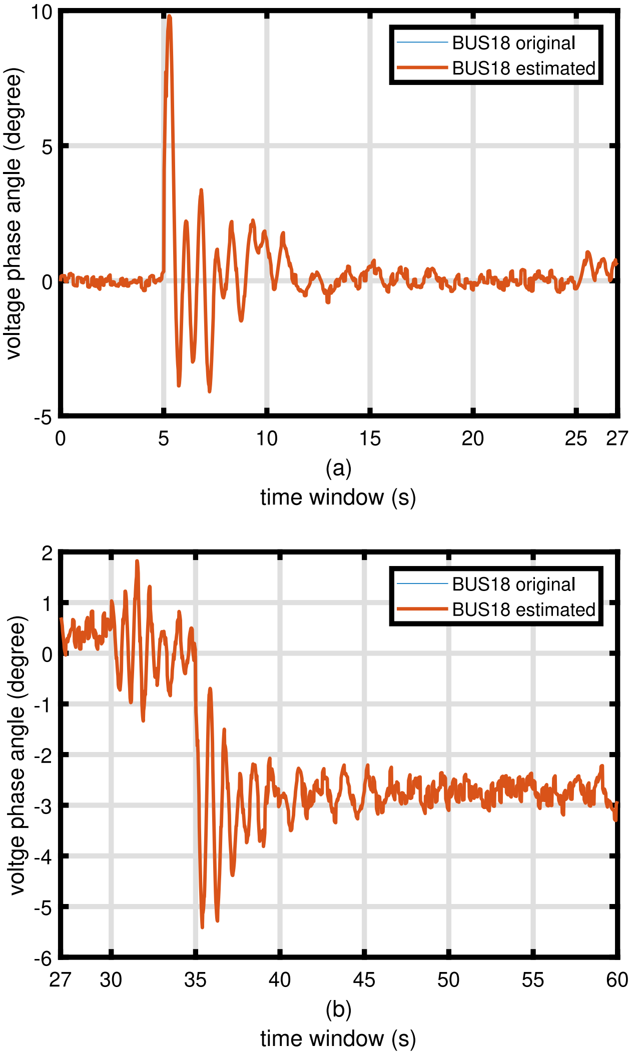

Fig. 7. Estimation performance of (a–b) Bus 18.

voltage is maintained across the DC link due to the employment of proper control of the voltage source converter (VSC).

(3) Renewable Energy Sources and Stable Operation: Renewable energy sources-based generators differ in operation from the conventional sources. This is because: (1) they cannot be scheduled due to their structure and power source, and (2) they are much smaller than conventional power stations. The current practice of utilizing the available renewable energy systems (PV and Wind) in electricity markets is just to reduce fossil-fuel consumption and carbon footprint. Due to the inherently variable and non-dispatchable nature of renewable energy sources, such as practice poses a threat to the power system integrity and requires utilities to maintain power balancing reserves to match supply and demand power levels. Maintaining these reserves for the uncertain renewable generation represents an additional cost for the utility, referred to as the short term balancing cost, which is mainly the cost of flexibility. Therefore, in this paper, the authors assumed that the renewable energy systems are balanced with an appropriate spinning reserve to ensure stable and secure operation of the transmission system. In addition, the access and control of the large scale renewable power plant can be realized at the PCC. It is due to this reason these renewable generators have the minimum involvement with test case integration. The uncertainty of RES power generation might have an impact which is worth investigation. The future studies and test cases will be aimed with direct involvement of renewable energy sources to provide local benefits to the power grid during peak demand while considering the intermittency of RES generation.

5.4. Injection attacks, hacker strategy, and data sets

(1) Attack Scenarios and Injections: To simulate the deliberate attack scenarios, the data-injections are made in the recorded synchrophasor measurements. To create a situation of regional attacks on measured data, the neighboring nature of nodes was considered (See Fig. 3). Simulated injection of attack scenarios at Bus 16–18 are as follows:

- *First Injection with High Energy Potency:* A high energy potency signal was injected at Bus 16 from 30.6 to 35 s.
- *Second Injection with Data-Repetition Attack:* A data-repetition attack of samples from Bus 17 at 10.2 s to 15 s was injected at the same bus from 30.2 s to 35 s.
- *Third Injection with Noise Attack:* A random noise attack at Bus 17 from 50 s to 55 s.
- *Fourth Injection with Coordinated Attack:* A coordinated attack at Bus 16 and 17 of random noise-like variations from 40 s to 45 s respectively.

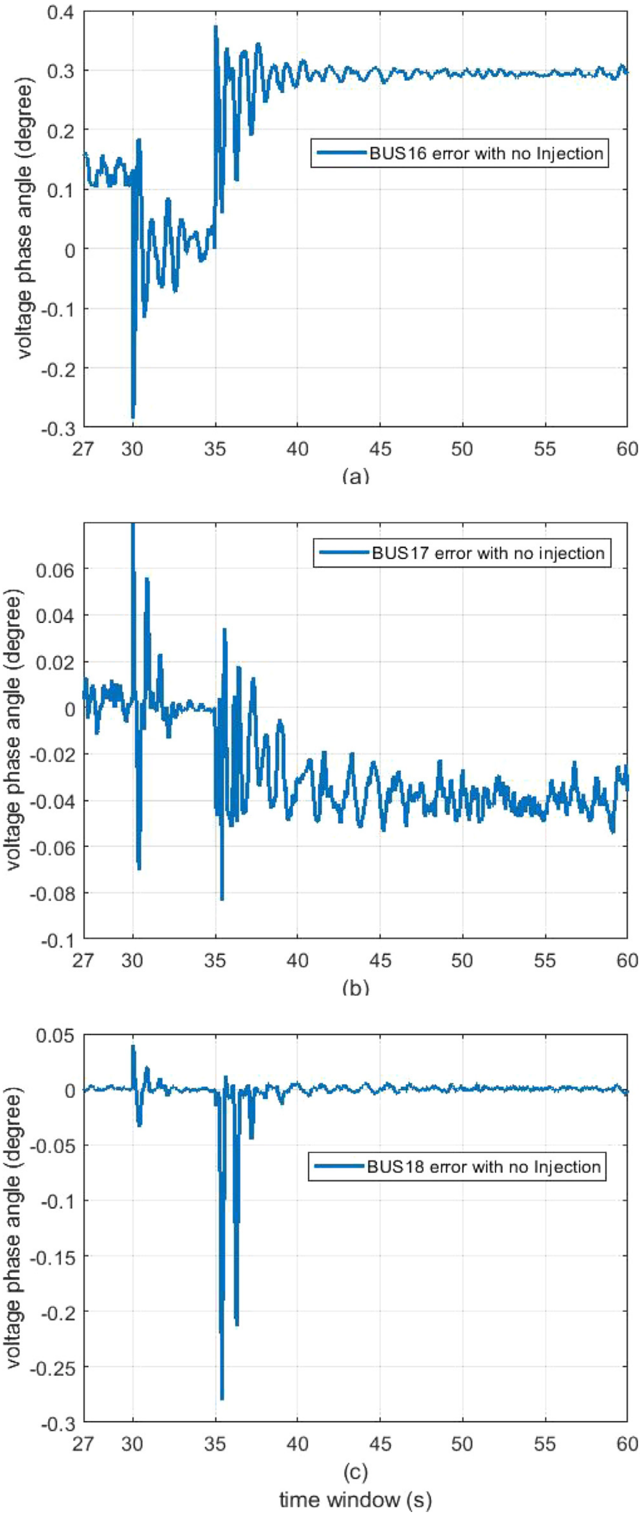

Fig. 8. Error Profile of (a) Bus 16, (b) Bus 17, and (c) Bus 18 with no injections.

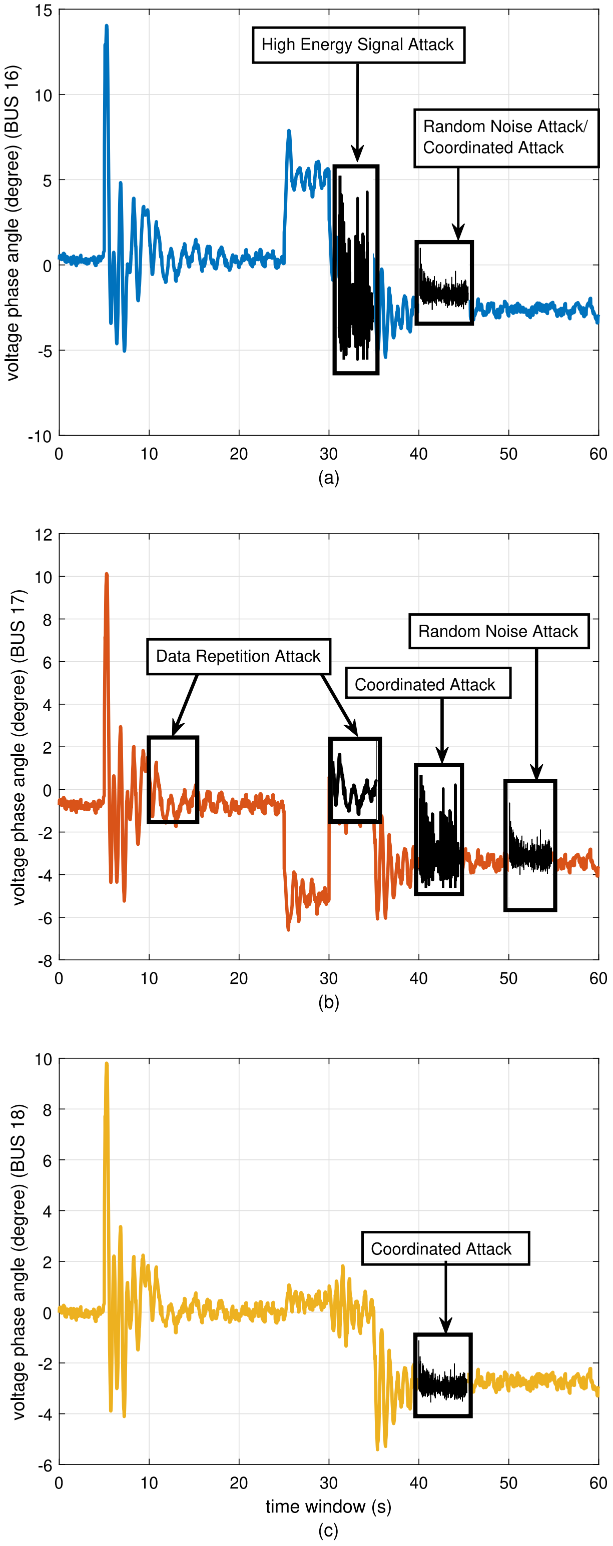

Fig. 9. Fault injections in (a) BUS 16, (b) BUS 17, and (c) BUS 18.

- *Fifth Injection with Coordinated Attack:* Another coordinated attack at Bus 16 and 18 of random noise-like variations from 40.2 s to 45.3 s respectively.

(2) Aim of an Hacker: The aim of an hacker is to intrude the system while remaining anonymous and unrecognized. A maximum duration with such an existence will allow the hacker to access important information and manipulate some level of coordination, which could lead to system instability and transient behavior. The first injection is a high-energy potency noise-like heavy signal. This injection aims to possibly bring down a local network. The second injection is a data-repetition attack. This attack is introduced to mislead the operators towards stability of the grid while delaying the supplementary damping actions. The third injection is a random noise attack. This is a typical

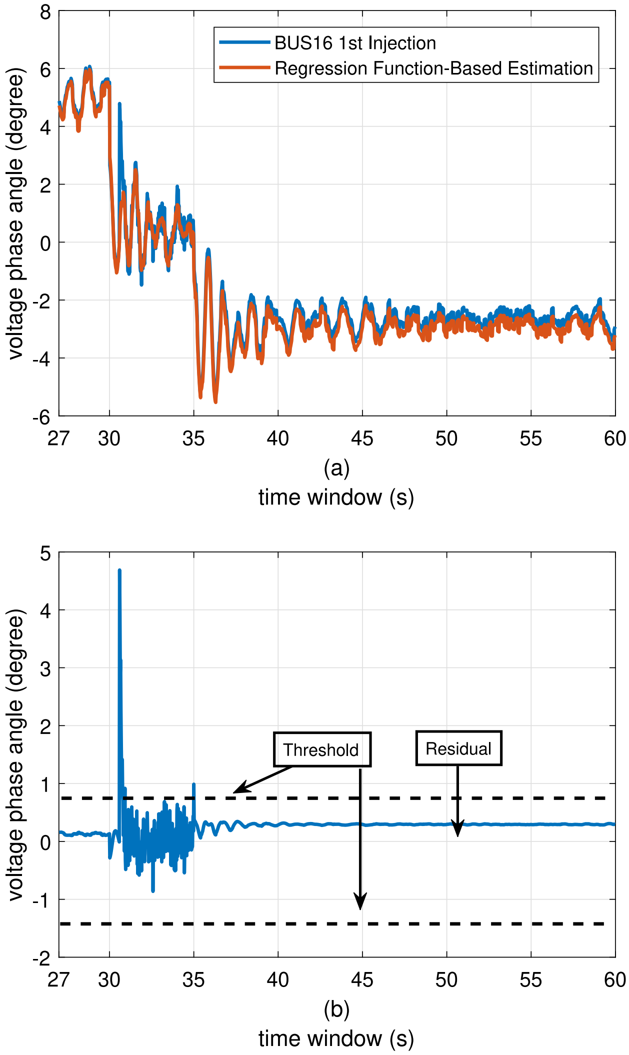

Fig. 10. Estimation performance of testing data-set and residual evaluation for (a–b) Bus 16 with its first injection.

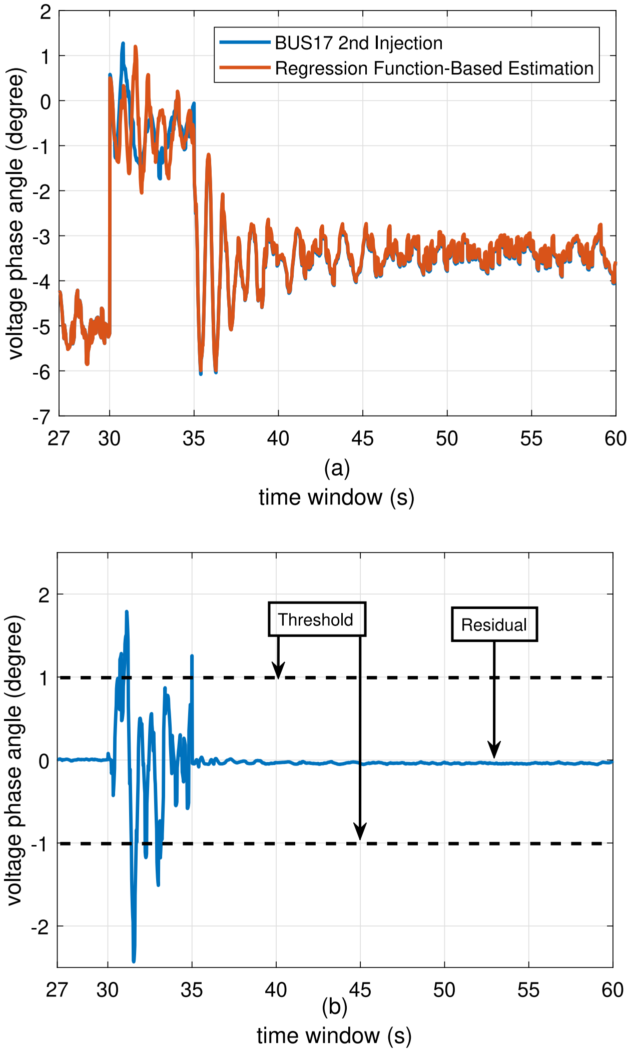

Fig. 11. Estimation performance of testing data-set and residual evaluation for (a–b) Bus 17 with its second injection.

random attack with no correlation to any signal characteristics. The fourth and fifth injections are a set of coordinated attacks. These attacks represent a set of regional attacks attempting to generate a spreading failure leading to wide-area blackouts. The purpose of injecting a variety of different signals as attacks in multiple locations is to access the robustness of the proposed scheme.

(3) Datasets — Modes of Training and Testing: Due to the non-availability of more than one data cycle, for the operation of the proposed MRF scheme, the data was split into two separate subsets for training and testing respectively. The training data-set represents a window of 0–27 s, i.e. 45% of the total time-window of 60 s. The remaining 55%, i.e. 27–60 s are reserved for testing. Note the classifiers are trained only on the training data-set.

5.5. Estimation performance with no attack injections

(1) Performance with no Injection Attacks: The performance of the proposed MRF scheme for estimation with no attack injections was made. Figs. 5(a–b), 6(a–b), and 7(a–b) show the training and testing results of such a case. The visually noticeable variation of the Bus signals between the training-data (0–27 s) and the testing-data (27–60 s) suggest a good capture of the regression model of the relationship between the Bus under investigation and the other signals of the grid.

(2) Training and Testing Error Values: Bus 16 is geographically located far from other two buses (Bus 17 and 18) on the grid, and thus showing higher error values for the training and testing. It is important to note that only part of the measurements collected from the grid were available to be included in the modeling, i.e. five generators, three loads and three buses. Therefore, it is understandable that certain quantities can be predicted better than others depending on how many dependent measurements were used in the training. Sparse regression methods eliminate non-pertinent inputs as part of the learning. Therefore, using a full or a larger set of the voltage measurements collected from the system will certainly reduce the error for all buses estimations. The error profile of these estimations with no attack injections can be seen in Fig. 8 (a–c).

5.6. Estimation performance with injected attacks

Once, the estimation performance is evaluated for an attack-free situation, it is followed by the evaluation of state estimation with situation of injected attacks. The fault injections were made in Bus 16–18 as shown in Fig. 9(a–c).

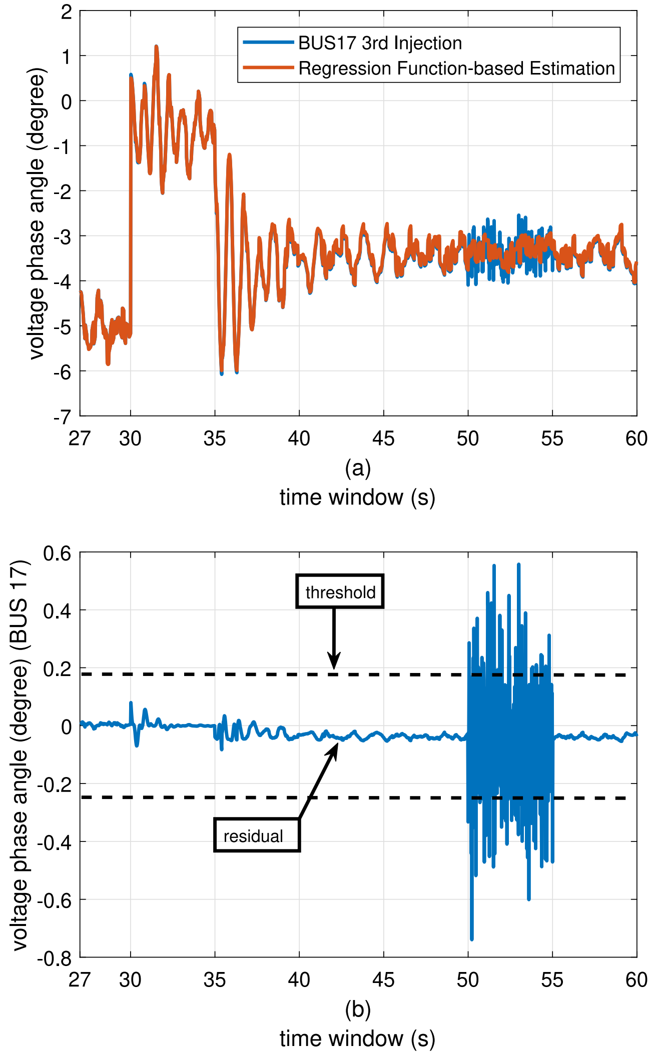

Fig. 12. Estimation performance of testing data-set and residual evaluation for (a–b) Bus 17 with its third injection.

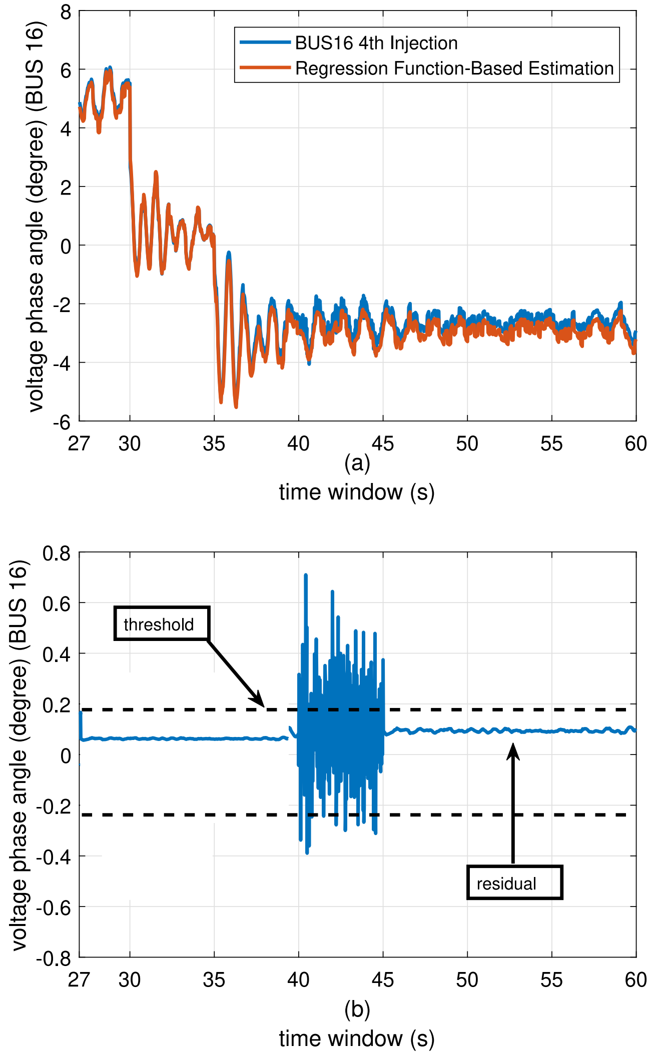

Fig. 13. Estimation performance of testing data-set and residual evaluation for (a–b) Bus 16 with its fourth injection.

(1) First Injection Scenario — A High Potency Attack: In the first injection scenario, a large spike was introduced during 30.6–35 s time-window of Bus 16 (Fig. 10(a)). Due to the location of the injection, the corrupted Bus 16 signal does not show a significant visually apparent change which makes the detection of the attack a challenging task. However, the estimation error signal shows a significant increase of during 30.6–35 s compared to the profile before and after the attack. This was well detected by the coherence spectra-based residual evaluation method while avoiding the false alarms as shown in Fig. 10(b).

(2) Second Injection Scenario — A Data Repetition Attack: In the second injection scenario, a data-repetition attack at Bus 17 from 10.2–15 s time-window was injected replicating the same measurements as of 30.2 to 35 s (Fig. 11(a)). Although the chosen repeated window (10.2 to 15 s in Bus 17) has similar local variation as to the attacked window (32.2 to 35 s in Bus 17) in the original signal, the estimation error signal shows a significant variation during 30.6–35 s in the residual evaluation, which were well captured by the proposed residual evaluation method. This can be seen in Fig. 11(b).

(3) Third Injection Scenario — Noise Attack: In the third injection scenario, a random noise attack was injected at Bus 17 from 50 to 55 s as shown in Fig. 12(a). This is a typical random attack with no correlation to any signal characteristics. Note the original signal of Bus 17 in time-window 50 to 55 s also mimics to a random attack signal. Therefore, injecting a similar random attack signal had a better chance to deceive the operator and pass undetected. However, the residual evaluation showed a significant dip during the attack period which was well detected by the threshold (See Fig. 12(b)).

(4) Fourth and Fifth Injection — Coordinated Attack: To mitigate regional attacks on measured data affecting more than one Bus, two scenarios of coordinated attacks were injections in sets. The first set comprises of a coordinated attack on Buses 16 and 17 (40–45 s) (See Figs. 13(a)–(b) and 14(a)–(b)), and the second set comprises of a simulated coordinated attack on Buses 16 and 18 (40–45 s) (See Figs. 15(a)–(b) and 16(a)–(b)). These attacks mimic an attempt to create a spreading failure leading to wide-area blackouts. The random attacks were injected in regions where the original signals look random-alike and the attack remain undetected. The estimation error signals show a significant increase in variations during the attack period compared to the signals before and after the attack. Moreover, there were some variations in the non-attack zone too. This could be due to the coordinated nature of the attack. However, the proposed threshold-based detection scheme was able to detect the presence of these attacks adequately. This can be seen in (See Figs. 13(b), 14(b), 15(b), and 16(b)).

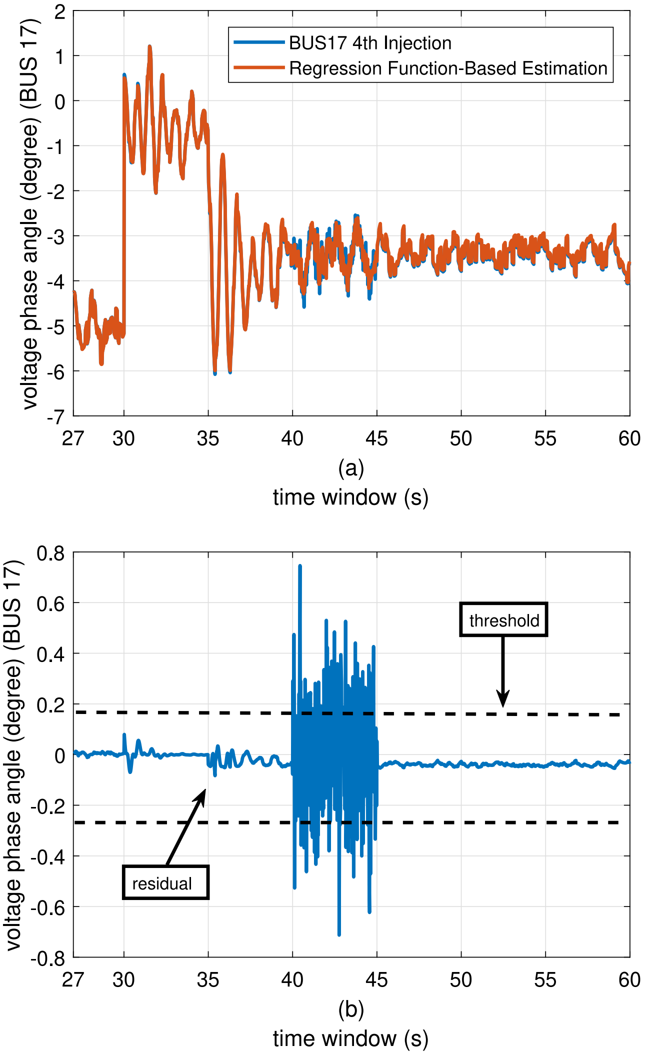

Fig. 14. Estimation performance of testing data-set and residual evaluation for (a–b) Bus 17 with its fourth injection.

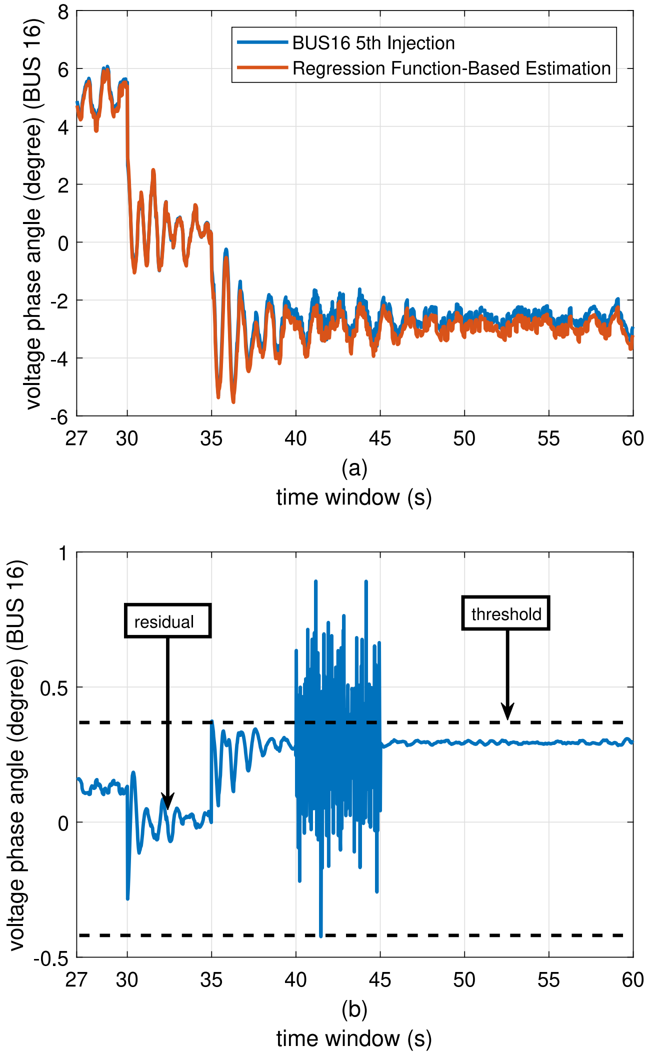

Fig. 15. Estimation performance of testing data-set and residual evaluation for (a–b) Bus 16 with its fifth injection.

5.7. Comparative analysis

(1) Estimation Comparison with Track Fusion Technique of [18]: An estimation comparison was made with the track fusion technique of [18]. The comparison was made using mean-square error (MSE). The performance comparison can be seen in Fig. 17(a). The tracking performance without the presence of data-injections can be observed in 0–30 s time-window. The only impact was the occurrence of disturbances during this time-window. Both methods were able to estimate the state oscillations decently. A variation and slight increase in MSE was observed during this time-window of 0–27 s. This is due to the occurrence of multiple disturbances during this time-window. Infact during 10–15 s time-window, the TFMP scheme loss track to the estimation. This is due to the computation of cross-covariance performed at each sensor node. The computation at each node could not capture the fast dynamics. The MSE was high for both methods in this time-window. This follows with the performance under deliberate data-injection attacks in 27–60 s time-window. The injection scenarios were a variation of high energy potency signal, data-repetition and coordinated injections which almost directly impacted time-windows of 30–35 s, 40–45 s, and 50–55 s respectively. The TFMP lost track to oscillation estimation once again due to high non-linear variations and its interaction with neighboring nodes to find the best fit. The proposed scheme kept track on all oscillations due to its regression property.

(2) Estimation Comparison with Regression Methods: An estimation comparison based on MSE was also made with the regression methods of (1) bagged trees, (2) support vector machine (SVM), (3) boosted trees, (4) linear regression, (5) Gaussian processes, (6) neural network (NN), and (7) median regression function [40–42] as shown in Fig. 17(b). The linear regression method has the lowest performance as compared to the other methods. This was expected due to its linear and least complex model representation. The bagged trees method and the NN method also followed the footsteps of a less precise and inconsistent performance. This was more visible with increased MSEs in the testing window. This is due to the random sampling nature of bagging technique and overfitting limitation of NN method. The trees and SVM were comparatively better in their performances with relatively less degradation in their test performances. In comparison with the proposed MRF technique, boosted trees and Gaussian Processes showed the most consistent performances with almost similar MSE for training and testing. However, there was a noticeable performance deterioration between their training and testing phase. On the other hand, the proposed MRF scheme was

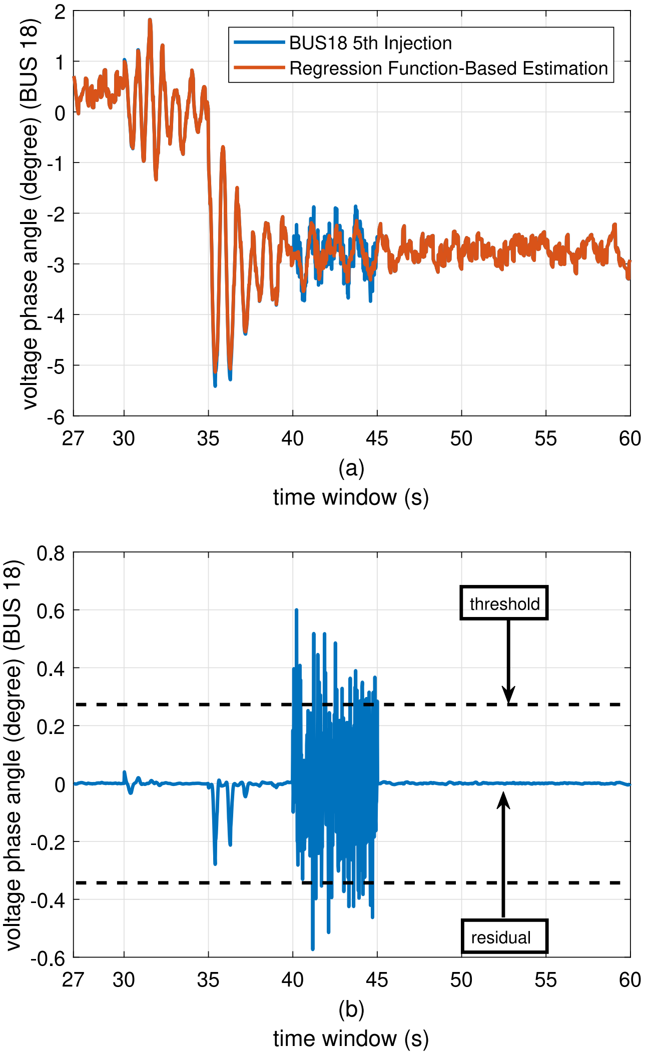

Fig. 16. Estimation performance of testing data-set and residual evaluation for (a–b) Bus 18 with its fifth injection.

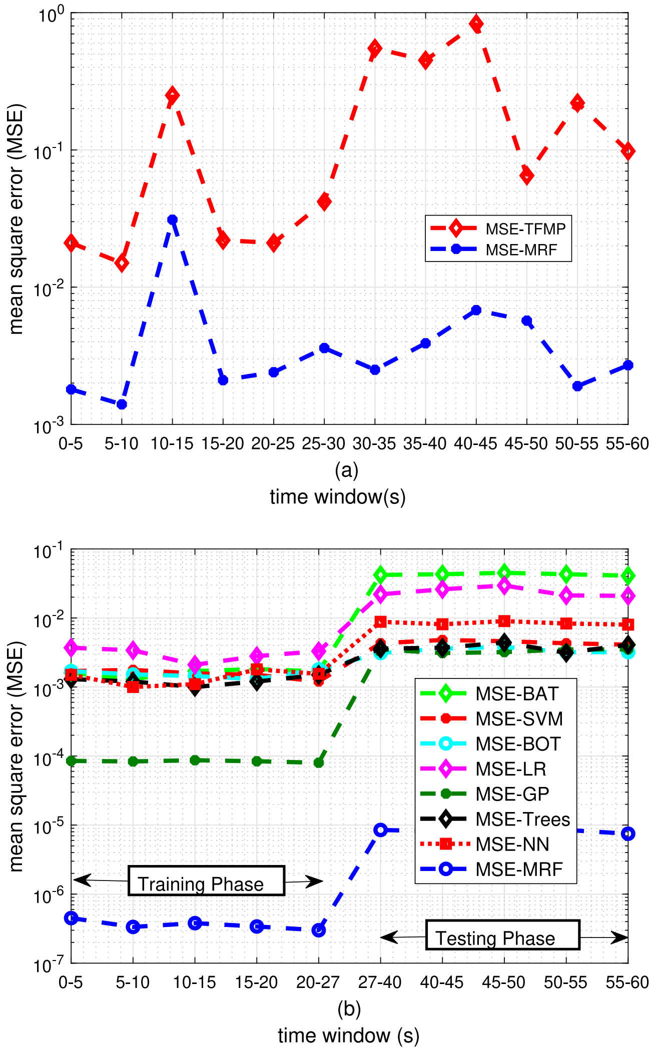

Fig. 17. State estimation MSE-based comparison with (a) TFMP [18], and (b) regression methods. The acronyms are defined as: (1) Bagged Trees (BAT), (2) Support Vector Machine (SVM), (3) Boosted Trees (BOT), (4) Linear Regression (LR), (5) Gaussian Processes (GP), (6) Neural Network (NN), and (s7) Median Regression Function (MRF).

consistent and had minimal dip in its accuracy towards both windows.

6. Conclusion and future work

The state estimation accuracy of an infected power grid is achieved in this work. The proposed scheme is validated on a revised IEEE 39-Bus New England test system with REI of large scale PV power plant. The state estimation of the grid is enhanced by the median regression function (MRF)-based algorithm which was well-supported by the mapping function for initial regression analysis. An exhaustive testing of the algorithm in the presence of multiple data-injection and its comparative analysis indicate a potential scope of deploying this algorithm in real-time while enhancing the cyber security situational awareness of grid towards uncertainties and deliberate injections. The trained regression model successfully captured the correlation between the different measurements of the grid. This also allowed the good prediction of the bus signals and the detection of different types of attacks at their occurrence. An improvement of 13% and 25% have been seen against the TFMP and regression methods respectively. The method would have performed even better when more measurements from the grid are available to use as input to the prediction models. This is due to the nature of the training process that it would naturally select pertinent input for the estimation of each bus to avoid the problem of estimation in high dimensionality.

Future work may lead towards: (1) scalability of the proposed scheme with a relatively a larger-scaled test system, (2) examine cyber-security risks at renewable generation sites of the modern power grid while involving wind farms and solar parks.

CRediT authorship contribution statement

Haris M. Khalid: Conception and design of study, Acquisition of data, Analysis and/or interpretation of data, Writing – original draft, Writing – review & editing. **Farid Flitti:** Conception and design of study, Acquisition of data, Analysis and/or interpretation of data, Writing – original draft, Writing – review & editing. **Magdi S. Mahmoud:** Conception and design of study, Acquisition of data, Analysis and/or interpretation of data, Writing – original draft, Writing – review & editing. **Mutaz M. Hamdan:** Acquisition of data, Writing – review & editing. **S.M. Muyeen:** Conception and design of study, Analysis and/or interpretation of data, Writing – original draft, Writing – review & editing. **Zhao Yang Dong:**

Conception and design of study, Analysis and/or interpretation of data, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgment

The publication of this article was funded by Qatar National Library. All authors approved the version of the manuscript to be published.

References

[1] A.G. Phadke, R.M. de Moraes, The wide world of wide-area measurement, IEEE Power Energy Mag. 6 (2008) 52–65.
[2] A. Phadke, J. Thorp, Synchronized Phasor Measurements and their Applications, Springer, New York, 2008.
[3] T. Ahmad, N. Senroy, Statistical characterization of PMU error for WAMS analytics, IEEE Trans. Power Syst. 35 (2) (2020) 920–928.
[4] X. Wang, D. Shi, Z. Wang, C. Xu, Q. Zhang, X. Zhang, Z. Yu, Online calibration of phasor measurement unit using density-based spatial clustering, IEEE Trans. Power Deliv. 33 (3) (2018) 1081–1090.
[5] H.M. Khalid, J.C.-H. Peng, Improved recursive electromechanical oscillations monitoring scheme: A novel distributed approach, IEEE Trans. Power Syst. 30 (2) (2015) 680–688.
[6] H.M. Khalid, J.C.-H. Peng, Tracking electromechanical oscillations: An enhanced maximum-likelihood based approach, IEEE Trans. Power Syst. 31 (3) (2016) 1799–1808.
[7] J. Follum, J.W. Pierre, R. Martin, Simultaneous estimation of electromechnical nodes and forced oscillations, IEEE Trans. Power Syst. 32 (5) (2016) 3958–3967.
[8] U. Agrawal, J.W. Pierre, Detection of periodic forced oscillations in power systems incorporating harmonic information, IEEE Trans. Power Syst. 34 (1) (2019) 782–790.
[9] J.B. Zhao, M. Netto, L. Mili, A robust iterated extended Kalman filter for power system dynamic state estimation, IEEE Trans. Power Syst. 32 (4) (2017) 3205–3216.
[10] G. Anagnostou, B.C. Pal, Derivative-free Kalman filtering based approaches to dynamic state estimation for power systems with unknown inputs, IEEE Trans. Power Syst. 33 (1) (2018) 116–130.
[11] A. Rouhani, A. Abur, Constrained iterated unscented Kalman filter for dynamic state and parameter estimation, IEEE Trans. Power Syst. 33 (3) (2018) 2404–2414.
[12] J.B. Zhao, L. Mili, Robust unscented Kalman filter for power system dynamic state estimation with unknown noise statistics, IEEE Trans. Smart Grid 10 (2) (2019) 1215–1224.
[13] J.B. Zhao, L. Mili, A decentralized H-infinity unscented Kalman filter for dynamic state estimation against uncertainties, IEEE Trans. Smart Grid 10 (5) (2019) 4870–4880.
[14] H.M. Khalid, S.M. Muyeen, J.C.H. Peng, Cyber-attacks in a looped energy-water nexus: An inoculated sub-observer-based approach, IEEE Syst. J. 14 (2) (2020) 2054–2065.
[15] R. Fu, X. Huang, Y. Xue, Y. Wu, Y. Tang, D. Yue, Security assessment for cyber–physical distribution power system under intrusion attacks, IEEE Access 7 (2019) (2018) 75615–75628.
[16] N. Forti, G. Battistelli, L. Chisci, S. Li, B. Wang, B. Sinopoli, Distributed joint attack detection and secure state estimation, IEEE Trans. Signal Inf. Process. Over Netw. 4 (1) (2018) 96–110.
[17] H.M. Khalid, J.C.-H. Peng, A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks, IEEE Trans. Smart Grid 7 (4) (2016) 2026–2037.
[18] H.M. Khalid, J.C.-H. Peng, Immunity towards data-injection attacks using track fusion-based model prediction, IEEE Trans. Smart Grid 8 (2) (2017) 697–707.
[19] A.S. Musleh, H.M. Khalid, S.M. Muyeen, Ahmed Al-Durra, A prediction algorithm to enhance grid resilience towards cyber attacks in WAMCS applications, IEEE Syst. J. 13 (1) (2019) 710–719.
[20] S. Ashraf, M.H. Shawon, H.M. Khalid, S.M. Muyeen, Denial-of-service attack on IEC 61850-based substation automation system: A crucial cyber threat towards smart substation pathways, MDPI–Sensors 21 (2021) 6415.
[21] M.S. Mahmoud, H.M. Khalid, M. Hamdan, Cyber-physical infra-structures in power systems: Architectures and vulnerabilities, in: Elsevier–S and T Books, 2021, pp. 1–496.
[22] R.M. Lee, M.J. Assante, T. Conway, Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case, Technical Report No. EISAC/SANS/Ukraine/DUC/5, E-ISAC, 2016, pp. 1–29.
[23] N.B. Westmoreland, J. Styczynski, S. Stables, When the Lights Went Out: Ukraine Cybersecurity Threat Briefing, Technical Report No. 2016/09, Booz Allen Hamilton, 2016, pp. 1–82.
[24] Cyber Security Notification – Meltdown & Spectre, Impact on Symphony Plus, ABB Security Not. Rep. ID 8VZZ000522, 2018, pp. 1–4.
[25] A. Abur, A.G. Exposito, Power System State Estimation: Theory and Implementation, Marcel Dekker, New York, 2004, pp. 1–327.
[26] Y.-F. Huang, S. Werner, J. Huang, N. Kashyap, V. Gupta, State estimation in electric power grids: Meeting new challenges presented by the requirements of the future grid, IEEE Signal Process. Mag. 29 (5) (2012) 33–43.
[27] A.G. -Expósito, A.V. Jaén, C.G. -Quiles, P. Rousseaux, T.V. Cutsem, A taxonomy of multi-area state estimation methods, Electr. Power Syst. Res. 81 (4) (2011) 1060–1069.
[28] Y.-F. Huang, S. Werner, J. Huang, N. Kashyap, V. Gupta, State estimation in electric power grids: Meeting new challenges presented by the requirements of the future grid, IEEE Signal Process. Mag. 29 (5) (2012) 33–43.
[29] J. Proakis, D. Manolakis, Digital Signal Processing: Principles, Algorithms, and Applications, Prentice-Hall, 1996, pp. 1–1016.
[30] T. Huang, B. Satchidanandan, P. Kumar, L. Xie, An online detection framework for cyber attacks on AGC, IEEE Trans. Power Syst. 33 (6) (2018) 6816–6827.
[31] H. Karimipour, V. Dinavahi, Robust massively parallel dynamic state estimation of power systems against cyber-attack, IEEE Access 6 (2017) 2984–2995.
[32] H. Karimipour, V. Dinavahi, On false data injection attack against dynamic state estimation on smart power grids, in: IEEE International Conference on Smart Energy Grid Engineering, SEGE, Oshawa, ON, Canada, 14-17 Aug, 2017, pp. 388–393.
[33] J. Zhao, G. Zhang, M.L. Scala, Z.Y. Dong, C. Chen, J. Wang, Short-term state forecasting-aided method for detection of smart grid general FDIA, IEEE Trans. Smart Grid 8 (4) (2017) 1580–1590.
[34] A. Anwar, A.N. Mahmood, Z. Tari, Ensuring data integrity of OPF module and energy database by detecting changes in PFP in smart grids, IEEE Trans. Ind. Inform. 13 (6) (2017) 3299–3311.
[35] Y. Li, J. Li, X. Luo, X. Wang, X. Guan, Cyber attack detection and isolation for smart grids via unknown input observer, in: 37th Chinese Control Conference, CCC, Wuhan China, 25-27 Jul, 2018, pp. 1–6.
[36] H.M. Khalid, Q. Ahmed, J.C.-H. Peng, Health monitoring of Li-ion battery systems: A median expectation-based diagnosis approach (MEDA), IEEE Trans. Transp. Electr. 1 (1) (2015) 94–105.
[37] I. Hiskens, IEEE PES Task Force on Benchmark Systems for Stability Controls, Technical Report, 2013.
[38] L. Wang, Q.-S. Vo, A.V. Prokhorov, Stability improvement of a multimachine power system connected with a large-scale hybrid wind-photovoltaic farm using a supercapacitor, IEEE Trans. Ind. Appl. 54 (1) (2017) 50–60.
[39] DIgSILENT, PowerFactory 15 user manual, 2013.
[40] D.J.C. MacKay, Information Theory, Inference and Learning Algorithms, Cambridge Uni. Press, New York, NY, USA, 2002, pp. 1–640.
[41] S. Haykin, Neural Networks: A Comprehensive Foundation, Prentice Hall, Upper Sddle River, New Jersey, 1999, pp. 1–842.
[42] J.S. Taylor, N. Cristianini, Kernel Methods for Pattern Analysis, Cambridge Uni. Press, 2004, pp. 1–462.