A Two-stage Kalman Filter for Cyber-attack Detection in Automatic Generation Control System

Ayyarao S. L. V. Tummala and Ravi Kiran Inapakurthi

***Abstract*—Communication plays a vital role in incorporating smartness into the interconnected power system. However, historical records prove that the data transfer has always been vulnerable to cyber-attacks. Unless these cyber-attacks are identified and cordoned off, they may lead to black-out and result in national security issues. This paper proposes an optimal two-stage Kalman filter (OTS-KF) for simultaneous state and cyber-attack estimation in automatic generation control (AGC) system. Biases/cyber-attacks are modeled as unknown inputs in the AGC dynamics. Five types of cyber-attacks, i.e., false data injection (FDI), data replay attack, denial of service (DoS), scaling, and ramp attacks, are injected into the measurements and estimated using OTS-KF. As the load variations of each area are seldom available, OTS-KF is reformulated to estimate the states and outliers along with the load variations of the system. The proposed technique is validated on the benchmark two-area, three-area, and five-area power system models. The simulation results under various test conditions demonstrate the efficacy of the proposed filter.**

***Index Terms*—Cyber-security, automatic generation control (AGC), load frequency control, false data injection, cyber-attack detection.**

I. Introduction

POWER system is monitored and controlled by supervisory control and data acquisition (SCADA) and energy management system (EMS). However, the large-scale integration of renewable energy systems, the development of microgrids, i.e., load-side or localized generation, and the increasing size of power systems deteriorate the flexibility and reliability of power systems, in spite of being positive indicators of an economy. The inclusion of communication links in the power system brings smartness and provides reliable and real-time data acquisition, which results in effective power transmission [1], [2]. Smart grids are essential for improving the flexibility and reliability. In addition, communication systems help the power system in deregulation, which facilitates the energy market to be efficient. However, owing to the usage of internet connectivity, the power system is susceptible to cyber-attacks. Cyber-attack is one of the greatest challenges that destabilizes the economic development of nations. In the event of a cyber-attack, the transmitted data is either corrupted or blocked, which leads to huge financial losses and creates chaos in the power system. Several events of cyber-attacks on the power system are recorded in history [3]. Cyber-attacks on dynamic state estimation, automatic generation control (AGC), electricity market crisis, and stability and security issues are some of the examples of cyber-attacks in the power system [4]-[9]. The idea of cyber-attack is illustrated in Fig. 1, where the hacker attacks the communication system, injects false data, and misguides the centralized monitoring and control system. It is possible to hack communication data at various levels such as weather prediction, generation, load scheduling, etc.

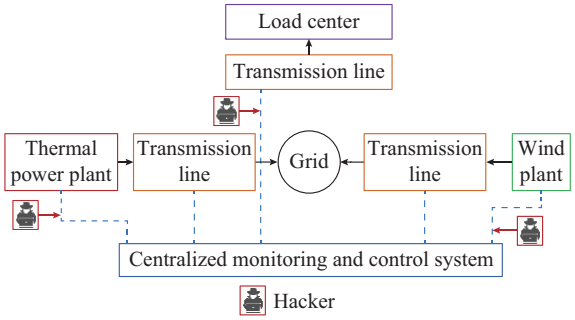

Fig. 1. Illustration of cyber-attacks on power system.

Cyber-attacks are classified into false data injection (FDI), data replay attack (DRA), denial of service (DoS) attack, scaling attack, ramp attack, man-in-the-middle attack, intelligent attack, etc. This paper mainly focuses on the detection of FDI, DRA, DoS, scaling, and ramp attacks. In case of an FDI attack, the intruder adds false data to the actual data. This results in improper generation due to the faulty operation of governor valve. In addition, the manipulated data may be perceived as sudden generation or load loss by the energy traders that lures them towards either fresh positions or clear positions. Hence, hackers destabilize the energy trading system. Further, renewable energy data can be manipulated and alter the renewable energy certificate (REC) trading mechanism. Similarly, in the case of DRA, the intruder injects previous event data and confuses the monitoring system, with similar effects to FDI attack. Lastly, if the communication between the measuring device and the control center is lost, the data being sent are absent during the jam peri-

Manuscript received: October 25, 2019; revised: July 14, 2020; accepted: December 3, 2020. Date of CrossCheck: December 3, 2020. Date of online publication: February 9, 2021.

A. S. L. V. Tummala (corresponding author) is with the GMR Institute of Technology, Rajam, Srikakulam, Andhra Pradesh, India (e-mail: ayyarao.tummala@gmail.com).

R. K. Inapakurthi is with the Raghu Engineering College, Dakamarri, Visakhapatnam, Andhra Pradesh, India (e-mail: ravithebhagat@gmail.com).

DOI: 10.35833/MPCE.2019.000119

od, which happens in the case of DoS attack. Even though several measures are taken to avoid these cyber-attacks, advanced hacking systems have been developed. Hence, the manipulated/jammed data must be detected, and proper corrective measures are to be taken to mitigate serious issues in the smart grid.

AGC is a mechanism for regulating the load frequency in power systems by transmitting the data of frequency and tie-line power deviations using communication channel IEC 6150. A control signal that regulates the position of governor valve is developed based on area control error in the centralized control unit, and is transmitted to each generation unit. When the intruder attacks the AGC, it may lead to frequency instability as well as financial loss. The intrusion detection in power system is broadly classified into three categories. The first category is based on model-based intrusion detection. In this method, an observer is designed based on the power system model, which is useful for the cyber-attack detection in power systems [10]-[14]. The second category is based on machine learning techniques through which the intrusion detection is achieved [15]-[18]. Likewise, the last category is a hybrid method, which is a combination of model-based method and artificial intelligence [19], [20]. A combination of residue and forecasting error is applied in [19] for the detection of data manipulation. The cyber-attacks on the AGC system are modeled as unknown inputs and are estimated using an unknown input observer in [21]. The proposed method has a promising performance with smaller load forecasting error. However, in the case of large errors in load or renewable energy forecasting, the performance of this method is compromised. A stochastic unknown-input observer-based intrusion detection technique is proposed in [22]. The residue of the Kalman filter is a useful tool in estimating cyber-attacks. Cyber-attacks are identified if the residue is higher than the threshold [10]. However, it is quite tedious to select an optimal threshold under load disturbances. The detection based on dynamic watermarking algorithm is proposed in [23]. A game-theory approach for the identification of intrusion is proposed in [24]. In [25], a graphical approach is proposed to identify vulnerable networks prone to the cyber-attacks, and to sectionalize them to avoid any global effect due to any local manipulations. In [26], a large-scale power system is linearized and a two-stage estimator is proposed to deal with the scalable state estimation of the complex non-linear system when the measurement data are abundant but cannot be trusted.

Statistical methods are ineffective in detecting coordinated cyber-attacks and/or when the attacker has full knowledge of the system dynamics. Machine-learning-based detection has two major challenges. The first is that these algorithms cannot quantify the cyber-attacks. The second is that the performance of these methods may be severely affected in the presence of measurement noise. Further, for effective cyber-attack detection and mitigation, real-time load data are required, which may not be feasible due to the load uncertainties. In the absence of accurate load data, the detection relies on load forecasting data, and hence, the errors in load forecasting may adversely affect the performance of the detection process.

Kalman filter is a powerful means for estimating the states of the power system in a noisy environment. Owing to its advantages, many variants of the Kalman filter have been developed in the literature. However, its performance deteriorates when an accurate plant model is not available or when there exists bias or failure of the sensor. The optimal two-stage Kalman filter (OTS-KF) is a variant of the Kalman filter for estimating the states even in the presence of random bias [27]. In this paper, an OTS-KF is proposed for cyber-attack detection, which is reformulated to suit cyber-attack detection and mitigation in a multi-area power system. The cyber-attacks are considered as unknown inputs in the dynamic model. An OTS-KF is designed for estimating the states and cyber-attacks on the power system. The OTS-KF is a two-stage algorithm in which state estimation and bias estimation filters run in parallel. Kalman filter based bias estimation algorithms in the literature assume the load variations in each area to be measurable. However, because of the integration of renewable energy systems into the power system, the net load variations affecting the load frequency are seldom available [28]. Hence, the load variations are considered as unknown inputs and a modified OTS-KF algorithm is developed. The proposed technique is validated for five types of cyber-attacks on the benchmark two-area, three-area, and five-area power system models.

The major contributions of this paper are as follows.

1) This paper proposes an OTS-KF for cyber-attack detection on the AGC system. In the first stage, the states are estimated under bias-free (attack-free) condition; while in the second stage, the biases (attacks) are estimated.

2) Because of the integration of small- and medium-scale renewable energy systems into the power system, there is a huge gap between functional planning and operations. As a result, continuous load monitoring is challenging. The load fluctuations are considered as new unknown inputs.

3) The proposed OTS-KF is modified to estimate net demand and cyber-attacks.

4) The performance of the proposed OTS-KF is evaluated for various cyber-attacks such as FDI, DRA, DoS, scaling, and ramp attacks.

The remainder of this paper is organized as follows. Section II briefly introduces the modeling of AGC with cyber-attack. Section III elaborates on various types of cyber-attacks and their detection using a two-stage Kalman filter algorithm. Section IV describes the application of OTS-KF in cyber-attack estimation with and without load measurement. Section V details the simulation results for various types of cyber-attacks. Finally, concluding remarks are given in Section VI.

II. System Modeling

The power system is highly nonlinear and distributed where the load frequency is regulated by using AGC. For the design of the controller, power system dynamics are linearized at an operation point. The linearized model of a two-area power system is considered as a plant to design the proposed filter.

The plant dynamics are shown in (1)-(9), and the dynamics of the AGC are represented in the state-space form [18],

[19] as (10) and (11).

$$\Delta\dot{f}_1(t)=-\frac{D_1}{2H_1}\Delta f_1(t)+\frac{1}{2H_1}\Delta P_{g1}(t)-\frac{1}{2H_1}u_1(t)-\frac{1}{2H_1}\Delta P_{12}(t) \tag{1}$$

$$\Delta\dot{P}_{g1}(t)=-\frac{1}{T_{T1}}\Delta P_{g1}(t)+\frac{1}{T_{T1}}\Delta X_{g1}(t) \tag{2}$$

$$\Delta\dot{X}_{g1}(t)=-\frac{1}{R_1T_{G1}}\Delta f_1(t)-\frac{1}{T_{G1}}\Delta X_{g1}(t)+\frac{1}{T_{G1}}ACE_1(t) \tag{3}$$

$$A\dot{C}E_1(t)=-K_{I1}B_1\Delta f_1(t)-K_{I1}\Delta P_{12}(t) \tag{4}$$

$$\Delta\dot{f}_2(t)=-\frac{D_2}{2H_2}\Delta f_2(t)+\frac{1}{2H_2}\Delta P_{g2}(t)-\frac{1}{2H_2}u_2(t)+\frac{1}{2H_2}\Delta P_{12}(t) \tag{5}$$

$$\Delta\dot{P}_{g2}(t)=-\frac{1}{T_{T2}}\Delta P_{g2}(t)+\frac{1}{T_{T2}}\Delta X_{g2}(t) \tag{6}$$

$$\Delta\dot{X}_{g2}(t)=-\frac{1}{R_2T_{G2}}\Delta f_2(t)-\frac{1}{T_{G2}}\Delta X_{g2}(t)+\frac{1}{T_{G2}}ACE_2(t) \tag{7}$$

$$A\dot{C}E_2(t)=-K_{I2}B_2\Delta f_2(t)+K_{I2}\Delta P_{12}(t) \tag{8}$$

$$\Delta\dot{P}_{12}(t)=P_s\Delta f_1(t)-P_s\Delta f_2(t) \tag{9}$$

$$\dot{\boldsymbol{x}}=\boldsymbol{A}_o\boldsymbol{x}+\boldsymbol{B}_o\boldsymbol{u}+\boldsymbol{w} \tag{10}$$

$$\boldsymbol{y}=\boldsymbol{C}\boldsymbol{x}+\boldsymbol{v} \tag{11}$$

where $\boldsymbol{x}=\left[\Delta f_1\ \Delta P_{g1}\ \Delta X_{g1}\ ACE_1\ \Delta f_2\ \Delta P_{g2}\ \Delta X_{g2}\ ACE_2\ \Delta P_{12}\right]^{\mathrm{T}}$; $\boldsymbol{u}=\left[u_1\ \ u_2\right]^{\mathrm{T}}$; $\boldsymbol{y}=\left[\Delta P_{12}(t)\ \ \Delta f_1(t)\ \ \Delta f_2(t)\right]^{\mathrm{T}}$; $\boldsymbol{A}_o=$

$$\begin{bmatrix}
-\frac{D_1}{2H_1} & \frac{1}{2H_1} & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{2H_1} \\
0 & -\frac{1}{T_{T1}} & \frac{1}{T_{T1}} & 0 & 0 & 0 & 0 & 0 & 0 \\
-\frac{1}{R_1T_{G1}} & 0 & -\frac{1}{T_{G1}} & \frac{1}{T_{G1}} & 0 & 0 & 0 & 0 & 0 \\
-K_{I1}B_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -K_{I1}B_1 \\
0 & 0 & 0 & 0 & -\frac{D_2}{2H_2} & \frac{1}{2H_2} & 0 & 0 & \frac{1}{2H_2} \\
0 & 0 & 0 & 0 & 0 & -\frac{1}{T_{T2}} & \frac{1}{T_{T2}} & 0 & 0 \\
0 & 0 & 0 & 0 & -\frac{1}{R_2T_{G2}} & 0 & -\frac{1}{T_{G2}} & -\frac{1}{T_{G2}} & 0 \\
0 & 0 & 0 & 0 & -K_{I2}B_2 & 0 & 0 & 0 & K_{I2}B_2 \\
P_s & 0 & 0 & 0 & -P_s & 0 & 0 & 0 & 0
\end{bmatrix};$$

$$\boldsymbol{B}_0=\begin{bmatrix}
-\frac{1}{2H_1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -\frac{1}{2H_2} & 0 & 0 & 0 & 0
\end{bmatrix}^{\mathrm{T}};\qquad \boldsymbol{C}=\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0
\end{bmatrix};$$

Δf_i is the change in frequency; ΔP_{gi} is the change in power output of generator; ΔX_{gi} is the change in valve position of governor; ACE_i is the area control error; ΔP_{12} is the line power deviation; u_i is the change in load demand; T_{Ti} is the time constant of turbine; T_{Gi} is the time constant of governor; B_i is the frequency bias factor; R_i is the speed regulation coefficient; P_s is the synchronizing power coefficient; K_{Ii} is the integral control constant; H_i is the inertia; D_i is the frequency sensitivity load coefficient; $i=1, 2$; $\boldsymbol{x}$ is the state vector; $\boldsymbol{y}$ is the measurement vector; $\boldsymbol{u}$ is the input vector; $\boldsymbol{v}$ is the measurement noise; and $\boldsymbol{w}$ is the process noise.

III. Cyber-attack Modeling and Detection

This section focuses on the effects of cyber-attacks on the power system, the capabilities of attacker and defender, and cyber-attack modeling and detection.

A. Effect of Cyber-attacks

As discussed in Section I, cyber-attacks are resorted with two goals: network destabilization and financial disruption. The destabilization of power system may be instigated by terrorist groups (on a larger scale), governments in conflict (in the case of interconnected grids), or resentful individuals (on a smaller scale). The goals of the attackers can be either to disrupt the industrial activity or to gain access to secured areas. These players eavesdrop for a long period of time to gain knowledge of the power system parameters to inflict the maximum damage. These types of cyber-attacks are rare, but if successful, will lead to devastating results. However, the intention to affect market operations, mostly done by market operators or insiders, can be more frequent and stealthier as they have full knowledge of power system. This intention may not lead to instability, but gives rise to financial implications and affects the fair energy trading. This type of cyber-attack can be akin to stock markets in a deregulated environment.

B. Capabilities of Attacker and Defender

The attacker has full knowledge of power system and full access to the measurement data for a certain period of time prior to the cyber-attack. The attacker also has sufficient information of weak communication lines, and can decide the point of cyber-attack without being caught. However, it is assumed that the attacker does not have the information of the system parameters. Further, the attacker has no control over the power system after the cyber-attack is initiated. The defender has full information of the power system and its parameters. Besides, the full information of the filter is also known. The defender has the capability to respond to the cyber-attacks if it is detected by the filter.

C. Cyber-attack Modeling

1) FDI

FDI is the most common type of cyber-attack where the intruder injects false data into real data. The intruder has no knowledge of the system parameters or previous event data. An optimum FDI attack can lead to frequency instability [29], which is modeled as:

$$\boldsymbol{y}_k=\begin{cases}\boldsymbol{C}\boldsymbol{x}_k+\boldsymbol{v}_k & k<\tau\\ \boldsymbol{C}\boldsymbol{x}_k+\boldsymbol{b}_k+\boldsymbol{v}_k & k\geq\tau\end{cases} \tag{12}$$

where the subscript k represents the value at a given discrete-time instant k; $\boldsymbol{b}$ is the bias/attack vector added to the measure-

ments; and τ is the instant at which attackers becomes active.

2) DoS Attack

The intruder identifies a weak node or receiving node, and pumps in huge amounts of data packets so that the communication is jammed between the measuring device and control center for a certain period of time. The DoS attack is modeled as:

$$\boldsymbol{y}_k = \begin{cases} \boldsymbol{C}\boldsymbol{x}_k + \boldsymbol{v}_k & k < \tau \\ \boldsymbol{v}_k & k \geq \tau \end{cases} \tag{13}$$

3) DRA

The attacker collects previous event data and injects these data in place of real data.

$$\boldsymbol{y}_k = \begin{cases} \boldsymbol{C}\boldsymbol{x}_k + \boldsymbol{v}_k & k < \tau \\ \boldsymbol{y}_{k-z} + \boldsymbol{v}_k & k \geq \tau \end{cases} \tag{14}$$

where $\boldsymbol{y}_{k-z}$ is the previous event data before z time instants.

4) Scaling Attack

In this type of cyber-attack, the attacker scales down/up the current measurements.

$$\boldsymbol{y}_k = \begin{cases} \boldsymbol{C}\boldsymbol{x}_k + \boldsymbol{v}_k & k < \tau \\ \lambda\boldsymbol{C}\boldsymbol{x}_k + \boldsymbol{v}_k & k \geq \tau \end{cases} \tag{15}$$

where λ is the scaling factor.

5) Ramp Attack

The attacker injects false data that increases with time. Long-lasting sensor faults can be modeled in a similar way.

$$\boldsymbol{y}_k = \begin{cases} \boldsymbol{C}\boldsymbol{x}_k + \boldsymbol{v}_k & k < \tau \\ \lambda\boldsymbol{C}\boldsymbol{x}_k + \boldsymbol{b}_k k + \boldsymbol{v}_k & k \geq \tau \end{cases} \tag{16}$$

D. OTS-KF

Consider a linear invariant discrete system of the form:

$$\boldsymbol{x}_{k+1} = \boldsymbol{A}\boldsymbol{x}_k + \boldsymbol{B}\boldsymbol{u}_k + \boldsymbol{F}\boldsymbol{b}_k + \boldsymbol{w}_k \tag{17}$$

$$\boldsymbol{y}_k = \boldsymbol{C}\boldsymbol{x}_k + \boldsymbol{G}\boldsymbol{b}_k + \boldsymbol{v}_k \tag{18}$$

where $\boldsymbol{F}$ and $\boldsymbol{G}$ are matrices of suitable dimensions. An OTS-KF is proposed by Daroach and Keller. The filter has two major functions: one is to estimate the states of the system under bias/cyber-attack-free condition, and the second is to estimate the bias/cyber-attack. This filter is an extension to the Kalman filter where state estimation and cyber-attack estimations run in parallel. Similar to the Kalman filter, OTS-KF includes the basic steps of initialization: prediction and updating. The processes of OTS-KF state estimation and bias estimation are as follows:

$$\hat{\boldsymbol{x}}_{k+1/k+1} = \tilde{\boldsymbol{x}}_{k+1/k+1} + \boldsymbol{\xi}_{k+1/k+1}\hat{\boldsymbol{b}}_{k+1/k+1} \tag{19}$$

$$\boldsymbol{P}^x_{k+1/k+1} = \tilde{\boldsymbol{P}}^x_{k+1/k+1} + \boldsymbol{\xi}_{k+1/k+1}\boldsymbol{P}^b_{k+1/k+1}\boldsymbol{\xi}^{\mathrm{T}}_{k+1/k+1} \tag{20}$$

where $\hat{\boldsymbol{x}}_{k+1/k+1}$ is the estimated state vector; $\tilde{\boldsymbol{x}}_{k+1/k+1}$ is the cyber-attack-free estimated state vector; $\hat{\boldsymbol{b}}_{k+1/k+1}$ is the estimated bias/attack vector; $\boldsymbol{P}^x_{k+1/k+1}$ is the estimated error covariance matrix of $\hat{\boldsymbol{x}}_{k+1/k+1}$; $\tilde{\boldsymbol{P}}^x_{k+1/k+1}$ is the estimated error covariance matrix of $\tilde{\boldsymbol{x}}_{k+1/k+1}$; $\boldsymbol{P}^b_{k+1/k+1}$ is the estimated error covariance matrix of $\hat{\boldsymbol{b}}_{k+1/k+1}$; and $\boldsymbol{\xi}_{k+1/k+1}$ is the result matrix of coupling. The subscript $k+1/k+1$ indicates the updated value at the $(k+1)^{\text{th}}$ instant.

1) Bias/Cyber-attack-free Estimation

$$\tilde{\boldsymbol{x}}_{k+1/k} = \boldsymbol{A}\tilde{\boldsymbol{x}}_{k/k} + \boldsymbol{B}\boldsymbol{u}_k + \boldsymbol{r}_k\hat{\boldsymbol{b}}_{k/k} - \boldsymbol{\xi}_{k+1/k}\hat{\boldsymbol{b}}_{k/k} \tag{21}$$

$$\tilde{\boldsymbol{P}}^x_{k+1/k} = \boldsymbol{A}\tilde{\boldsymbol{P}}^x_{k/k}\boldsymbol{A}^{\mathrm{T}} + \boldsymbol{W}^x + \boldsymbol{r}_k\boldsymbol{P}^b_{k/k}\boldsymbol{r}_k^{\mathrm{T}} - \boldsymbol{\xi}_{k+1/k}\boldsymbol{P}^b_{k+1/k}\boldsymbol{\xi}^{\mathrm{T}}_{k+1/k} \tag{22}$$

$$\tilde{\boldsymbol{K}}^x_{k+1} = \tilde{\boldsymbol{P}}^x_{k+1/k}\boldsymbol{C}^{\mathrm{T}}\left(\boldsymbol{C}\tilde{\boldsymbol{P}}^x_{k+1/k}\boldsymbol{C}^{\mathrm{T}} + \boldsymbol{V}\right)^{-1} \tag{23}$$

$$\tilde{\boldsymbol{P}}^x_{k+1/k+1} = \left(\boldsymbol{I} - \tilde{\boldsymbol{K}}^x_{k+1}\boldsymbol{C}\right)\tilde{\boldsymbol{P}}^x_{k+1/k} \tag{24}$$

$$\tilde{\boldsymbol{x}}_{k+1/k+1} = \tilde{\boldsymbol{x}}_{k+1/k} + \tilde{\boldsymbol{K}}^x_{k+1}\left(\boldsymbol{y}_{k+1} - \boldsymbol{C}\tilde{\boldsymbol{x}}_{k+1/k}\right) \tag{25}$$

where $\boldsymbol{r}_k$ is the bias coefficient matrix; $\boldsymbol{W}^x$ is the process-noise covariance matrix; $\tilde{\boldsymbol{K}}^x_{k+1}$ is the updated controller gain at the $(k+1)^{\text{th}}$ instant; $\boldsymbol{V}$ is the measurement-noise covariance matrix; the subscript k/k indicates the measured values at the k^{th} instant; and the subscript $k+1/k$ indicates the estimated value.

2) Bias/Cyber-attack Estimation

$$\hat{\boldsymbol{b}}_{k+1/k} = \hat{\boldsymbol{b}}_{k/k} \tag{26}$$

$$\boldsymbol{P}^b_{k+1/k} = \boldsymbol{P}^b_{k/k} + \boldsymbol{W}_b \tag{27}$$

$$\boldsymbol{K}^b_{k+1} = \boldsymbol{P}^b_{k+1/k}\boldsymbol{H}^{\mathrm{T}}_{k+1/k}\left(\boldsymbol{C}\tilde{\boldsymbol{P}}^x_{k+1/k}\boldsymbol{C}^{\mathrm{T}} + \boldsymbol{V} + \boldsymbol{H}_{k+1/k}\boldsymbol{P}^b_{k+1/k}\boldsymbol{H}^{\mathrm{T}}_{k+1/k}\right)^{-1} \tag{28}$$

$$\boldsymbol{P}^b_{k+1/k+1} = \left(\boldsymbol{I} - \boldsymbol{K}^b_{k+1}\boldsymbol{H}_{k+1/k}\right)\boldsymbol{P}^b_{k+1/k} \tag{29}$$

$$\hat{\boldsymbol{b}}_{k+1/k+1} = \hat{\boldsymbol{b}}_{k/k} + \boldsymbol{K}^b_{k+1}\left(\left(\boldsymbol{y}_{k+1} - \boldsymbol{C}\tilde{\boldsymbol{x}}_{k+1/k}\right) - \boldsymbol{H}_{k+1/k}\hat{\boldsymbol{b}}_{k/k}\right) \tag{30}$$

where $\boldsymbol{W}_b$ is the bias-noise covariance matrix; and $\boldsymbol{H}_{k+1/k}$ is the estimation matrix at the k^{th} instant.

3) Coupling Terms

$$\boldsymbol{r}_k = \boldsymbol{A}\boldsymbol{\xi}_{k/k} + \boldsymbol{F} \tag{31}$$

$$\boldsymbol{\xi}_{k+1/k} = \boldsymbol{r}_k\boldsymbol{P}^b_{k/k}\boldsymbol{P}^{b-1}_{k+1/k} \tag{32}$$

$$\boldsymbol{H}_{k+1/k} = \boldsymbol{G} + \boldsymbol{C}\boldsymbol{\xi}_{k+1/k} \tag{33}$$

$$\boldsymbol{\xi}_{k+1/k+1} = \boldsymbol{\xi}_{k+1/k} - \tilde{\boldsymbol{K}}^x_{k+1}\boldsymbol{H}_{k+1/k} \tag{34}$$

$$\boldsymbol{H}_{k+1/k+1} = \boldsymbol{G} + \boldsymbol{C}\boldsymbol{\xi}_{k+1/k+1} \tag{35}$$

IV. Application of OTS-KF in Bias/Cyber-attack Detection

A. With Load Measurement

The dynamics of AGC in the absence of outliers are given in (10) and (11). Figure 2 depicts the two-area power system model with potential cyber-attack points.

Three possible cyber-attacks are considered: ① cyber-attack on frequency measurement in area 1; ② cyber-attack on frequency measurement in area 2; ③ cyber-attack on tie-line power measurement.

The dynamics of AGC are modified by including above-mentioned cyber-attacks as given in (36) and (37).

$$A\dot{C}E_1 = -K_{I1}B_1\Delta f_1 - K_{I1}\Delta P_{12} - K_{I1}B_1 b_1 - K_{I1}b_3 \tag{36}$$

$$A\dot{C}E_2 = -K_{I2}B_2\Delta f_2 + K_{I2}\Delta P_{12} - K_{I2}B_2 b_2 - K_{I2}b_3 \tag{37}$$

where b_1 and b_2 are the biases/cyber-attacks in frequency measurement in areas 1 and 2, respectively; and b_3 is the bias/cyber-attack in tie-line power measurement.

The state-space representation in (10) and (11) is modified accordingly as:

$$\dot{\boldsymbol{x}} = \boldsymbol{A}_o\boldsymbol{x} + \boldsymbol{B}_o\boldsymbol{u} + \boldsymbol{F}_o\boldsymbol{b} + \boldsymbol{w} \tag{38}$$

$$\boldsymbol{y} = \boldsymbol{C}\boldsymbol{x} + \boldsymbol{G}_o\boldsymbol{b} + \boldsymbol{v} \tag{39}$$

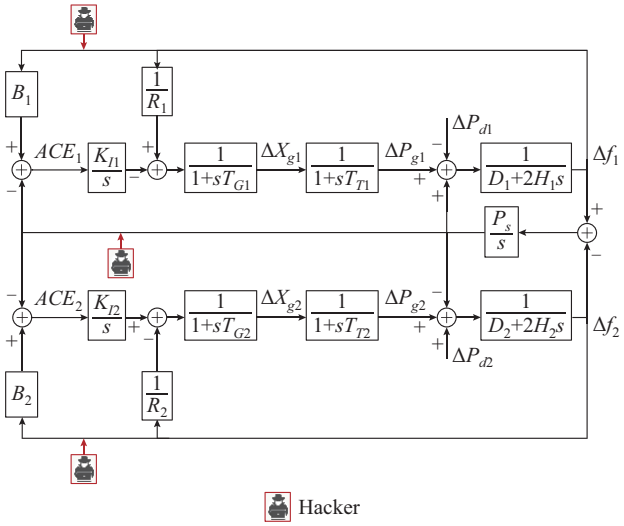

Fig. 2. Two-area power system model with potential cyber-attack points.

where $\boldsymbol{b}=[b_3 \quad b_1 \quad b_2]^{\mathrm{T}}$; $\boldsymbol{G}_o=[\boldsymbol{C} \quad zeros(3,2)]$; and $\boldsymbol{F}_o=$

$$\begin{bmatrix} 0 & 0 & 0 & -\dfrac{1}{2H_1} & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -K_{I1}B_1 & 0 & -K_{I1} & 0 & 0 \\ 0 & 0 & 0 & 0 & -\dfrac{1}{2H_2} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & -K_{I2}B_2 & K_{I2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

The power system dynamics given in (38) and (39) are modified and converted to discrete form as (17) and (18). The OTS-KF algorithm is now applied to estimate the bias/cyber-attack. The step-by-step procedure of the OTS-KF filter is given in Algorithm 1.

Algorithm 1: OTS-KF algorithm

1 Initialize the two-stage Kalman filter: $\hat{\boldsymbol{x}}_0=\boldsymbol{E}(\boldsymbol{x}_0)$, $\hat{\boldsymbol{b}}=\boldsymbol{E}(\boldsymbol{b}_0)$, $\boldsymbol{P}_0^x=\boldsymbol{E}\left[\left(\boldsymbol{x}_0-\hat{\boldsymbol{x}}_0\right)\left(\boldsymbol{x}_0-\hat{\boldsymbol{x}}_0\right)^{\mathrm{T}}\right]$, $\boldsymbol{P}_0^b=\boldsymbol{E}\left[\left(\boldsymbol{b}_0-\hat{\boldsymbol{b}}_0\right)\left(\boldsymbol{b}_0-\hat{\boldsymbol{b}}_0\right)^{\mathrm{T}}\right]$, where $\boldsymbol{x}_0$, $\boldsymbol{b}_0$, $\hat{\boldsymbol{x}}_0$, and $\hat{\boldsymbol{b}}_0$ are the states, biases, and their estimated values, respectively; and $\boldsymbol{E}$ is the expected value
while $k>0$
2 Predict the states and bias/cyber-attack using (21) and (26)
3 Calculate the gains using (23) and (28) and the coupling terms using (31)-(35)
4 Update the states and bias/cyber-attack signals using (25) and (30)
$k=k+1$
end while
5 Display states and cyber-attack signals

B. Without Load Measurement

The load connected to the power system is stochastic and continuously varies with time. With the injection of stochastic renewable energy into the power system, the net demand affecting the load frequency is not monitored by a centralized monitoring system. To address this challenge, load variations are estimated along with cyber-attack signals. This subsection discusses cyber-attack detection without load measurement.

The dynamics given in (38) and (39) are modified assuming the loads in both areas as unknown inputs.

$$\dot{\boldsymbol{x}}=\boldsymbol{A}_o\boldsymbol{x}+\boldsymbol{F}_1\boldsymbol{b}_1+\boldsymbol{w} \tag{40}$$

$$\boldsymbol{y}=\boldsymbol{C}\boldsymbol{x}+\boldsymbol{G}_1\boldsymbol{b}_1+\boldsymbol{v} \tag{41}$$

where $\boldsymbol{F}_1$ and $\boldsymbol{b}_1$ are the bias coefficients and bias, respectively; and $\boldsymbol{G}_1$ is the bias coefficient in the output matrix. The dynamic model of AGC system is then transferred from continuous to discrete time representation.

$$\boldsymbol{x}_{k+1}=\boldsymbol{A}\boldsymbol{x}_k+\boldsymbol{F}'\boldsymbol{b}'_k+\boldsymbol{w}_k \tag{42}$$

$$\boldsymbol{y}_k=\boldsymbol{C}\boldsymbol{x}_k+\boldsymbol{G}'\boldsymbol{b}'_k+\boldsymbol{v}_k \tag{43}$$

where $\boldsymbol{F}'$, $\boldsymbol{b}'_k$, and $\boldsymbol{G}'$ are the coefficients in the discrete time domain. The procedure of modified OTS-KF is the same as before except for the prediction step, which is given as:

$$\tilde{\boldsymbol{x}}_{k+1/k}=\boldsymbol{A}\tilde{\boldsymbol{x}}_{k/k}+\boldsymbol{r}_k\hat{\boldsymbol{b}}_{k/k}-\boldsymbol{\xi}_k\hat{\boldsymbol{b}}_{k/k} \tag{44}$$

The step-by-step procedure of modified OTS-KF is given in Algorithm 2.

Algorithm 2: modified OTS-KF algorithm

1 Initialize the two-stage Kalman filter
while $k>0$
2 Predict the states and bias/cyber-attack using (44) and (26)
3 Calculate the gains using (23) and (28) and the coupling terms using (31)-(35)
4 Update the states and bias/cyber-attack signals using (25) and (30)
$k=k+1$
end while
5 Display states, load demand, and cyber-attack signals

V. Simulation Results and Discussion

The proposed idea of state and bias/attack estimation is simulated for a two-area power system model in MATLAB/Simulink for various cases of cyber-attacks. A zero-mean Gaussian noise with a standard deviation of 10^{-4} is considered as the process noise and measurement noise. The parameters used for simulation are given in Appendix A.

A. With Load Measurement

1) FDI Attack

To evaluate the performance of the proposed filter, we develop a random cyber-attack signal, which is a combination of step and ramp signals added to the tie-line power deviations. Figure 3 depicts the actual and estimated cyber-attack signals with random FDI using the OTS-KF.

2) DoS Attack

For cyber-attack generation, we assume that the communication channel is blocked from 1 s to 10 s, and the centralized monitoring and control unit has no idea of actual measurements. DoS attack can be viewed as an FDI attack with the bias signal as the inverse of the missing signal. The actual and estimated tie-line power deviations are illustrated in Fig. 4.

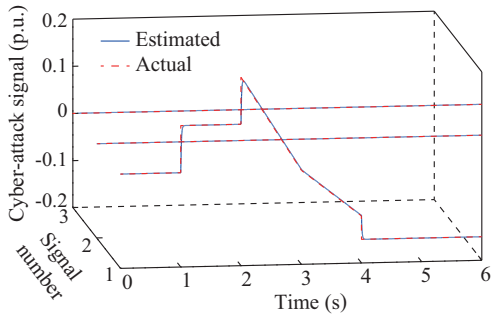

Fig. 3. Actual and estimated cyber-attack signals with random FDI.

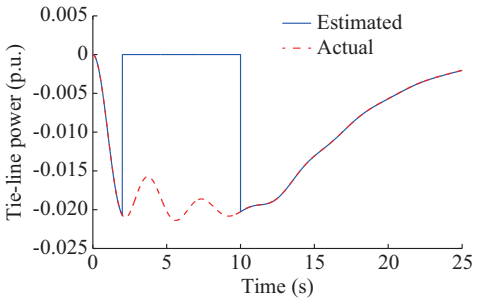

Fig. 4. Actual and estimated tie-line power deviations.

3) DRA

To generate this cyber-attack signal, we have simulated the system for a step change of 0.15 p.u. load demand, and the frequency measurements are saved into the workspace. The saved frequency variations are injected as a cyber-attack signal under a non-load condition. The actual and estimated DRA signals are shown in Fig. 5.

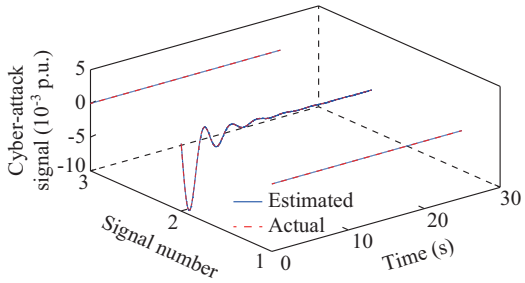

Fig. 5. Actual and estimated DRA signals.

B. Without Load Measurement

1) Two-area Power System

The modern power system is a combination of conventional energy systems and renewable energy systems. As renewable energy systems are stochastic, the net demand affecting the frequency variation on each area at every instant is seldom available in the centralized system. Without online load data, the system operator has to depend on load forecasting data. Table I shows that in the case of load forecasting, the errors largely affect the cyber-attack estimation. A new OTS-KF is formulated and applied to the two-area power system model. In this case, the load and cyber-attack estimations run simultaneously [21]. In Fig. 6, signals 1-3 show the actual and estimated cyber-attack signals, while signals 4 and 5 show the load changes in areas 1 and 2, respectively.

TABLE I
ROOT-MEAN-SQUARE ERROR (RMSE) WITH LOAD FORECASTING ERROR

Load forecasting error (%)	RMSE
0	1.03×10^{-4}
2	8.82×10^{-4}
4	1.70×10^{-3}

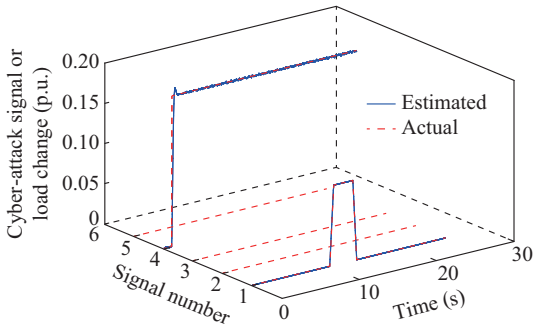

Fig. 6. Actual and estimated cyber-attack signals and load changes.

2) Three-area Power System

Now the proposed filter is validated on a three-area power system model [28] assuming that the tie-line measurements are prone to cyber-attacks. We have considered six operation scenarios:

1) Scenario 1: FDI on tie-line with constant load change in area 1.

2) Scenario 2: FDI on tie-line with continuous load change in area 1.

3) Scenario 3: tie-line power deviations scaled to 1.2 times the actual value.

4) Scenario 4: ramp attack on tie-line power deviations.

5) Scenario 5: multiple attacks on the tie-line power deviations.

6) Scenario 6: multiple load changes with random FDI attack on tie-line power measurements.

The simulated results for the first two scenarios are depicted in Fig. 7. The tie-line power deviations with and without cyber-attack as well as the estimated tie-line power deviation with the proposed method for scenario 3 are shown in Fig. 8.

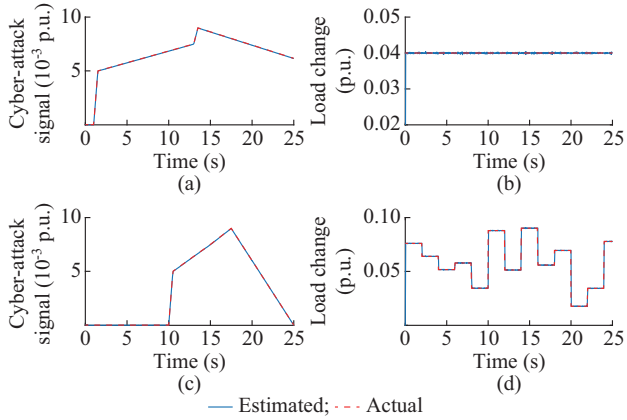

Fig. 7. Cyber-attack and load signals for scenarios 1 and 2. (a) Cyber-attack signals for scenario 1. (b) Load change signals for scenario 1. (c) Cyber-attack signals for scenario 2. (d) Load change signals for scenario 2.

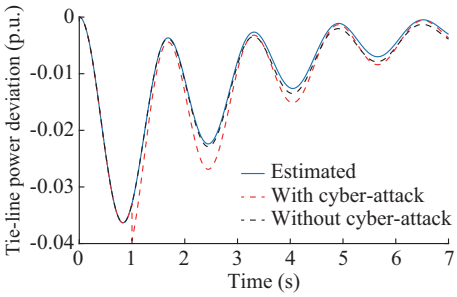

Fig. 8. Tie-line power deviations for scenario 3.

It can be observed that except for low values of tie-line power deviations, the estimated signal tracks the actual signal. Long-lasting sensor failures are quite difficult to detect and adversely affect the system performance. These faults and ramp attacks are identical in terms of their behaviors. The system is simulated with a ramp attack. The estimated and actual cyber-attack signals with ramp attack are depicted in Fig. 9.

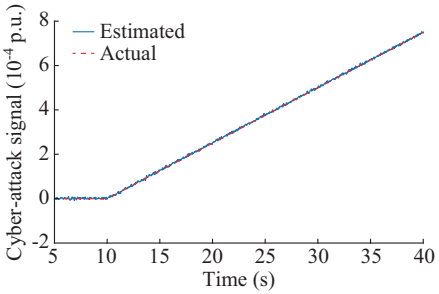

Fig. 9. Actual and estimated cyber-attack signals with ramp attack.

The proposed filter is evaluated for multiple attacks. Figure 10 shows the efficacy of the proposed method. Figure 11 illustrates the frequency deviations in all three areas for a random FDI attack with load changes. The actual and estimated load changes and cyber-attack signal are also shown in Fig. 11. Even the cyber-attack signals with small magnitudes have a considerable influence over frequency deviations, as shown in Fig. 12.

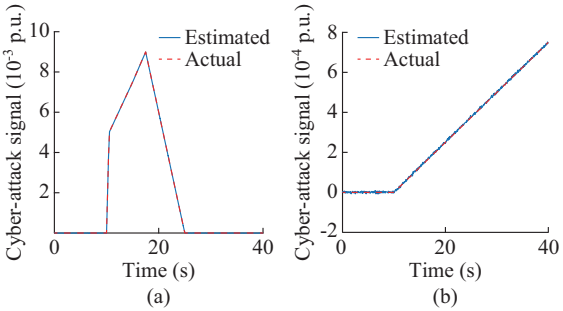

Fig. 10. Actual and estimated cyber-attack signals with multiple attacks. (a) Tie-line 1. (b) Tie-line 2.

C. Five-area Power System

The proposed dynamic cyber-attack estimation procedure is also applied for the benchmark five-area power system model that is widely used in literature for load frequency studies [30], [31]. We have assumed that the tie-line power deviations in this large-scale system are subjected to cyber-attacks, whereas the frequency measurements are cyber-attack-free. To investigate the effect of cyber-attacks on the power system, a ramp signal is injected into the tie-line power measurements of ΔP_{12}. The frequency deviations in area 2 are damped to zero in the absence of cyber-attacks, which are represented with red color in Fig. 13. However, frequency deviations are highly influenced by the cyber-attack magnitude, which are represented with blue color.

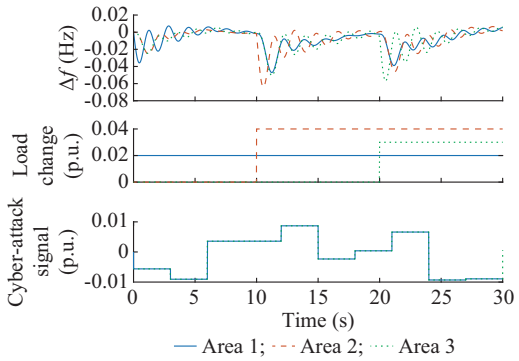

Fig. 11. System response for scenario 6 including changes in frequency signals, load, and actual and estimated cyber-attack signals.

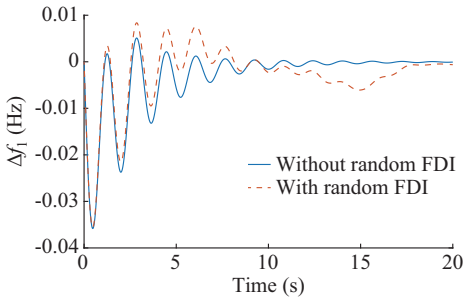

Fig. 12. Frequency deviations with and without random FDI.

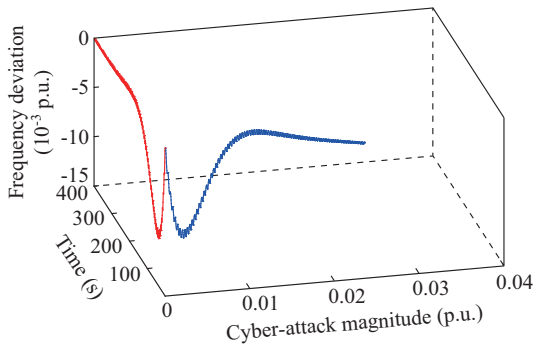

Fig. 13. Influence of cyber-attack signal on frequency deviations.

In addition, we have considered a simultaneous load change in area 1 while the tie-line power deviations in area 4 are subjected to cyber-attacks. In the five-area system, there are ten unknown inputs, where five represent load changes and the rest represent the cyber-attack signals. Figure 14 shows the load and cyber-attack estimations in five-area power system. The proposed algorithm is superior in detecting even small load changes, as shown in Fig. 14. Further, it can be observed that the operator can easily identify vulnerable measurements that are attacked in area 4.

D. Cyber-attack Mitigation

Attack mitigation is a crucial phase in dealing with cyber-attacks. It improves the frequency stability during the cyber-attack. Once the cyber-attack is quantified using the OTS-KF, the attack component of the measured signals is removed from the vulnerable measured signals. In Fig. 15, it is shown that the proposed OTS-KF can effectively mitigate a ramp-down attack. The proposed algorithm could quantify the cyber-attack and could successfully mitigate it within the time constraints of the system. Without it, the chances of the system getting out of synchronism may increase.

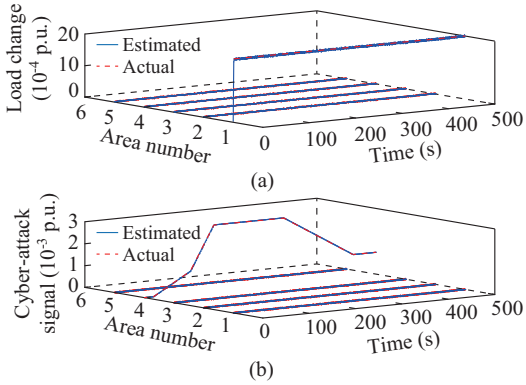

Fig. 14. Load and cyber-attack estimations in five-area power system. (a) Load estimation. (b) Cyber-attack estimation.

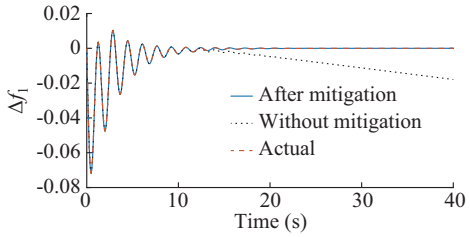

Fig. 15. Frequency change in area 1 with ramp attack mitigation.

E. Further Discussion: Filter Sensitivity to Process and Measurement Noises

The practical power system may have higher noise variances compared with the base values of the available filter, and hence, the test system is simulated with process and measurement noises which are ten times the base value. Figure 16 illustrates the estimation error in presence of measurement noise covariance and process noise covariance. The subscript 0 in Fig. 16 represents actual error covariance. The errors in process noise covariance $\boldsymbol{W}^x$ and measurement noise covariance $\boldsymbol{V}$ will not have much impact on the cyber-attack estimation, and, in turn, may not influence the attack alarms.

F. Comparative Analysis

In this sub-section, a comparative analysis of the proposed technique with related ones is presented. Most of the cyber-attack detection algorithms in the literature are limited to FDI. However, we have tested for five different cyber-attacks. The robust observer for unknown input estimation [8] is limited for certain applications as it is based on the rank condition. It has been verified that this observer is prone to ill-conditioning for the proposed formulation.

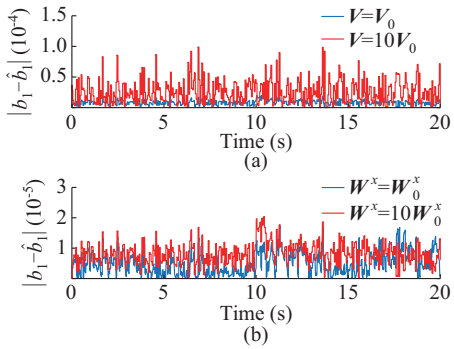

Fig. 16. Estimation error in presence of measurement noise covariance and process noise covariance. (a) Actual and unknown measurement noise covariance. (b) Actual and unknown process noise covariance.

Cyber-attack detection, estimation, mitigation, state estimation, and load data independence are the main features of the proposed idea. Cyber-attack detection based on the residual function of the unknown input observer is proposed in [10]. However, an attacker with adequate system knowledge can insert small amounts of bad data and circumvent the detection system. The approach proposed in [19] relies on load forecasting data. However, with the increased penetration levels of stochastic renewable energy, there is a huge gap between planning and dispatch. Since this method is a statistical method, the load forecasting error may severely affect the performance of the algorithm during a cyber-attack. Cyber-attack estimation based on the unknown input observer proposed in [21] has shown consistent performance only in the presence of online load data. Nevertheless, in the absence of load data, this approach must rely on the load forecasting data. Estimation error with load forecasting error in load data may lead to false cyber-attack alarms as illustrated in Fig. 17.

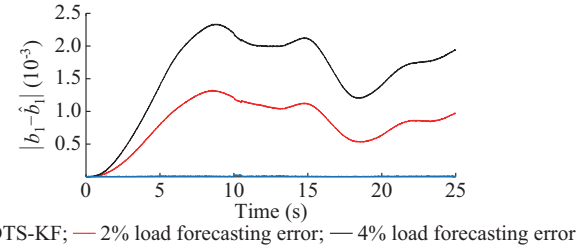

Fig. 17. Estimation error with load forecasting error.

We have simulated the system in the presence of 2% and 4% errors in the load forecasting data. Similarly, in [22] and [23], dynamic methods are explored using stochastic unknown input estimators and online detection methods, respectively, though the cyber-attacks could not be mitigated. Real-time state estimation at the centralized monitoring unit improves the secure monitoring and control process of the power system. State estimation, along with an cyber-attack estimate, will further enhance the security of the system. The algorithms proposed in [10], [22], [23], and [30] focus on the cyber-attack detection rather than the mitigation. The proposed OTS-KF is compared with other model-based techniques in the literature and the results are shown in Table II.

TABLE II
COMPARISON OF VARIOUS TECHNIQUES

Technique	Dynamic method	Attack detection	Attack estimation	Load data independence	State estimation	Attack mitigation
[10]	√	√	×	√	×	×
[19]	√	√	√	×	×	√
[21]	√	√	√	×	√	√
[22]	√	√	×	√	√	×
[23]	√	√	×	×	√	×
[29]	√	√	√	×	√	√
[32]	√	√	×	√	×	×
OTS-KF	√	√	√	√	√	√

Note: √ indicates that the given reference has the capability to address the given problem, while × indicates that they cannot address the same.

VI. CONCLUSION

Modern power systems are undergoing drastic changes with an increase in the expanse and penetration of renewable energy. Though it reflects economic betterment, it results in wide frequency deviations. To alleviate this problem, the power system is stepping towards the smart grid. However, smartness comes with internet connectivity and communication links. As these are prone to cyber-attacks, there is a need to detect and avoid any potential threat. This paper addresses the issue of estimating various types of cyber-attacks such as FDI, DRA, DoS, scaling, and ramp attacks. In this paper, an OTS-KF is implemented in the AGC of the benchmark two-area, three-area, and five-area power system models to estimate the cyber-attacks. Due to the inclusion of distributed generation systems to the power grid, the net load variations affecting the load frequency are seldom available. To address this challenge, the proposed OTS-KF is modified to estimate the load variations along with outliers. The simulation results show the effectiveness of the proposed filter for various test cases. Cyber-attack identification is based on the linearized power system model, and hence, the computation speed and/or efficiency will not be compromised by the system size. However, in the case of a very large-scale system, the system may be divided into subsystems, forming multiple power grids. Filters can be placed in each subsystem to facilitate better detection. This idea can also be extended to deal with intelligent and dummy attacks on the smart grid.

APPENDIX A

TABLE AI
SIMULATION PARAMETERS OF TWO-AREA SYSTEM

Parameter	Value
T_{T1}, T_{T2} (s)	0.5, 0.6
T_{G1}, T_{G2} (s)	0.2, 0.3
H_1, H_2 (s)	5, 4
D_1, D_2 (p.u./Hz)	0.6, 0.3
R_1, R_2 (rad/p.u.)	0.05, 0.0625
K_{I1}, K_{I2}	0.3, 0.3
P_s	2

TABLE AII
SIMULATION PARAMETERS OF THREE-AREA SYSTEM

Parameter	Value
T_{Ti} (s)	0.3
T_{Gi} (s)	0.08
R_i (rad/p.u.)	2.4
B_i	0.425
T_{ij} (s)	0.544

REFERENCES

[1] X. Yu and Y. Xue, "Smart grids: a cyber-physical systems perspective," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1058-1070, May 2016.

[2] Y. Xue and X. Yu, "Beyond smart grid–a cyber-physical-social system in energy future," *Proceedings of the IEEE*, vol. 105, no. 12, pp. 2290-2292, Dec. 2017.

[3] E. Bou-Harb, C. Fachkha, M. Pourzandi *et al.*, "Communication security for smart grid distribution networks," *IEEE Transactions on Communication Magazine*, vol. 51, no. 1, pp. 42-49, Jan. 2013.

[4] R. Fu, X. Huang, Y. Xue *et al.*, "Security assessment for cyber physical distribution power system under intrusion attacks," *IEEE Access*, vol. 7, pp. 75615-75628, Jul. 2018.

[5] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210-224, Jan. 2012.

[6] G. Liang, J. Zhao, F. Luo *et al.*, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630-1638, Jul. 2017.

[7] M. Jin, J. Lavaei, and K. H. Johansson, "Power grid AC-based state estimation: vulnerability analysis against cyber attacks," *IEEE Transactions on Automatic Control*, vol. 64, no. 5, pp. 1784-1799, May 2019.

[8] A. F. Taha, J. Qi, J. Wang *et al.*, "Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 886-899, Mar. 2018.

[9] G. Liang, S. R. Weller, F. Luo *et al.*, "Generalized FDIA-based cyber topology attack with application to the Australian electricity market trading mechanism," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3820-3829, Jul. 2018.

[10] A. Ameli, A. Hooshyar, E. F. El-Saadany *et al.*, "Attack detection and identification for automatic generation control systems," *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 4760-4774, Sept. 2018.

[11] H. Karimipour and V. Dinavahi, "Robust massively parallel dynamic state estimation of power systems against cyber-attack," *IEEE Access*, vol. 6, pp. 2984-2995, Dec. 2017.

[12] R. Deng, P. Zhuang, and H. Liang, "CCPA: coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2420-2430, Sept. 2017.

[13] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715-2729, Nov. 2013.

[14] N. Živković and A. T. Sarić, "Detection of false data injection attacks using unscented Kalman filter," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 847-859, Sept. 2018.

[15] J. Yu, Y. Hou, and V. Li, "Online false data injection attack detection with wavelet transform and deep neural networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 3271-3280, Jul. 2018.

[16] M. Esmalifalak, L. Liu, N. Nguyen *et al.*, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1644-1652, Sept. 2017.

[17] E. Hossain, I. Khan, F. Un-Noor *et al.*, "Application of big data and machine learning in smart grid, and associated security concerns: a review," *IEEE Access*, vol. 7, pp. 13960-13988, Jan. 2019.

[18] A. Jindal, A. Dua, K. Kaur *et al.*, "Decision tree and SVM-based data analytics for theft detection in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 3, pp. 1005-1016, Jun. 2016.

[19] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580-591, Mar. 2014.

[20] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1636-1646, Jul.

2016.
[21] M. Khalaf, A. Youssef, and E. El-Saadany, "Joint detection and mitigation of false data injection attacks in AGC systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 4985-4995, Sept. 2018.
[22] A. Ameli, A. Hooshyar, A. H. Yazdavar *et al.*, "Attack detection for load frequency control systems using stochastic unknown input estimators," *IEEE Transactions on Information Forensics Security*, vol. 13, no. 10, pp. 2575-2590, Oct. 2018.
[23] T. Huang, B. Satchidanandan, P. R. Kumar *et al.*, "An online detection framework for cyber attacks on automatic generation control," *IEEE Transactions on Power Systems*, vol. 33, no. 6, pp. 6816-6827, Nov. 2018.
[24] Y. W. Law, T. Alpcan, and M. Palaniswami, "Security games for risk minimization in automatic generation control," *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 223-232, Jan. 2015.
[25] M. Jin, J. Lavaei, S. Sojoudi *et al.* (2019, Aug.). Boundary defense against cyber threat for power system operation. [Online]. Available: https://arxiv.org/abs/1908.10315
[26] J. Jin, I. Molybog, and R. Mohammadi-Ghazi, "Scalable and robust state estimation from abundant but untrusted data," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 1880-1894, May 2020.
[27] J. Y. Keller and M. Darouach, "Optimal two-stage Kalman filter in the presence of random bias," *Automatica*, vol. 33, no. 9, pp. 1745-1748, Sept. 1997.
[28] A. S. L. V. Tummala, R. Inapakurthi, and P. V. Ramanarao, "Observer based sliding mode frequency control for multi-machine power systems with high renewable energy," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 3, pp. 473-481, May 2018.
[29] R. Tan, H. Nguyen, E. Foo *et al.*, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Transactions on Information Forensics Security*, vol. 12, no. 7, pp. 1609-1624, Jul. 2017.
[30] L. C. Saikia, J. Nanda, and S. Mishra, "Performance comparison of several classical controllers in AGC for multi-area interconnected thermal system," *International Journal of Power and Energy Systems*, vol. 33, no. 3, pp. 394-401, Mar. 2011.
[31] K. Jagatheesan, B. Anand, S. Samanta *et al.*, "Design of a proportional-integral-derivative controller for an automatic generation control of multi-area power thermal systems using firefly algorithm," *IEEE/CAA Journal of Automatica Sinica*, vol. 6, no. 2, pp. 503-515, Mar. 2019.
[32] K. Pan, P. Palensky, and P. M. Esfahani, "From static to dynamic anomaly detection with application to power system cyber security," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1584-1596, Mar. 2020.

Ayyarao S. L. V. Tummala received the B.Tech. degree in electrical & electronics engineering from Jawaharlal Nehru Technological University, Andhra Pradesh, India, in 2005, and the M. Tech. degree in power & industrial drives from Jawaharlal Nehru Technological University, Kakinada, Andhra Pradesh, India, in 2009. He received the Ph.D. degree from Acharya Nagarjuna Univeristy, Andhra Pradesh, India, in 2019. He is currently working as an Assistant Professor in the Department of Electrical and Electronics Engineering, GMR Institute of Technology, Rajam, India. His research interests include load frequency control, doubly-fed induction generator (DFIG)-fed wind energy conversion, optimization, and data driven control.

Ravi Kiran Inapakurthi received the B.Tech. degree in electrical & electronics engineering from Jawaharlal Nehru Technological University, Andhra Pradesh, India, in 2008, and the M.Tech. degree in power electronics from National Institute of Technology, Calicut, India, in 2011. He is currently working as an Associate Professor in the Department of Electrical and Electronics Engineering, Raghu Engineering College, Visakhapatnam, India. His research interests include control of DC/DC converters, optimization, and renewable energy systems.