Iranian Journal of Electrical and Electronic Engineering 03 (2020) 279–291
Special Issue on Smart Grids

Iranian Journal of Electrical and Electronic Engineering

Journal Homepage: ijeee.iust.ac.ir

Research Paper

An Effective Attack-Resilient Kalman Filter-Based Approach for Dynamic State Estimation of Synchronous Machine

Z. Kazemi* and A. A.Safavi*(C.A.)

Abstract: Kalman filtering has been widely considered for dynamic state estimation in smart grids. Despite its unique merits, the Kalman Filter (KF)-based dynamic state estimation can be undesirably influenced by cyber adversarial attacks that can potentially be launched against the communication links in the Cyber-Physical System (CPS). To enhance the security of KF-based state estimation, in this paper, the basic KF-based method is enhanced by incorporating the dynamics of the attack vector into the system state-space model using an observer-based preprocessing stage. The proposed technique not only immunizes the state estimation against cyber-attacks but also effectively handles the issues relevant to the modeling uncertainties and measurement noises/errors. The effectiveness of the proposed approach is demonstrated by detailed mathematical analysis and testing it on two well-known IEEE cyber-physical test systems.

Keywords: Cyber Attack (CA), Cyber-Physical System (CPS), Kalman Filter (KF), Smart Grid, Synchronous Machine.

1 Introduction

RELIABILITY and security of smart power grids are of great importance as they have critical impacts on society and people's life. However, smart grids are potentially subjected to significant cyber threats due to the use of vulnerable communication networks and cyber components. The Cyber-Attacks (CAs) on smart grid communication links can lead to costly and irreparable consequences. For instance, in August 2003, an electric power blackout occurred in some parts of the Midwest and the Northeast United States and Ontario, Canada, which resulted in more than $4 billion U.S. dollars and $2 billion Canadian dollars losses, respectively [1]. Likewise, in December 2015, CAs occurred against three different distribution companies in Ukraine, which resulted in several power outages and approximately 225,000 customers lost power [2]. Therefore, cybersecurity has been considered as one of the critical issues in modern smart grids.

In the smart grids, the condition of the system is usually assessed based on the readings of the sensors and phasor measurement units (PMUs), which are solely placed at important and pre-determined locations of the smart grid. The information about other system variables can be obtained using the PMUs measurements and state estimation. In the state estimation process, the measurements of the meters and the system model are usually used to obtain accurate estimations of the system's unknown variables. Such information can subsequently be used to fulfill important objectives in the smart grid such as power grid control, transient stability analysis, load shedding, contingency analysis, etc. [3, 4]. However, due to the excessive number of communication links in the smart grid, it is probable that the information of the meters will be compromised and manipulated by attackers, which undesirably affects the security and reliability of the smart grid. It is noteworthy that the commonly used residual-based bad data detection (BDD) methods are not effective enough for the detection of such CAs [5, 6]. Therefore, efficient algorithms must be devised to nullify the CAs for improving the security posture of the smart grid [6-8].

A large number of research works have been conducted to address the abovementioned problem. The

Iranian Journal of Electrical and Electronic Engineering, 2020.
Paper first received 25 September 2019, revised 19 February 2020, and accepted 28 February 2020.
* The authors are with the Advanced Control Laboratory, School of Electrical and Computer Engineering, Shiraz University, Shiraz, Iran.
E-mails: z.kazemi@shirazu.ac.ir and safavi@shirazu.ac.ir.
Corresponding Author: A. A.Safavi.

research works can be broadly divided into three categories: 1- theoretical research works; 2- application research works; and 3- defensive research works [8]. The main goal of the theoretical research works is to analyze the problem from the attacker's point of view, by devising and constructing innovative and undetectable CA vectors. For example, in some works, the attack vector is constructed under the premises of limited access of the attacker to the information of the meters [5, 9], incomplete system information [10], false system topology [11], utilization of the AC power flow model [12], etc. On the other hand, the application research works mainly concern analyzing the effects of the CAs on the operation of the smart grid, e.g. market management systems and energy management systems [13]. Moreover, the main target in the defensive research works is to develop effective defense mechanisms from the smart grid's perspective for mitigating the battering effects of the CAs [14-17]. The defensive mechanisms are crucial for protecting the smart grid against economic and security threats of the CAs. In this sense, many algorithms have so far been proposed. These algorithms can be generally classified into three different groups as follows:

Protection-based methods: An extensive amount of work has so far been fulfilled on the protection-based methods in the literature. The methods in this category are mainly based on the protection of a set of basic measurements [8]. These methods deal with obtaining a minimum set of measurements, which is sufficient to solve the secure state estimation problem in the smart grid. For example, Liu *et al.* [5] showed that if an attacker could compromise a measurement set with at least m-n+1 observations, with m being the number of measurements and n being the number of state variables in a DC state estimation model, an attack vector always exists, which can potentially inject false data and can also bypass the system BDDs. Bi and Zhang [14] used graphical methods to carefully select meter measurements such that no attack could be launched to compromise any set of state variables. Deng *et al.* [15] focused on designing a least-budget defense strategy for a suitable selection of the meters that have to be protected. In addition, the amount of the defense budget that should be deployed on each of the selected meters is also determined in Deng's research.

Detection-based methods: In the detection-based methods, the existence of the attacks is discerned by analysis of the measurements. For example, an interleaved Hop-by-hop authentication scheme has been proposed to filter out the injected false data in [16]. Likewise, Li *et al.* [17] proposed a sequential detector based on the Generalized Likelihood Ratio (GLR) for the robust detection of the attacks.

Resilient estimation-based methods: Salehghaffari and Khorrami [18] designed a resilient static state estimator by applying perturbations to the impedance of the transmission lines and monitoring of subsequent impacts on the power system. Subsequently, an optimization problem is formulated to minimize the maximum injected additive error to true state estimations. Chakhchoukh and Ishii [19] utilized multiple least trimmed squares estimators for secure static state estimation of the power system.

Although the design of resilient estimators has been widely discussed in the literature [18-21], by far, only a few papers have addressed the problem of smart grid secure dynamic state estimation in presence of the CAs. Taha *et al.* [22] proposed a Sliding Mode Observer-based (SMO) secure dynamic state estimation strategy for estimating states and unknown inputs. This approach has very good robustness against the modeling uncertainties. However, this approach has a relatively high computational burden which is due to the need for calculations of the SMO algorithm, solving an optimization program, using a separate algorithm for CAs, etc. In [23], considering the features of the traditional chi-square statistics and historical statistical information of power system state variables in normal conditions, a real-time chi-square CA detection method associated with two kinds of Kalman Filter (KF)-based state estimators has been proposed. The advantage of this method lies in its high robustness against the measurement noises. In [24], a robust Generalized Maximum Likelihood Iterated Extended KF (GM-IEKF) has been proposed for dynamic state estimation in smart grids. In this method, first, a batch-mode regression form for enhancing the data redundancy is built to detect the outliers. Then, a GM-based estimator using the convex Huber cost function is used to suppress the negative impacts of the outliers. The method provides very good robustness against the measurement noises and modeling uncertainties. In [25], a resilient algorithm has been proposed, which consists of local Luenberger estimators, local residual detectors, and a global fusion process. In the local stage, the Luenberger-based estimators are used to estimate the system states for different local groups of the sensors. Then, based on local residual detectors, the sets of valid state estimates are selected and sent to the global estimation stage. Finally, the ultimate results of the state estimates are obtained using a global fusion process.

The main contribution of this paper which makes it completely different from the above-reviewed works is that a KF-based estimator that simultaneously estimates both the system states as well as the attack vector is proposed. The KF-based joint estimation of the states and attack vector is achieved by deriving the attack vector dynamics in a primary stage using an observer-based technique. The proposed strategy not only enhances the estimation accuracy but also provides the estimation of the attack vector which can be used to enhance the security posture of the power grid. To confirm the effectiveness of the proposed method, it is evaluated in two well-established cyber-physical systems, namely IEEE 14-bus and 30-bus test systems,

for estimation of the synchronous generators state variables. The rest of this paper is organized as follows. In Section 2, the utilized dynamic model of the power system for dynamic state estimation problem is presented. The operating principles, detailed analytical analysis, and design considerations of the proposed approach are discussed in Section 3. The simulation results of the proposed method on the IEEE 14-bus and 30-bus test systems are included in Section 4. Finally, Section 5 presents the main conclusions of the paper.

2 Synchronous Machine Model

The nonlinear and linearized dynamic models for the synchronous machine are presented in different subsections as follows.

2.1 Nonlinear Dynamic Model

The second-order swing equations for a synchronous generator in a power system with n synchronous generators can be expressed as follows [26]:

$$M_i \frac{dw_i}{dt} = P_{mi} - E_i{}^2 \hat{G}_{ii} - \sum_{\substack{j=1,\\ j\neq i}}^{n} |E_i||E_j| \left[\hat{B}_{ij} \sin(\delta_i - \delta_j) + \hat{G}_{ij} \cos(\delta_i - \delta_j) \right] - D_i w_i \qquad \frac{d\delta_i}{dt} = w_i \quad i = 1,2,...,n \tag{1}$$

The output electric power for each synchronous generator can also be written as follows:

$$P_{Gi} = E_i{}^2 \hat{G}_{ii} + \sum_{j=1, j\neq i}^{n} |E_i||E_j| \left[\hat{B}_{ij} \sin(\delta_i - \delta_j) + \hat{G}_{ij} \cos(\delta_i - \delta_j) \right] \tag{2}$$

In (1) and (2), the vector of rotor angles δ and rotor speeds w are considered as the states of the system, P_{mi} is the mechanical input power of each generation unit, which is considered to be known and constant, and P_{Gi} is the active power supplied by synchronous generator i, which is considered as the output of the system. Moreover, M_i, $\hat{G}_{ij}$, $\hat{B}_{ij}$, E_i, and D_i are inertia constant, transfer conductance, transfer susceptance, internal voltage and damping constant of generator i, respectively. The foregoing variables are defined in a vector form as follows:

$$\delta = [\delta_1 ... \delta_i ... \delta_n]^T, \quad w = [w_1 ... w_i ... w_n]^T$$
$$u = [P_{m1} ... P_{mi} ... P_{mn}]^T, \quad y = [P_{G1} ... P_{Gi} ... P_{Gn}]^T \tag{3}$$

Thus, the nonlinear state-space representation of the power system can be written as:

$$\begin{cases} \dot{X}(t) = \begin{bmatrix} \dot{\delta} \\ \dot{w} \end{bmatrix} = f(X, u) \\ y(t) = h(X) \end{cases} \tag{4}$$

In the case of large-scale power systems, analyzing the above nonlinear state-space equations will be very difficult and computationally demanding. Hence, the linearized equations of the power system are derived in the next subsection.

2.2 Linearized Dynamic Model of Power System

In this subsection, a linear time-invariant (LTI) representation of the power system dynamic model is obtained considering the following two assumptions:

Assumption 1. Since the difference between the phase angles in power systems are usually small, it is assumed that $\sin\theta \approx \theta$.

Assumption 2. The power losses of the power system are neglected and thus, the real part of the admittance matrix is considered to be zero $\hat{G}_{ij} = 0\ \forall i, j$.

Considering the abovementioned assumptions, (1) and (2) can be rewritten as follows:

$$M_i \frac{dw_i}{dt} = P_{mi} - \sum_{j=1, j\neq i}^{n} |E_i||E_j| \left[\hat{B}_{ij} (\delta_i - \delta_j) \right] - D_i w_i$$
$$\frac{d\delta_i}{dt} = w_i \qquad i = 1,2,...,n \tag{5}$$

$$P_{Gi} = \sum_{j=1, j\neq i}^{n} |E_i||E_j| \left[\hat{B}_{ij} (\delta_i - \delta_j) \right] \tag{6}$$

Therefore, the LTI representation of the state-space dynamic model of the power system can be expressed as follows:

$$\begin{cases} \dot{X}(t) = AX(t) + Bu(t) \\ y(t) = CX(t) \end{cases} \tag{7}$$

where matrix $A \in \mathbb{R}^{2n\times 2n}$ is obtained as follows:

$$A = \begin{bmatrix} 0 & \boldsymbol{I} \\ Z & D \end{bmatrix}$$

where $\mathbf{0} \in \mathbb{R}^{n\times n}$ and $\mathbf{I} \in \mathbb{R}^{n\times n}$ are zero and identity matrices. In addition, $Z \in \mathbb{R}^{n\times n}$ and $D \in \mathbb{R}^{n\times n}$ are given in the Appendix. With the foregoing representation, matrix A in the LTI state-space dynamic model is a singular matrix, i.e. its determinant is equal to zero $|A| = 0$. Since the singular matrix A is not invertible, it causes difficulties for the implementation of the proposed method. To tackle the foregoing problem, an alternative state-space representation of the system model is derived. We define new states of the system as follows:

$$\begin{cases} \delta_1 - \delta_2 = x_1 \\ \vdots \\ \delta_1 - \delta_i = x_{i-1} \\ \vdots \\ \delta_1 - \delta_n = x_{n-1} \end{cases}, \begin{cases} w_1 = x_n \\ \vdots \\ w_i = x_{n+i-1} \\ \vdots \\ w_n = x_{2n-1} \end{cases}, X = \begin{bmatrix} x_1 \\ \vdots \\ x_{2n-1} \end{bmatrix} \quad (8)$$

Substituting (8) in (5) and (6), the LTI state-space representation of the dynamic model of the power system is obtained as follows:

$$\frac{dw_i}{dt} = \frac{1}{M_i}(P_{mi} - \sum_{j=1, j\neq i}^{n} |E_i||E_j|\left[\hat{B}_{ij}(x_{j-1} - x_{i-1})\right] - D_i w_i) \quad i = 1,...,n \ , \ x_0 = 0$$

$$\frac{dx_i}{dt} = w_1 - w_{i+1} \qquad i = 1,2,...,n-1 \quad (9)$$

$$P_{Gi} = \sum_{j=1, j\neq i}^{n} |E_i||E_j|\left[\hat{B}_{ij}(x_{j-1} - x_{i-1})\right] \ i = 1,...,n \ , \ x_0 = 0 \quad (10)$$

Therefore, the final form of the $A \in \mathbb{R}^{(2n-1)\times(2n-1)}$, $B \in \mathbb{R}^{(2n-1)\times n}$, and $C \in \mathbb{R}^{n\times(2n-1)}$ matrices in the state-space model of the power system are obtained as shown in (11).

$$A = \left[\begin{array}{c|c} \mathbf{0} \in \mathbb{R}^{(n-1)\times(n-1)} & \begin{matrix} 1 & -1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \underbrace{0 \quad \cdots \quad -1}_{-\mathbf{I} \in \mathbb{R}^{(n-1)\times(n-1)}} \end{matrix} \\ \hline S \in \mathbb{R}^{n\times(n-1)} & \underbrace{\begin{matrix} -\frac{D_1}{M_1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & -\frac{D_n}{M_n} \end{matrix}}_{n\times n} \end{array}\right],$$

$$B = \left[\begin{array}{c} \mathbf{0} \in \mathbb{R}^{(n-1)\times n} \\ \hline \underbrace{\begin{matrix} \frac{1}{M_1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \frac{1}{M_n} \end{matrix}}_{n\times n} \end{array}\right], C = \left[H \in \mathbb{R}^{n\times(n-1)} \mid \mathbf{0} \in \mathbb{R}^{n\times n}\right] \quad (11)$$

3 The Proposed Attack-Resilient KF-Based Approach

In this Section, the problem description and different steps of the proposed state estimation method are provided. The main problem in the proposed method is to estimate the dynamics of the attack vector and the system states at the same time. To fulfill this, first, we derive the dynamic of the attack vector in a preprocessing with an observer. Then, the derived dynamic of the attack vector is augmented with the main system model and finally, the KF algorithm is applied to simultaneously estimate both the system and attack vector state variables. In the following, different steps for designing the proposed attack-resilient KF-based estimator are provided with details.

3.1 Observer Design for Deriving the Attack Vector Dynamics

In this subsection, based on the derived dynamic model in Section 2, the Unknown Input Observer (UIO) is designed and used for deriving the dynamics of the attack vector. The state-space model of the power system in the presence of a CA can be described as follows:

$$\begin{cases} \dot{X}(t) = AX(t) + Bu(t) \\ y^a(t) = CX(t) + a(t) \end{cases} \quad (12)$$

where $a(t)$ is the attack vector that is injected into the measurement data by an adversary.

For the system model (12) the UIO equations can be given by:

$$\begin{cases} \dot{z} = Fz + TBu + Gy^a \\ \hat{X}_{UIO} = z + Ny^a \end{cases} \quad (13)$$

Definition 1. The state observer (13) is a UIO if the state estimation error $e = X - \hat{X}_{UIO}$ converges to zero asymptotically, regardless of the value of the unknown input [27].

Based on the foregoing definition and considering (12) and (13) and $\alpha(t) = H \times q(t)$, the sufficient conditions for designing the UIO are derived as follows [28]:

$$\begin{cases} \text{a)} I - NC = T \\ \text{b)} G - FN = \bar{G} \\ \text{c)} TA - \bar{G}C = F \\ \text{d)} \bar{G}H = 0 \\ \text{e)} NH\dot{q}(t) = 0 \\ \text{f)} \dot{e}(t) = Fe(t) \text{ is asymptotically stable} \\ \text{g)} (C, A - NCA) \text{ is detectable pair} \end{cases} \quad (14)$$

Thus, the problem of designing the UIO is reduced to finding the UIO matrices $N \in \mathbb{R}^{(2n-1)\times n}$, $F \in \mathbb{R}^{(2n-1)\times(2n-1)}$, $T \in \mathbb{R}^{(2n-1)\times(2n-1)}$, and $\bar{G} \in \mathbb{R}^{(2n-1)\times n}$ such that the foregoing matrices satisfy the conditions of (14). These conditions are obtained as a linear matrix equation as follows:

$$\Phi\Lambda = \Psi \quad (15)$$

where $\Phi \in \mathbb{R}^{(2n-1)\times(6n-2)}$, $\Lambda \in \mathbb{R}^{(6n-2)\times(8n-4)}$, and $\Psi \in \mathbb{R}^{(2n-1)\times(8n-4)}$ are defined as follows:

$$\Phi = \left[T \quad N \quad F \quad \bar{G}\right]$$

$$\Lambda=\left[\begin{array}{c|c|c|c} \mathbf{I}\in\mathbb{R}^{(2n-1)\times(2n-1)} & \mathbf{0}\in\mathbb{R}^{(2n-1)\times(2n-1)} & A & \mathbf{0}\in\mathbb{R}^{(2n-1)\times(2n-1)} \\ \hline C & \mathbf{0}\in\mathbb{R}^{n\times(2n-1)} & \mathbf{0}\in\mathbb{R}^{n\times(2n-1)} & H \\ \hline \mathbf{0}\in\mathbb{R}^{(2n-1)\times(2n-1)} & \mathbf{0}\in\mathbb{R}^{(2n-1)\times(2n-1)} & -\mathbf{I}\in\mathbb{R}^{(2n-1)\times(2n-1)} & \mathbf{0}\in\mathbb{R}^{(2n-1)\times(2n-1)} \\ \hline \mathbf{0}\in\mathbb{R}^{n\times(2n-1)} & H & -C & \mathbf{0}\in\mathbb{R}^{n\times(2n-1)} \end{array}\right]$$

$$\Psi=\left[\boldsymbol{I}\in\mathbb{R}^{(2n-1)\times(2n-1)} \quad 0\in\mathbb{R}^{(2n-1)\times(6n-3)}\right]$$

Equation (15) can be easily solved using any semidefinite program solvers such as MATLAB's LMI solver. It should be mentioned that the design of the UIO is fulfilled based on the system equations of (12), which neglects the modeling uncertainties and measurement errors. Nonetheless, in practice, the effects of modeling uncertainties and measurement errors should be considered in the system model as follows:

$$\begin{cases}\dot{X}(t)=AX(t)+Bu(t)+n(t)\\ y^{a}(t)=CX(t)+a(t)+v(t)\end{cases} \tag{16}$$

where $n(t)$ and $v(t)$ are Gaussian white noises with zero mean and covariance matrices Q and R, which account for the modeling uncertainties and measurement errors, respectively. It is noteworthy that the Gaussian noise assumption is a prerequisite and basis for optimal state estimation with the KF algorithm [29] and many of the existing KF-based dynamic state estimation approaches have also considered measurement noises with Gaussian distribution [30-34]. Although the foregoing assumption has been considered in several research studies it might not exactly match the practical cases where the noise might have a different distribution such as Laplace distribution. To resolve this problem, some research works have so far been conducted which include the use of GM-Unscented KF (GM-UKF) [35], Huber's M-estimation-based cubature KF [36], H-infinity UKF [37], etc. It should also be noted that the foregoing derivations of the KF algorithm can be used in the proposed approach with some modifications to resolve the non-Gaussian noise problem. A detailed analysis of the noise effect is relegated to future work.

In the proposed method, the dynamic model of the attack vector should be derived. At first, based on the estimation results of the designed UIO, the estimated attack vector is obtained as follows:

$$\hat{a}_{UIO}=y^{a}-\hat{y}_{UIO}=CX+a+v(t)-C\hat{X}_{UIO} \tag{17}$$

where y^a is the system measurement affected by the attack. In addition, $\hat{y}_{UIO}$ and $\hat{X}_{UIO}$ are the estimated output and estimated system states by the UIO, respectively. Using (17) and considering (13), (14), and (17), the dynamic model of the attack can then be derived as follows [28]:

$$\begin{aligned}\dot{\hat{a}}_{UIO}&=C\dot{X}+\dot{a}+\dot{v}(t)-C\dot{\hat{X}}_{UIO}\\ &=C\left(AX+Bu+n(t)\right)+\dot{a}+\dot{v}(t)-C(\dot{z}+N\dot{y}^{a})\\ &=CAX+CBu+Cn(t)+\dot{a}+\dot{v}(t)-CF(\overbrace{\hat{X}_{UIO}-Ny^{a}}^{z})\\ &\quad -CTBu-CGy^{a}-CNC(AX+Bu+n(t))-CN\dot{a}(t)\\ &\quad -CN\dot{v}(t)=CF(X-\hat{X}_{UIO})+(I-CN)\dot{a}(t)\\ &\quad +C(I-NC)n(t)+(I-CN)\dot{v}(t)\\ &\Rightarrow(CN-I)\dot{a}=CF(X-\hat{X}_{UIO})-\dot{\hat{a}}_{UIO}(t)\\ &\qquad +C(I-NC)n(t)+(I-CN)\dot{v}(t)\end{aligned} \tag{18}$$

3.2 Robust and Secure State Estimation With KF

In this section, to jointly estimate the states of the system and attack vector, the derived dynamic of the attack vector (18) should be augmented with the system model (16). The dynamic model for state estimation with the KF algorithm is derived for two different scenarios in the following.

Case 1: *The attack vector is a linear combination of the column vectors of matrix C* [5]: This attack scenario is introduced in [5]. It has been proved that under the aforementioned condition, many of the conventional state estimation methods and BDD approaches will lead to erroneous results. The condition of this scenario can be represented as follows:

$$a(t)=C\times q(t) \tag{19}$$

Substituting (19) in the UIO design equations of (14) leads to:

$$\begin{cases}I=T\\ G=AN\\ A=F\\ NC=0\\ \dot{e}(t)=Ae(t)\ \text{is asymptotically stable}\\ (C,A)\ \text{is detectable pair}\end{cases} \tag{20}$$

Therefore, for the attack scenario of *Case 1*, the conditions of (20) must be applied to the proposed UIO design. In (20), the feasibility of the last two conditions must also be confirmed, which is fulfilled in the following:

Definition 2. Matrix A is asymptotically stable if and only if every eigenvalue of A lies in the open left-hand half complex plane.

According to Definition 2, the eigenvalues of matrix A should be derived and assessed. Thus, the characteristic equation of matrix A is derived to find the eigenvalues of A. In order to simplify the calculation of $|s\mathbf{I}-A|$, some elementary row and column operations are used (see (A.1) and (A.2) in the Appendix). Therefore, the stability of matrix A can be confirmed by checking the roots of (21).

$$\det(sI-A)=\det\left(\left[\begin{array}{c|c} sI^{(n-1)\times(n-1)}-0^{(n-1)\times(n-1)} & \Gamma^{(n-1)\times n} \\ \hline -S^{n\times(n-1)} & \Sigma^{n\times n}\end{array}\right]\right)$$

$$= \frac{1}{s^{n-1}} \det\left(\left[\begin{array}{c|c} sI^{(n-1)\times(n-1)} & 0^{(n-1)\times n} \\ \hline -S^{n\times(n-1)} & \Omega^{n\times n} \end{array}\right]\right)$$

$$= \frac{1}{s^{n-1}} \underbrace{\det\left(sI^{(n-1)\times(n-1)}\right)}_{s^{n-1}} \det(\Omega) = \det(\Omega) = 0 \qquad (21)$$

Definition 3. Pair (C, A) is detectable if and only if the following condition is satisfied:

$$rank\begin{bmatrix} sI - A \\ C \end{bmatrix} = \dim(A) = 2n - 1$$

For the derived dynamic model of the power system, the condition of Definition 3 is satisfied (see the proof in Appendix). In addition, substituting (20) in (18), the dynamic model of the attack vector is derived and then, by augmenting the derived dynamic of the attack vector with the system model of (16), the new model (22) is obtained as follows:

$$\underbrace{\begin{bmatrix} \dot{X}(t) \\ \dot{a} \end{bmatrix}}_{\dot{X}_{aug}} = \underbrace{\begin{bmatrix} A & \mathbf{0} \\ -CA & \mathbf{0} \end{bmatrix}}_{A_{aug}} \underbrace{\begin{bmatrix} X(t) \\ a(t) \end{bmatrix}}_{X_{aug}} + \underbrace{\begin{bmatrix} B & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & -CA & \boldsymbol{I} \end{bmatrix}}_{B_{aug}} \underbrace{\begin{bmatrix} u(t) \\ -\hat{X}_{UIO} \\ \dot{\hat{a}}_{UIO}(t) \end{bmatrix}}_{u_{aug}} + \underbrace{\begin{bmatrix} n(t) \\ k(t) \end{bmatrix}}_{n_{aug}}$$

$$y^a(t) = \underbrace{\begin{bmatrix} C & \boldsymbol{I} \end{bmatrix}}_{C_{aug}} \underbrace{\begin{bmatrix} X(t) \\ a(t) \end{bmatrix}}_{X_{aug}} + v(t) \qquad (22)$$

where $k(t) = C\dot{n}(t) + \dot{v}(t)$, $\hat{X}_{UIO}$ is estimated system states by the UIO, and $\dot{\hat{a}}_{UIO}$ is derivative of $\hat{a}_{UIO}$ which is obtained by (17).

Case 2: Attack vector is a piecewise constant function: In this scenario, since it is considered that the attack vector is a piecewise constant function in the time domain, the dynamic of the attack at each time interval is assumed to be zero. Therefore, the UIO design equations can be rewritten as follows:

$$\begin{cases} I - NC = T \\ G = FN \\ TA = F \\ \bar{G} = 0 \\ \dot{e}(t) = (I - NC)Ae(t) \text{ is asymptotically stable} \\ (C, A - NCA) \text{ is detectable pair} \end{cases} \qquad (23)$$

Matrix N in (23) needs to be determined such that the last two conditions are satisfied. Other design matrices can be easily obtained upon calculation of N and then, the dynamic of the attack vector is calculated by (18). As can be seen, there is more degree of freedom to find the appropriate matrix N rather than the previous case. Thus, matrix N can be selected such that the real parts of the eigenvalues of $(I\text{-}NC)A$ not only are negative but also have larger absolute values to increase the convergence speed of the state estimation. By augmenting the derived dynamic of the attack vector with the system model of (16), the augmented model (24) is derived which is used in the second part of the proposed method.

$$\underbrace{\begin{bmatrix} \dot{X}(t) \\ \dot{a} \end{bmatrix}}_{\dot{X}_{aug}} = \underbrace{\begin{bmatrix} A & \mathbf{0} \\ (CN - \boldsymbol{I})^{-1}CF & \mathbf{0} \end{bmatrix}}_{A_{aug}} \underbrace{\begin{bmatrix} X(t) \\ a(t) \end{bmatrix}}_{X_{aug}}$$

$$+ \underbrace{\begin{bmatrix} B & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & (CN - \boldsymbol{I})^{-1}CF & -(CN - \boldsymbol{I})^{-1} \end{bmatrix}}_{B_{aug}} \underbrace{\begin{bmatrix} u(t) \\ -\hat{X}_{UIO} \\ \dot{\hat{a}}_{UIO}(t) \end{bmatrix}}_{u_{aug}} + \underbrace{\begin{bmatrix} n(t) \\ k(t) \end{bmatrix}}_{n_{aug}}$$

$$y^a(t) = \underbrace{\begin{bmatrix} C & \boldsymbol{I} \end{bmatrix}}_{C_{aug}} \underbrace{\begin{bmatrix} X(t) \\ a(t) \end{bmatrix}}_{X_{aug}} + v(t) \qquad (24)$$

where $k(t) = (CN\text{–}\mathbf{I})^{-1}\,(C(\mathbf{I}\text{–}\mathrm{NC})n(t) + (\mathbf{I}\text{–}CN)\dot{v}(t))$. As mentioned before, the attack vector is considered as a new state variable and augmented with the system model. The derived augmented model for case 1 and case 2, can be rewritten as follows:

$$\begin{aligned} \dot{X}_{aug} &= A_{aug}X_{aug} + B_{aug}u_{aug} + n_{aug} \\ y^a(t) &= C_{aug}X_{aug} + v(t) \end{aligned} \qquad (25)$$

where X_{aug}, A_{aug}, B_{aug}, u_{aug}, n_{aug}, and C_{aug} are defined in (24). The discrete-time state-space representation of the above equation can be expressed as follows:

$$\begin{aligned} X_{aug}(k) &= A_d X_{aug}(k-1) + B_d u_{aug}(k-1) + n_{aug}(k-1) \\ y^a(k) &= C_{aug}X_{aug}(k) + v(k) \end{aligned} \qquad (26)$$

where A_d and B_d are the discretized form of matrices A_{aug} and B_{aug}. The KF formulation is applied to (26) for joint estimation of the system states and attack vector using a prediction-correction filtering process as follows [38-40]:

1) *Prediction step*: In this step, the estimation of the state variables and covariance matrix of the estimation error are fulfilled based on the system matrices as follows:

$$\begin{aligned} \hat{X}_{aug}(k|k-1) &= A_d\hat{X}_{aug}(k-1|k-1) + B_d u_{aug}(k-1) \\ P(k|k-1) &= A_d P(k-1|k-1)A_d^T + Q_{aug}(k-1) \end{aligned} \qquad (27)$$

2) *Correction step:* In the correction step, the estimation of the state variables and covariance of the estimation error are fulfilled taking the measurements and obtained priori estimates of the previous step into account as follows:

$$\begin{aligned} K(k) &= P(k|k-1)C_{aug}^T\left[C_{aug}P(k|k-1)C_{aug}^T + R(k)\right]^{-1} \\ \hat{X}_{aug}(k|k) &= \hat{X}_{aug}(k|k-1) + K(k)\left[y^a(k) - C_{aug}\hat{X}_{aug}(k|k-1)\right] \\ P(k|k) &= P(k|k-1) - K(k)C_{aug}P(k|k-1) \end{aligned} \qquad (28)$$

where Q_{aug} and K are the covariance matrix of $n_{aug}(k)$

and the Kalman gain, respectively.

In the following, an analysis is carried out to indicate the disruptive effect of the attacks on the state estimation problem without the utilization of the proposed method, e.g. when the state estimation is fulfilled with only the KF algorithm. Under such conditions, the attack vector is not considered as a state variable and it appears in the output equation as follows:

$$\begin{aligned} X(k) &= AX(k-1) + Bu(k-1) + n(k-1) \\ y^a(k) &= CX(k) + a(k) + v(k) \end{aligned} \tag{29}$$

The estimation of the states at sample k can be obtained considering both system model and measurements as follows:

$$\begin{aligned} &\hat{X}(k|k) = \hat{X}(k|k-1) + K_k\left(y^a(k) - C\hat{X}(k|k-1)\right) \\ &\text{where} \quad \hat{X}(k|k-1) = A\hat{X}(k-1|k-1) + Bu(k-1) \end{aligned} \tag{30}$$

The system measurement vector at sample k can be written as follows:

$$\begin{aligned} y^a(k) &= CX(k) \\ &= C\left(AX(k-1) + Bu(k-1)\right) \quad \text{without attack} \\ y^a(k) &= CX(k) + a(k) \\ &= C\left(AX(k-1) + Bu(k-1)\right) + a(k) \quad \text{with attack} \end{aligned} \tag{31}$$

When there is no attack on the PMUs, the estimated state vector is obtained as follows:

$$\begin{aligned} \hat{X}(k|k) &= A\hat{X}(k-1|k-1) + Bu(k-1) + \\ &\quad K(k)\Big(C\left(AX(k-1) + Bu(k-1)\right) \\ &\qquad - C\left(A\hat{X}(k-1|k-1) + Bu(k-1)\right)\Big) \\ &= A\hat{X}(k-1|k-1) + Bu(k-1) \\ &\quad + K(k)CA\left(X(k-1) - \hat{X}(k-1|k-1)\right) \end{aligned} \tag{32}$$

Assuming the attack is launched at sample k, the estimated state vector in presence of the attack $\hat{X}^a(k)$ is obtained as follows:

$$\begin{aligned} &\hat{X}^a(k|k) \\ &= A\hat{X}(k-1|k-1) + Bu(k-1) + \\ &\quad K(k)\big(C\left(AX(k-1) + Bu(k-1)\right) + a(k) \\ &\qquad - C\left(A\hat{X}(k-1|k-1) + Bu(k-1)\right)\big) \\ &= \underbrace{\hat{X}(k-1|k-1) + Bu(k-1) + K(k)CA\left(X(k-1) - \hat{X}(k-1|k-1)\right)}_{\hat{X}(k|k)} \\ &\quad + \underbrace{K(k)a(k)}_{\text{error term caused by attack}} \end{aligned} \tag{33}$$

As seen in (33), in the presence of the attack, an error term appears in the state estimates results of (33). Similarly, the estimated vector for sample k+1 can be obtained as follows:

$$\begin{aligned} \hat{X}^a(k+1|k+1) &= A\underbrace{\hat{X}^a(k|k)}_{\hat{X}(k|k)+K(k)a(k)} + Bu(k) \\ &\quad + K(k+1)\Big(C\left(AX(k) + Bu(k)\right) + a(k+1) \\ &\qquad - C\Big(A\underbrace{\hat{X}^a(k|k)}_{\hat{X}(k|k)+K(k)a(k)} + Bu(k)\Big)\Big) \\ &= \underbrace{A\hat{X}(k|k) + Bu(k) + K(k+1)CA\left(X(k) - \hat{X}(k|k)\right)}_{\hat{X}(k+1|k+1)} \\ &\quad + \underbrace{AK(k)a(k) - K(k+1)CAK(k)a(k) + K(k+1)a(k+1)}_{\text{error term caused by attack}} \end{aligned} \tag{34}$$

From (33) and (34), it can be easily deduced that the attack may cause inaccuracy or failure of the estimation depending on the nature of the launched attack. If the attack vector includes unbounded entries, the state estimation diverges from the reference state values (the state estimation fails). However, when the attack vector includes only bounded entries, it can result in the inaccuracy or failure of the estimation. Different steps of the proposed method are illustrated in Fig. 1. More details about the KF algorithm and its classical equations can be found in [40-42].

4 Results and Discussions

The proposed method is verified on the IEEE 14-bus and 30-bus test system with five and six synchronous machines, respectively. The dynamic model derived in Section II is used. The machine speeds and angles are considered as the state variables in the proposed method. Moreover, the active powers of the synchronous machines are considered as the system outputs. The values of the parameters for the synchronous generators are presented in Table 1. The resolution of the measurements is considered to be 40 frames per second to effectively mimic the real field conditions. Two different CA scenarios are considered during the tests. The artificially added attack vector takes the following form:

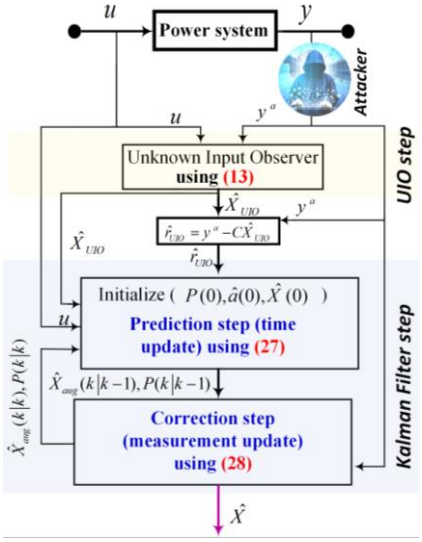

Fig. 1 Flowchart of the proposed approach for secure dynamic state estimation in presence of the CA.

$a(t) = [a_1(t)\ a_2(t)\ \dots\ a_m(t)]^T$
where $a_1(t)$ to $a_m(t)$ (m = 5 for IEEE 14-bus and m = 6 for IEEE 30-bus) are constructed based on the scenarios given in Section 3.2 Different attacks are simulated by changing the entries of $a(t)$. Some of the obtained results are presented and discussed in the following.

In Fig. 2, the state estimation results for the synchronous generator located on bus 2 under CA with two different attack scenarios with and without using the proposed approach are presented. It is assumed that the CAs occur at t = 11 seconds. The attack is constructed by deliberately changing the entries of the attack vector. From Fig. 2, it is seen that the actual system states, state estimates with only the KF algorithm (without utilizing the proposed approach), and the state estimates with the proposed approach are nearly matched before the occurrence of the attack. Upon the occurrence of the attack at t = 11 seconds, it is observed that the estimated states with the KF diverge. However, the state estimations with the proposed approach successfully converge to the actual system states after a short period of time. In both attack scenarios, the frequency and angle of the synchronous machine are accurately estimated.

To assess the performance of the proposed method more effectively, the average root-mean-square error (RMSE) for different simulation cases during the first five seconds after the occurrence of the attack is calculated using the following formula:

$$RMSE_{x_i} = \frac{\sum_{j=1}^{N_T}\left(\left(\sum_{k=1}^{N_s}\left(x_i(k)-\hat{x}_i(k)\right)^2\right)/N_s\right)_j}{N_T} \quad (35)$$

where N_T is the number of simulated test cases and N_s is the number of samples in each simulated test case. A total number of 29 different CA test cases are analyzed. The results are summarized in Fig. 3. It is observed that the proposed method successfully removes the disruptive effect of the attack on the state estimation while the state estimation error is favorably low.

To effectively examine the performance of the proposed estimator, the estimation error covariance is numerically solved in MATLAB considering standard noise levels in the power system based on ANSI C89.2, IEEE C37.118.1, and IEEE 656-2018. Based on these standards, measurement noises with Signal to Noise Ratio (SNR) of 30 dB is considered for the analysis. The results for IEEE 14-bus and 30-bus test systems are shown in Fig. 4. In Fig. 4, the variances of the estimation error (diagonal entries of the estimation error covariance matrix) when the proposed approach is used for dynamic state estimation are provided. Overall, it can be seen that all variances approach zero, which means that we have increasingly more confidence in our estimates as we obtain more measurements [29]. Thus, the filter is stable and state estimation results are reliable.

Table. 1 Generator data for IEEE test systems.

Parameter [*p.u.*]	Gen #1	Gen #2	Gen #3	Gen #4	Gen #5	Gen #6
x_d	0.2995	0.185	0.185	0.232	0.232	0.232
M	0.027	0.034	0.034	0.026	0.026	0.026
D	2	2	2	2	2	2

Generators 1 to 5 are used for IEEE 14-bus test system and generators 1 to 6 are used for IEEE 30-bus test system. For all cases, S_{base} = 100 MVA and f_{syn} = 60 Hz are considered.

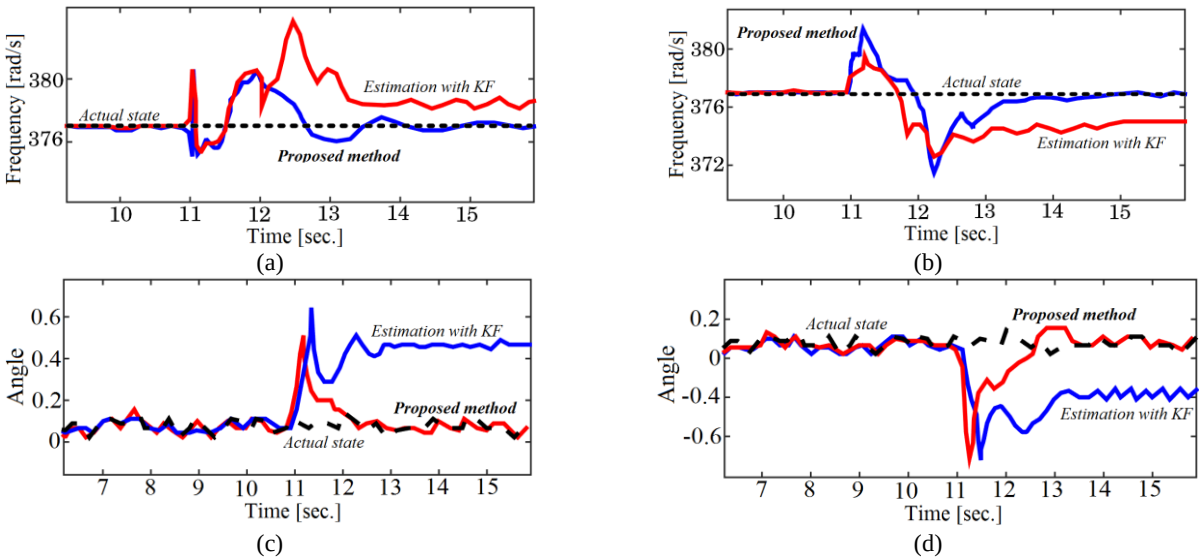

Fig. 2 The state estimation results (actual states, estimated states with KF only, and estimated states with the proposed method) for the synchronous generator located at bus #2 when a CA occures at t = 11 seconds. a) Frequency of the generator under CA with the first attack scenario, b) Angle of the generator under CA with the first attack scenario, c) Frequency of the generator under CA with the second attack scenario, and d) Angle of the generator under CA with the second attack scenario.

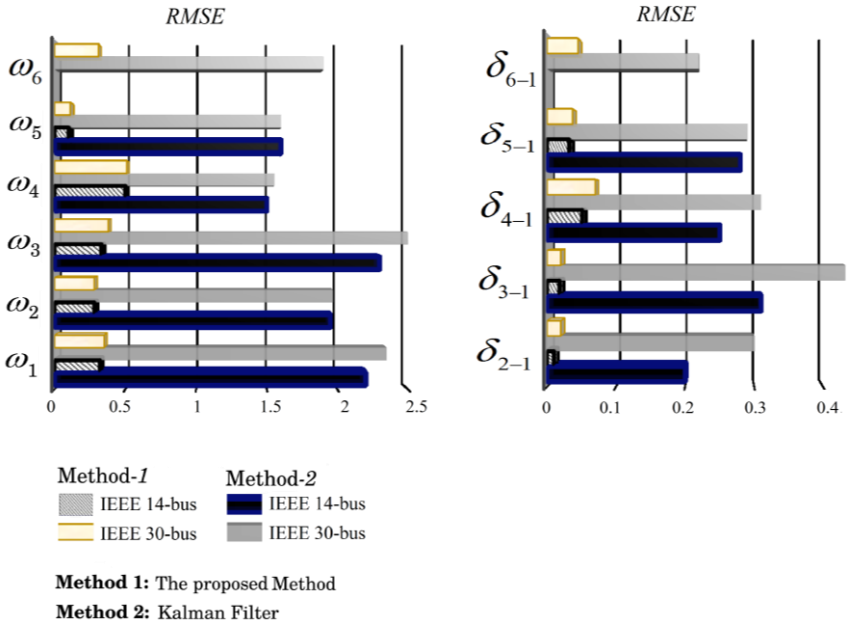

Fig. 3 Average RMSE values for different system states in the IEEE 14-bus and IEEE 30-bus test systems.

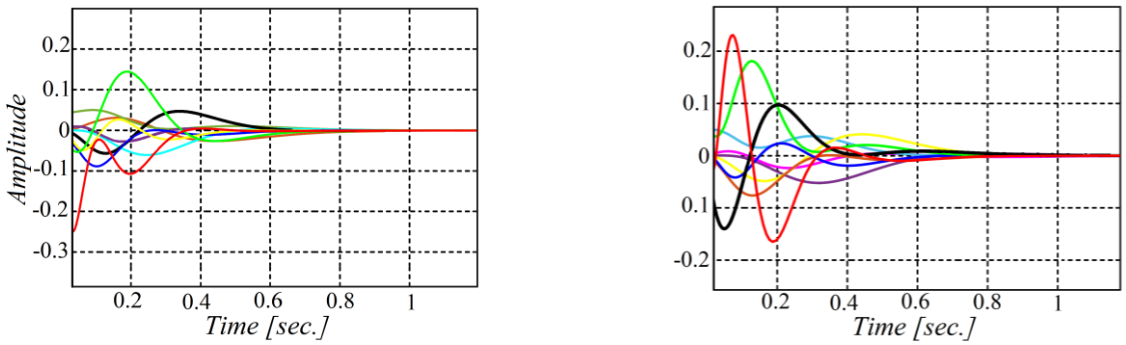

Fig. 4 Variances of the estimation error when the proposed method is used for state estimation with SNR of 30 dB; a) Variances of the estimation error related to the frequencies and angles of generators 1 to 5 for IEEE 14-bus test system and b) Variances of the estimation error related to the frequencies and angles of generators 1 to 6 for IEEE 30-bus test system.

5 Concluding Remarks and Future Work

With the extension of cyberinfrastructures in modern smart grids, the cybersecurity importance becomes substantially high. In such systems, the CAs may be launched by adversaries with the aim of manipulating the sensory measurements by injecting false data, which leads to the degradation of the performance of the system state estimators. Remarkably, the conventional bad data detectors and KF-based estimators are not able to tackle this problem. In this paper, the traditional KF-based dynamic state estimator is enhanced by incorporating the dynamics of the attack vector into the system state-space model. The dynamics of the attack are derived in a pre-processing stage using UIO. With the proposed method, in each iteration of the filtering process, the estimations of the attack vector become available along with the estimations of the system states. In addition, the overall estimation accuracy is increased compared to the case where only the KF algorithm is used. The effectiveness of the proposed method is demonstrated by testing it on two typical CPSs, namely IEEE 14-bus and 30-bus test systems.

In this work, the proposed approach is tested considering a simple and linear synchronous generator model, which is not capable of tracking the system dynamics when the power flow changes. To tackle this problem, the polytopic model of the system that captures different linearized portions corresponding to various loading conditions (power flow conditions) for different time-periods can be used. For future work, it would also be worthwhile to enhance the proposed approach for nonlinear state estimation with, for example, EKF, UKF, or Cubatur KF (CKF) algorithms.

Appendix

In Section II.B, matrices $Z \in \mathbb{R}^{n\times n}$ and $D \in \mathbb{R}^{n\times n}$ in matrix $A \in \mathbb{R}^{2n\times 2n}$ are derived as follows:

$$Z=\left[\begin{array}{c|c|c|c} -\frac{1}{M_1}\sum_{j=2}^{n}|E_1||E_j|\hat{B}_{1j} & \frac{1}{M_1}|E_1||E_2|\hat{B}_{12} & \cdots & \frac{1}{M_1}|E_1||E_n|\hat{B}_{1n} \\ \hline \frac{1}{M_2}|E_2||E_1|\hat{B}_{21} & -\frac{1}{M_2}\sum_{j=1,j\neq 2}^{n}|E_2||E_j|\hat{B}_{2j} & \cdots & \frac{1}{M_2}|E_2||E_n|\hat{B}_{2n} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline \frac{1}{M_n}|E_n||E_1|\hat{B}_{n1} & \frac{1}{M_n}|E_n||E_2|\hat{B}_{n2} & \cdots & -\frac{1}{M_n}\sum_{j=1}^{n-1}|E_n||E_j|\hat{B}_{nj} \end{array}\right], D=\operatorname{diag}\left(\frac{-D_1}{M_1},\cdots,\frac{-D_i}{M_i},\cdots,\frac{-D_n}{M_n}\right)$$

In (11), $S \in \mathbb{R}^{n\times(n-1)}$ and $H \in \mathbb{R}^{n\times(n-1)}$ are derived as follows:

$$S=\left[\begin{array}{c|c|c|c} -\frac{1}{M_1}|E_1||E_2|\hat{B}_{12} & -\frac{1}{M_1}|E_1||E_3|\hat{B}_{13} & \cdots & -\frac{1}{M_1}|E_1||E_n|\hat{B}_{1n} \\ \hline \frac{1}{M_2}\sum_{j=1,j\neq 2}^{n}|E_2||E_j|\hat{B}_{2j} & -\frac{1}{M_2}|E_2||E_3|\hat{B}_{23} & \cdots & -\frac{1}{M_2}|E_2||E_n|\hat{B}_{2n} \\ \hline -\frac{1}{M_3}|E_3||E_1|\hat{B}_{31} & \frac{1}{M_3}\sum_{j=1,j\neq 3}^{n}|E_3||E_j|\hat{B}_{3j} & \cdots & -\frac{1}{M_3}|E_3||E_n|\hat{B}_{3n} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline -\frac{1}{M_n}|E_n||E_1|\hat{B}_{n1} & -\frac{1}{M_n}|E_n||E_2|\hat{B}_{n2} & \cdots & \frac{1}{M_n}\sum_{j=1}^{n-1}|E_n||E_j|\hat{B}_{nj} \end{array}\right]$$

$$H=\left[\begin{array}{c|c|c|c} |E_1||E_2|\hat{B}_{12} & |E_1||E_3|\hat{B}_{13} & \cdots & |E_1||E_n|\hat{B}_{1n} \\ \hline -\sum_{j=1,j\neq 2}^{n}|E_2||E_j|\hat{B}_{2j} & |E_2||E_3|\hat{B}_{23} & \cdots & |E_2||E_n|\hat{B}_{2n} \\ \hline |E_3||E_1|\hat{B}_{31} & -\sum_{j=1,j\neq 3}^{n}|E_3||E_j|\hat{B}_{3j} & \cdots & |E_3||E_n|\hat{B}_{3n} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline |E_n||E_1|\hat{B}_{n1} & |E_n||E_2|\hat{B}_{n2} & \cdots & -\sum_{j=1}^{n-1}|E_n||E_j|\hat{B}_{nj} \end{array}\right]$$

The elementary row and column operations for obtaining (21) are included in (A.1). In (A.1), c_i denote the i-th column of matrix $s\boldsymbol{I}-A$. In addition, matrices Ω, Γ, and Σ in (21) are also derived as presented in (A.2).

$$\det\left(s\mathbf{I}-A\right)=\det\left(\left[\begin{array}{c|c} s\mathbf{I}^{(n-1)\times(n-1)}-\mathbf{0}^{(n-1)\times(n-1)} & \overbrace{\begin{matrix}-1 & 1 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ -1 & 0 & \cdots & 1\end{matrix}}^{(n-1)\times n} \\ \hline -S^{\,n\times(n-1)} & \underbrace{\begin{matrix}s+\frac{D_1}{M_1} & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & s+\frac{D_n}{M_n}\end{matrix}}_{n\times n} \end{array}\right]\right)$$

$$\xrightarrow[\substack{c_i+c_{n+i}\to c_{n+i}\\ i=1,\ldots,n-1}]{\substack{c_n+\ldots+c_{2n-1}\to c_n\\ -s\times c_{n+i}\to c_{n+i}}} \frac{1}{(-s)^{n-1}}\det\left(\left[\begin{array}{c|c} s\mathbf{I}^{(n-1)\times(n-1)} & \mathbf{0}^{(n-1)\times n} \\ \hline -S^{\,n\times(n-1)} & \Omega^{n\times n} \end{array}\right]\right)=\frac{1}{s^{n-1}}\underbrace{\det\left(s\mathbf{I}^{(n-1)\times(n-1)}\right)}_{s^{n-1}}\det(\Omega)=\det(\Omega) \qquad \text{(A.1)}$$

$$\Omega=\begin{bmatrix} s+\frac{D_1}{M_1} & \frac{1}{M_1}|E_1||E_2|\hat{B}_{12} & \frac{1}{M_1}|E_1||E_3|\hat{B}_{13} & \cdots & \frac{1}{M_1}|E_1||E_n|\hat{B}_{1n} \\ s+\frac{D_2}{M_2} & -\frac{1}{M_2}\sum_{j=1,j\neq 2}^{n}|E_2||E_j|\hat{B}_{2j}-s\left(s+\frac{D_2}{M_2}\right) & \frac{1}{M_2}|E_2||E_3|\hat{B}_{23} & \cdots & \frac{1}{M_2}|E_2||E_n|\hat{B}_{2n} \\ s+\frac{D_3}{M_3} & \frac{1}{M_3}|E_3||E_1|\hat{B}_{31} & -\frac{1}{M_3}\sum_{j=1,j\neq 3}^{n}|E_3||E_j|\hat{B}_{3j}-s\left(s+\frac{D_3}{M_3}\right) & \cdots & \frac{1}{M_3}|E_3||E_n|\hat{B}_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s+\frac{D_n}{M_n} & \frac{1}{M_n}|E_n||E_1|\hat{B}_{n1} & \frac{1}{M_n}|E_n||E_2|\hat{B}_{n2} & \cdots & -\frac{1}{M_n}\sum_{j=1}^{n-1}|E_n||E_j|\hat{B}_{nj}-s\left(s+\frac{D_n}{M_n}\right) \end{bmatrix}$$

$$\Gamma^{(n-1)\times n}=\begin{bmatrix} -1 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & 0 & \cdots & 1 \end{bmatrix},\ \Sigma^{n\times n}=\operatorname{diag}\left(s+\frac{D_1}{M_1},\ldots,s+\frac{D_i}{M_i},\ldots,s+\frac{D_n}{M_n}\right) \tag{A.2}$$

The equations related to the observability of pair (*C*, *A*) in Definition 3 are obtained as follows

$$\operatorname{rank}\begin{bmatrix} s\mathbf{I}-A \\ C \end{bmatrix}=\operatorname{rank}\begin{bmatrix} s\mathbf{I}^{(n-1)\times(n-1)}-\mathbf{0}^{(n-1)\times(n-1)} & \Gamma^{(n-1)\times n} \\ -S^{\,n\times(n-1)} & \Sigma^{n\times n} \\ H^{\,n\times(n-1)} & \mathbf{0}^{n\times n} \end{bmatrix}$$

Based on Definition 3, if there exist 2*n*–1 linear independent vectors in column or row space of the above matrix, the rank of the above matrix is *2n-1* and observability of the (*C*, *A*) pair is proved. A combination of the linearly independent vectors can be written as follows:

$$\left(\overbrace{r_{2(C)},\ldots,r_{n(C)}}^{n-1},\overbrace{r_{n(s\mathbf{I}-A)},\ldots,r_{2n-1(s\mathbf{I}-A)}}^{n}\right)$$

where $r_i(c)$ is *i*-th row of the matrix *C* and $r_i(s\mathbf{I}–A)$ is *i*-th row of the matrix ($s\mathbf{I}$-*A*).

References

[1] B. Liscouski and W. Elliot, "Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations," *A Report to US Department of Energy*, Vol. 40, No. 4, p. 86, 2004.

[2] D. U. Case, "Analysis of the cyber attack on the Ukrainian power grid," *Electricity Information Sharing and Analysis Center*, 2016.

[3] J. Beiza, S. H. Hosseinian, and B. Vahidi. "Fault type estimation in power systems," *Iranian Journal of Electrical and Electronic Engineering*, Vol. 5, No. 3, pp. 185–195, 2009.

[4] T. Ghanbari, E. Farjah, and F. Naseri, "Three-phase resistive capacitor switching transient limiter for mitigating power capacitor switching transients," *IET Generation, Transmission & Distribution*, Vol. 10, No. 1, pp. 142–153, 2016.

[5] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, Vol. 14, No. 1, p. 13, 2011.

[6] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey," *IEEE Transactions on Industrial Informatics*, Vol. 13, No. 2, pp. 411–423, 2017.

[7] Z. Kazemi, A. A. Safavi, S. Pouresmaeeli, and F. Naseri. "A practical framework for implementing multivariate monitoring techniques into distributed control system," *Control Engineering Practice*, Vol. 82, pp. 118–129, 2019.

[8] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, Vol. 8, No. 4, pp. 1630–1638, 2017.

[9] Z. Zhao, and G. Chen, "An Overview of Cyber Security for Smart Grid," *IEEE International Symposium on Industrial Electronics*, pp. 1127–1131, 2018.

[10] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of local false data injection attacks with reduced network information," I*EEE Transactions on Smart Grid*, Vol. 6, No. 4, pp. 1686–1696, 2015.

[11] V. Kekatos, G. B. Giannakis, and R. Baldick, "Grid topology identification using electricity prices," in *PES General Meeting| Conference & Exposition*, pp. 1–5, 2014.

[12] G. Hug, and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, Vol. 3, No. 3, pp. 1362–1370, 2012.

[13] L. Jia, J. Kim, R. J. Thomas, and L. Tong, "Impact of data quality on real-time locational marginal price," *IEEE Transactions on Power Systems*, Vol. 29, No. 2, pp. 627–636, 2014.

[14] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Transactions on Smart Grid*, Vol. 5, No. 3, pp. 1216–1227, 2014.

[15] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Transactions on Industrial Informatics*, Vol. 13, No. 1, pp. 198–207, 2017.

[16] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," in *IEEE symposium on Security and Privacy*, pp. 259–271, 2004.

[17] S. Li, Y. Yılmaz, and X. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Transactions on Smart Grid*, Vol. 6, No. 6, pp. 2725–2735, 2015.

[18] H. Salehghaffari and F. Khorrami, "Resilient power grid state estimation under false data injection attacks," in *IEEE Power & Energy Society Innovative Smart Grid Technologies Conference*, pp. 1–5, 2018.

[19] Y. Chakhchoukh and H. Ishii, "Enhancing robustness to cyber-attacks in power systems through multiple least trimmed squares state estimations," *IEEE Transactions on Power Systems*, Vol. 31, No. 6, pp. 4395–4405, 2016.

[20] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Transactions on Smart* Grid, Vol. 8, No. 5, pp. 2505–2516, 2017.

[21] F. Naseri, E. Farjah, Z. Kazemi, E. Schaltz, T. Ghanbari, and J. Schanen, "Dynamic stabilization of DC traction systems using a supercapacitor-based active stabilizer with model predictive control," *IEEE Transactions on Transportation Electrification*, Vol. 6, No. 1, pp. 228–240, 2020.

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

[23] R. Chen, X. Li, H. Zhong, and M. Fei, "A novel online detection method of data injection attack against dynamic state estimation in smart grid," *Neurocomputing*, Vol. 344, pp. 73–81, 2019.

[24] J. Zhao, M. Netto and L. Mili, "A robust iterated extended kalman filter for power system dynamic state estimation," *IEEE Transactions on Power Systems*, Vol. 32, No. 4, pp. 3205–3216, 2017.

[25] Y. Nakahira and Y. Mo, "Attack-resilient H_2, H_∞, and l_1 state estimator," *IEEE Transactions on Automatic Control*, Vol. 63, No. 12, pp. 4353–4360, 2018.

[26] P. M. Anderson and A. A. Fouad, *Power system control and stability*. John Wiley & Sons. 2008.

[27] J. Chen and R. J. Patton, *Robust model-based fault diagnosis for dynamic systems*. Vol. 3, Springer Science & Business Media, 2012.

[28] Z. Kazemi, A. A. Safavi, F. Naseri, L. Urbas, and P. Setoodeh, "A secure hybrid dynamic state estimation approach for power systems under false data injection attacks," *IEEE Transactions on Industrial Informatics*, 2020.

[29] D. Simon, *Optimal state estimation: Kalman, H infinity, and nonlinear approaches*. John Wiley & Sons, 2006.

[30] Q. Huang, L. Shao, and N. Li, "Dynamic detection of transmission line outages using hidden Markov models," *IEEE Transactions on Power Systems*, Vol. 31, No. 3, pp. 2026–2033, 2015.

[31] E. Ghahremani and I. Kamwa, "Local and wide-area PMU-based decentralized dynamic state estimation in multi-machine power systems," *IEEE Transactions on Power Systems*, Vol. 31, No. 1, pp.547–562, 2015.

[32] Y. Yu, Z. Wang, and C. Lu, "A joint filter approach for reliable power system state estimation," in *IEEE Transactions on Instrumentation and Measurement*, Vol. 68, No. 1, pp. 87–94, Jan. 2019.

[33] M. Brown, M. Biswal, S. Brahma, S. J. Ranade, and H. Cao, "Characterizing and quantifying noise in PMU data," *IEEE Power and Energy Society General Meeting (PESGM)*, Boston, MA, pp. 1–5, 2016.

[34] G. Frigo, A. Derviškadić, A. Bach, and M. Paolone, "Statistical model of measurement noise in real-world PMU-based acquisitions," in *International Conference on Smart Grid Synchronized Measurements and Analytics (SGSMA)*, College Station, TX, USA, pp. 1–8, 2019.

[35] J. Zhao and L. Mili, "Robust unscented kalman filter for power system dynamic state estimation with unknown noise statistics*," IEEE Transactions on Smart Grid*, Vol. 10, No. 2, pp. 1215–1224, 2019.

[36] Y. Li, J. Li, J. Qi, and L. Chen, "Robust cubature kalman filter for dynamic state estimation of synchronous machines under unknown measurement noise statistics," *IEEE Access*, Vol. 7, pp. 29139–29148, 2019.

[37] J. Zhao and L. Mili, "A decentralized H-infinity unscented kalman filter for dynamic state estimation against uncertainties," *IEEE Transactions on Smart Grid*, Vol. 10, No. 5, pp. 4870–4880, Sep. 2019.

[38] F. Naseri, Z. Kazemi, M. M. Arefi, and E. Farjah, "Fast discrimination of transformer magnetizing current from internal faults: An extended Kalman filter-based approach," I*EEE Transactions on Power Delivery*, Vol. 33, No. 1, pp. 110–118, 2017.

[39] F. Naseri, E. Farjah, and T. Ghanbari, "KF-based estimation of diode turn-off power loss using datasheet information," Electronics Letters, 2019.

[40] F. Naseri, E. Farjah, T. Ghanbari, Z. Kazemi, E. Schaltz, and J. L. Schanon, "Online parameter estimation for supercapacitor state-of-energy and state-of-health determination in vehicular applications," *IEEE Transactions on Industrial Electronics*, 2019.

[41] F. Naseri, Z. Kazemi, E. Farjah, and T. Ghanbari, "Fast detection and compensation of current transformer saturation using extended kalman filter," *IEEE Transactions on Power Delivery*, Vol. 34, No. 3, pp. 1087–1097, 2019.

[42] T. Ghanbari, E. Farjah, F. Naseri, N. Tashakor, H. Givi, and R. Khayam. "Solid-state capacitor switching transient limiter based on kalman filter algorithm for mitigation of capacitor bank switching transients," *Renewable and Sustainable Energy Reviews*, Vol. 90, pp. 1069–1081, 2018.

Z. Kazemi received the B.Sc. degree in Electrical Engineering from Shiraz University of Technology, Shiraz, Iran, in 2013, and the M.Sc. degree in Control Engineering from Shiraz University, Shiraz, Iran, in 2015. She is currently a Ph.D. candidate in Control Engineering at Shiraz University in Iran. Her research interests include system identification and modeling, state estimation, industrial control and automation, fault detection and fault diagnosis, and cyber-physical systems.

A. A. Safavi received his B.Sc. degree in Electrical Engineering from Shahid Chamran University, Iran, in 1987, and his M.Sc. degree in Control Engineering from the University of NSW, Australia, in 1992. His Ph.D. in Process Systems Engineering was completed at Sydney University in 1995. In 1996, he was a Postdoctoral fellow at Sydney University. He joined Shiraz University in 1997. He is currently a Professor in the School of Electrical and Computer Engineering at Shiraz University in Iran. His research interests are model predictive control, wavelets, neural networks, system identification, networked-based control, and information technology, IIoT, and Industry 4.0. See http://safavi.home.shirazu.ac.ir/, http://linkedin.com/in/ali-akbar-safavi-90451039.