Stability Assessment of Secondary Frequency Control System With Dynamic False Data Injection Attacks

Article *in* IEEE Transactions on Industrial Informatics · August 2021

CITATIONS
0

READS
2

6 authors, including:

Mingjian Cui
University of Tennessee
70 PUBLICATIONS **1,269** CITATIONS
SEE PROFILE

Junbo Zhao
Mississippi State University
160 PUBLICATIONS **2,337** CITATIONS
SEE PROFILE

Fangxing Li
University of Tennessee
365 PUBLICATIONS **9,272** CITATIONS
SEE PROFILE

Stability Assessment of Secondary Frequency Control System With Dynamic False Data Injection Attacks

Chunyu Chen, *Member, IEEE*, Xiao Zhang, Mingjian Cui, *Senior Member, IEEE*, Kaifeng Zhang, *Member, IEEE*, Junbo Zhao, *Senior Member, IEEE*, and Fangxing Li, *Fellow IEEE*

***Abstract*—The progression of modern computing technologies assists the development of cyber-physical systems, which are transforming the legacy electrical power systems into smarter ones. The informationalization of the grid poses potential vulnerabilities concerning cyber attacks. With dynamic variations over time, cyber attacks can cause significant impacts on the secondary frequency control with various attack scenarios. In this paper, by divulging the characteristics of dynamic attacks, the stability and dynamic responses of secondary frequency control systems are analyzed. The complete attack models considering dynamic load altering attack and dynamic false data injection attack are both derived first. Then the system stability is evaluated with different attack models through mathematical analysis. Eventually, the simulation studies against two benchmark power system models validate the evaluation results.**

***Index Terms*—Cyber-physical systems, dynamic false data injection attack, dynamic load altering attack, stability evaluation, secondary frequency control.**

I. Introduction

Electrical power systems are undergoing a dramatic transformation into the cyber-physical system (CPS) [1]. The manual operation and maintenance in legacy power systems are upgraded to automatic ones with the aid of modern information and communication technologies. This newly-developed electrical CPS is a double-edged sword: on the one hand, it facilitates the well-functioning data-driven applications; on the other hand, it increases the grid's exposure to external risks [2]. As one foundational data-driven application that uses remote communication to stabilize the system frequency, the secondary frequency control (SFC) faces the potential menace, which is posed by malicious active power balance deterioration through cyber attacks. Thus, it is essential to study how the attack affects SFC and establish corresponding protection measures.

Cyber attacks could occur for any CPS infrastructures, e.g., air navigation systems, oil and gas production systems [3]. As for the electrical power system, its sheer scale complicates the attack process. The attacker could seize control of certain low-level components illegally. The high-level control centers may also be infiltrated [4], leading to a more rapid and large scale of damages. The low-level component usually refers to those that are widely distributed over certain geographic areas, e.g., the sensors and other field devices. They maintain the basic remote connection with each other or designated information hubs. In the hierarchy of control systems, they belong to the lower layers, taking charge of data collection & communication as well as the basic local control. Though the access level is low, collateral influences from their collapse cannot be overlooked. Cui *et. al.* [5] used the naive Bayes classification to identify anomalies in load forecasting data. Dynamic programming is used to calculate the occurrence and parameter of the anomaly. Instead of using pure data-driven detectors, Xiao *et. al.* [6] designed a distributed filtering strategy for corrupt state measurements to cope with malicious deception attacks upon the sensor nodes in smart grids. Liu *et. al.* [7] revealed that the false data in meter readings could be considered as anomalies and easily detected. Nevertheless, if specific constraints w.r.t. the detector are satisfied, the false data can be hidden. In [8], the false data injection attack (FDIA) on line current differential relays was analyzed concerning the unwarranted trip signal generation. Unknown input observers were designed to recover the real state information. System state information can be used in both the operation & control and the electricity market. In [9], the optimal critical parameters (measurement errors) were investigated for maximal profit gain from the attacker's perspective. Besides implementing countermeasures passively, defenders can also use proactive moving-target-defense mechanism to change the real parameters to prelude cyber attacks [10]. The emerging blockchain and edge computing techniques fundamentally change CPS architectures for offering intrinsic security. Recently, rather than filtering the false data, researchers begin to study how to resist the data corruption via the secure authentication [11], [12].

High-level penetration is more direct and lethal since attackers control all critical resources. Hence the countermeasure design is more challenging. Bypassing or disabling the advanced false data detector (FDD), attackers could instantaneously disrupt the operation & control functions, supposing that they infiltrate the control center. Therefore pure FDD-based attack mitigation measures are insufficient to guarantee system stability and safety. The idea of cyber attack-tolerant control (CATC) is thus proposed to either actively or passively counteract the attack influence [13], [14]. In [15], a defender-attacker-operator interdiction problem was considered by using tri-level programming. The optimal allocation scheme was

This work was supported in part by Natural Science Foundation of China under Grant 51977033 and in part by 'the Fundamental Research Funds for the Central Universities'(2020QN62) and in part by Project of Jiangsu Shuangchuang Doctor. Paper no. TII-21-2655. (Corresponding author: Xiao Zhang, Mingjian Cui.)

Chunyu Chen and Xiao Zhang are with China University of Mining and Technology, Xuzhou 221266, China (e-mail: chunyuchen@cumt.edu.cn; zhangxiao@cumt.edu.cn).

Mingjian Cui and Fangxing Li are with the University of Tennessee, Knoxville, TN 37996 USA (e-mail:mingjian.cui@ieee.org; fli6@utk.edu).

Kaifeng Zhang is with Southeast University, Nanjing 210096, China (e-mail:kaifengzhang@seu.edu.cn).

Junbo Zhao is with the Mississippi State University, Starkville, MS 39762 USA (e-mail: junbo@ece.msstate.edu).

achieved to palliate damages from worst cases. In [16], the active and passive attack-tolerant load frequency control schemes were designed. Besides treating attackers as inactive performer, game techniques are promising methodologies to analyze the interaction between attackers and defenders [17].

The victim of cyber attacks on SFC can also be categorized by the frequency sensor reading and control input, which correspond to the low and high-level components, respectively. Various studies have been recently researched concerning the FDD design [18] and CATC design [19], [20]. Though many satisfactory theoretical or experimental values are achieved w.r.t. the detection or mitigation of the false data. The following two aspects still demand further studies:

- What are the characteristics of the false data w.r.t. the secondary frequency control?
- How will the false data with different characteristics influence the long-term and short-term performance of SFC?

Though the aforementioned problems seem elementary, they lay the foundation for any frequency stability-related study under cyber attacks. If the features of the false data (i.e., the attack input of the SFC system in this context) and the corresponding impacts on the stability are not properly investigated, the remaining CATC design, irrespective of these two critical aspects, will be incomplete and even ungrounded. Therefore we systematically study them in this paper.

Most related studies center on the detection and mitigation of cyber attacks against SFC [21]–[24]. Attackers usually manipulate data mildly, out of consideration for the stealthiness. The abnormal frequency excursions in this context, though cannot cross the equilibrium, may remain within the allowable range of deviation. The grid may self-tolerate attacks instead of resorting to mitigatory and corrective actions. To further evaluate the compromised control performance, we first need to ascertain what the system response looks like with no additional protective control. In other words, we need to study the attack's influence upon the control performance. To the best of the authors' knowledge, none of the previous research presents a systematic analysis of the mechanism of different attacks on SFC [25], assessing the attack influence quantitatively and disclosing general laws (cause-effect relationship between attacks and corresponding system responses) behind observations of the specific attack events. These general laws can provide defenders with "a priori" knowledge of the stability performance and compromised system responses, which are fundamental to the resilience evaluation of the compromised control system during the pre-mitigation stage. Thus, we make an exploratory investigation by carefully studying the compromised system model under different attack scenarios.

Cyber attacks on SFC can be classified into FDIA and load altering attack (LAA) [26], which manipulates remotely accessible and controllable load to disrupt the grid. In this paper, FDIA specifically aims at the frequency measurement while LAA aims at the vulnerable load. Therefore the input channels of these two attacks are different. Since the frequency variable cannot be involved into the conventional state estimation (SE), FDIA on SE is not considered herein. Instead of being static, attack signals can be dynamic by following a certain trajectory over time, which leads to the dynamic load altering attack (D-LAA) and dynamic false data injection attack (D-FDIA). There're two main characteristics of the dynamic attack input signal.

- *time-varying*: The attack input signal is time-varying and can take many forms such as the pulse, step, and periodic function.
- *uncertainty*: The attack input signal is uncertain through taking the form of certain stochastic processes.

Considering these two characteristics of attack signals above, we first derive the complete SFC model under cyber attacks. Specifically, the deterministic and stochastic attack scenarios are both modeled. In the former model, it is assumed that the attack input signal is deterministic but time-varying; in the latter one, the attack input signal considers the stochastic process. Furthermore, the stability of the compromised SFC is assessed using the built models. In the stability assessment of deterministic scenarios, the dynamic responses of the system frequency are also derived to characterize the real-time attack impacts. The main contributions of this paper include:

- Without any detection and mitigation of SFC-oriented attacks, which attracts intensive attention in existing theoretical or practical studies, we delve into a rarely researched topic of the repression capability of SFC under cyber attacks. We expound on the idea of a "mild attack" in which attackers make a small change of data or load rather than aggressively change them. We demonstrate the feasibility of this attack mode by addressing its advantage and the problem of its counterpart (aggressive attack mode).
- We model the complete attack process in the context of SFC under the mild attack mode. By considering the variation of attack signals' characteristics and targets, we develop compromised system models corresponding to multiple attack scenarios, which can imitate real-life attack activities. Specifically, we consider D-LAA and D-FDIA. We use deterministic models to characterize the time-varying but deterministic attack signals. Meanwhile, we use stochastic processes to describe the uncertain attack signals. With the developed compromised system models, we check the stability and derive the system responses from both theoretical and numerical analyses. To validate the results, we use the detailed benchmark power system models which can reproduce the real-life systems. Hence, the practicality in real-life engineering is guaranteed.

The remainders are presented in the following sections: Section II briefly addresses backgrounds of dynamic attacks for SFC; Section III presents the detailed procedure of how to establish the mathematical compromised SFC models; Section IV presents the stability evaluation via mathematical deductions. Section V uses two benchmark power systems to validate the conclusions in Section IV. Closing conclusions and future work are briefly described in Section VI.

II. Basic Backgrounds of Dynamic Attacks on Secondary Frequency Control

A. Dynamic Load Altering Attack

The dynamic load altering attack (D-LAA) is previously studied in [26], in which the power system stability under closed-loop D-LAA is considered. Unlike the closed-loop D-LAA, which uses sensor readings to "intelligently" deteriorate stability, the D-LAA considered herein is an open-loop system, independent of sensor readings of any power system state:

$$-P_{is}+P_{id}\left(t\right)=U_i\sum_{j=1}^{n}U_j\left(G_{ij}\cos\theta_{ij}+B_{ij}\sin\theta_{ij}\right),\forall i\in\mathcal{L} \tag{1}$$

where P_{is} and P_{id} are the nominal load consumption and compromised load variation at load bus i; U_j is the voltage magnitude at bus j; $G_{ij}+jB_{ij}$ represents the complex admittance value between bus i and j. By hacking into the demand response (DR) program, attackers can manipulate load control signals (e.g., the switch-on or switch-off signal), thus causing malicious load change and influencing SFC. From the attacker's perspective, this manipulated load can be regarded as a "control input". Specifically, attackers can assume the role of the DLC center and use load switches or thermostats to make the dynamic (e.g., pulse-like and step-like) load change. For illustrative purposes, we give the schematic of step-like load change via controlling the switches of air-conditioners in Fig. 1. Similarly, attackers can achieve LAA via closed-loop control of other DR sources such as electric vehicles and storage batteries.

Unlike the normal load variation, which is usually treated as a step function [27], $P_{id}(t)$ dynamically changes over time, leading to drastically different system responses compared with the "simple" step function-powered LAA.

B. Dynamic False Data Injection Attack

Wherever FDIA occurs w.r.t. SFC, the equivalent FDIA signal $F_d(t)$ can be expressed by the disturbance in the controlled output channel:

$$y_d=y_r+F_d\left(t\right) \tag{2}$$

where y_d and y_r represent the compromised and real controlled output. The multi-area system is considered as an aggregated single system, and the flat frequency control (FFC) mode is used herein. Due to the spatial-temporal difference of different measuring points, the frequency responses would be different even in the non-compromised situations. Hence, it would be difficult to detect cyber attacks via comparing measurements from different nodes. As with D-LAA, $F_d(t)$ in D-FDIA is time-varying but independent of the system state (frequency). The working principle of D-FDIA and D-LAA is illustrated in Fig. 2.

C. Dynamic Attack Input Signal

$P_{id}(t)$ and $F_d(t)$ are equivalent to the dynamic attack input signal (DAIS) u_a in the mathematical model of SFC. Several widely used attack templates include [28]: 1) pulse attack; 2) step attack; 3) periodic attack; and 4) ramp attack.

Besides the time-varying characteristic, the uncertainty is another feature of DAIS considering the irregular behaviors of

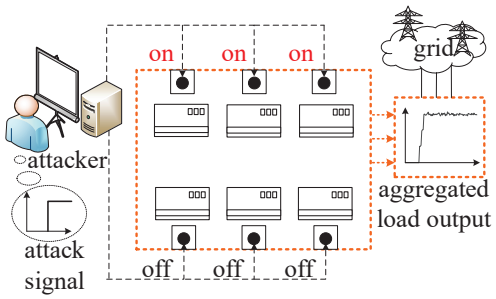


Fig. 1. Schematic diagram of D-FDIA and D-LAA in the SFC system

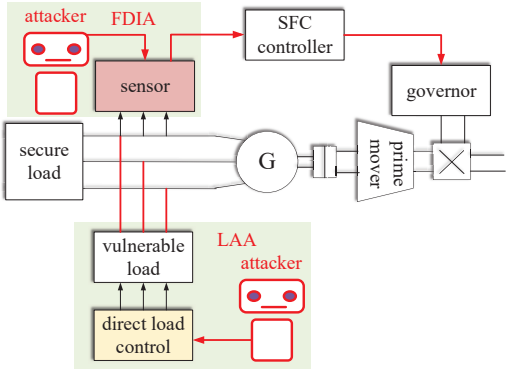


Fig. 2. Schematic diagram of D-FDIA and D-LAA in the SFC system

the attacker. In this paper, the stochastic differential equation (SDE) is used to characterize this uncertainty [29]:

$$du_a=\mu\left(t,u_a\right)dt+\sigma\left(t,u_a\right)dB_t \tag{3}$$

where μ and σ are used to measure the short-term increase and variability of u_a. B_t is the continuous-time stochastic process, which powers the stochastic change of u_a.

III. Mathematical Model of Dynamic Attack on Secondary Frequency Control

Based on the introduction in Section II, we first build the complete dynamic attack model. Then we study the dynamic attack (D-LAA and D-FDIA) upon SFC by focusing on two points:

- ***System Stability Evaluation*** For a specific attack scenario, e.g., D-LAA featuring step attack signal, we evaluate the system stability.
- ***System Response Derivation*** Besides the long-term stability analysis, we derive the short-term system responses.

Before we evaluate the system stability under the dynamic attack, we need to establish the compromised system model. This section discusses the models of dynamic systems considering D-LAA and D-FDIA, respectively.

Whether it is D-LAA or D-FDIA, the attack input changes from zero to nonzero values after the attack is launched. These nonzero values are assumed to be within the stability region and the linearized (small-signal) model can still be used to formulate the complete attack model. Large attack

signals will cause the transient instability particularly when the post-attack system is never or slowly achieved. Emergency or protective control should be used in this case, which is not concerned in this paper. In the remainder of this section, the state space representation of the compromised system model under different attack scenarios is briefly derived.

The detailed nonlinear power system model is [30]–[32]:

$$\begin{cases} \dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{z}, \boldsymbol{u}, t) \\ \boldsymbol{0} = \boldsymbol{g}(\boldsymbol{x}, \boldsymbol{z}, \boldsymbol{u}, t) \\ \boldsymbol{y} = \boldsymbol{h}(\boldsymbol{x}, \boldsymbol{z}, \boldsymbol{u}, t) \end{cases} \tag{4}$$

where $\boldsymbol{x} \in \mathbb{R}^n$ represents the vector of system states; $\boldsymbol{z} \in \mathbb{R}^s$ represents the vector of internal algebraic variables; $\boldsymbol{u} \in \mathbb{R}^i$ is the vector of input variables which contain both the control and disturbance inputs; $\boldsymbol{y} \in \mathbb{R}^o$ represents the vector of outputs. $\boldsymbol{f}$, $\boldsymbol{g}$ and $\boldsymbol{h}$ are the nonlinear functions.

A. Mild Attack Considering Stealthiness

Some might argue that attackers can change data or load aggressively, leading to a major disturbance and the ensuing instability. It is a "feasible" plan at first glance. However, the following problems may arise:

- *high likelihood of detection*: Suppose an LAA with a large volume of load change could occur. The power transfers surge up and may not sustain the stable voltage. Then the collapse of voltage causes contingency and triggers a self-protection mechanism. However, this large volume of load change is usually accompanied by large end-users (e.g., a large load aggregator in the transmission system). Unlike residential loads, the consumption of these large end-users is recorded and sent to dispatch centers. Every electrical load has its comparatively stable consumption pattern. An abrupt demand surge will surely raise suspicion and facilitate the detection. Likewise, when attackers inject large false data, it will cause exorbitant generation loss or gain in a short time, which is deemed as the generator fault, and make the attack more detectable. From the perspective of attackers, they do not want to expose their identities. For example, the high likelihood of detection indicates we can block attacks out, which is not in the interest of attackers.
- *operational restriction*: In practice, the frequency regulation units have capacity limits. Even if attackers produce a large control error by injecting large false data. The generation change cannot exceed the limits. Likewise, the capacity of adjustable or switchable loads is fixed. Attackers cannot change it arbitrarily.

In this paper, we assume that attackers mildly attack SFC to overcome the two problems above. The mild attack can simultaneously affect the frequency quality and have more stealthiness, which is more desirable in the long run. Mild attacks not only can shun the detection but also cause damages. For example, enduring frequency deviations under mild step attacks could lead to the fracture of turbine blade and deteriorated quality of motor-driven products. The oscillation under periodic attacks will make it difficult to estimate the real mode and mode shape of the power system. As for this mild attack, we can use the small-signal model to characterize the compromised system by linearizing (4). Specifically, we present the compromised SFC model as follows.

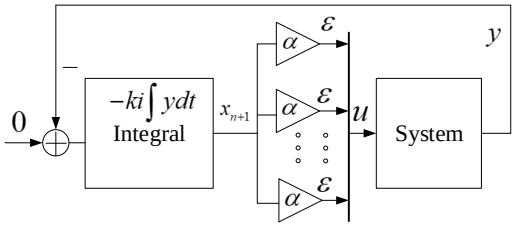


Fig. 3. Schematic diagram of Integral controller-based secondary frequency control system

B. Dynamic System Model Considering D-LAA

1) Deterministic System Model Considering D-LAA: Suppose that the internal algebraic variables are not perturbed. By linearizing the nonlinear power system model (4) around the equilibria and preserving only the active power-frequency control-related control inputs (e.g., the reference power of the governor), the attack system model can be written by a deterministic state-space model:

$$\begin{cases} \dot{\boldsymbol{x}} = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{B_u}\boldsymbol{u} + \boldsymbol{B_d}\boldsymbol{P_d} \\ y = c^T\boldsymbol{x} \end{cases} \tag{5}$$

where Δ for the variables or inputs is omitted in the linearized small-signal system. $\boldsymbol{u} \in \mathbb{R}^r$ herein means the control input, which is the vector of the reference power adjustment. The D-LAA vector $\boldsymbol{P_d} \in \mathbb{R}^p$ is the disturbance input. $\boldsymbol{A}$, $\boldsymbol{B_u}$, $\boldsymbol{B_d}$, and c represent the coefficient matrix or vector. The center-of-inertia (COI) system frequency (weighted sum of rotor speeds) is denoted by: $y = \sum_j H_j\omega_j \Big/ \sum_j H_j$. Unlike step function-like normal load variation, $\boldsymbol{P_d}$ assumes more forms, e.g., the pulse function and periodic function.

Suppose that SFC uses the integral controller and the allocation coefficients $\alpha = 1/r$, we have $\boldsymbol{u} = \begin{bmatrix} \varepsilon & \varepsilon & \cdots & \varepsilon \end{bmatrix}^T \in \mathbb{R}^{r\times 1}$, where $\varepsilon = -k_i/r \int c^T x dt$. The control input $\boldsymbol{u}$ is shown in Fig. 3.

Let the extended state be $x_{n+1} = r\varepsilon$. (5) can be transformed into:

$$\begin{cases} \dot{\bar{\boldsymbol{x}}} = \bar{\boldsymbol{A}}\bar{\boldsymbol{x}} + \bar{\boldsymbol{B}}_{\boldsymbol{d}}\boldsymbol{P_d} \\ y = \bar{c}^T\bar{\boldsymbol{x}} \end{cases} \tag{6}$$

where $\bar{\boldsymbol{x}} = \begin{bmatrix} \boldsymbol{x}^T & x_{n+1} \end{bmatrix}^T$, $\boldsymbol{R} = \begin{bmatrix} 1/r & \cdots & 1/r \end{bmatrix}^T$

$$\bar{\boldsymbol{A}} = \begin{bmatrix} \boldsymbol{A} & \boldsymbol{0} \\ -k_i c^T & 0 \end{bmatrix} + \begin{bmatrix} \boldsymbol{B_u} \\ \boldsymbol{0} \end{bmatrix} \boldsymbol{R} \begin{bmatrix} \boldsymbol{0_{1\times n}} & 1 \end{bmatrix}$$

$$\bar{\boldsymbol{B}}_{\boldsymbol{d}} = \begin{bmatrix} \boldsymbol{B_d^T} & \boldsymbol{0_{p\times 1}} \end{bmatrix}^T$$

$$\bar{c}^T = \begin{bmatrix} c^T & 0 \end{bmatrix}^T$$

From (6), the only exogenous disturbance is the LAA vector $\boldsymbol{P_d}$. It means that the system response of y is determined by the characteristics of $\boldsymbol{P_d}$ once all the endogenous system parameters are fixed, i.e., $\bar{\boldsymbol{A}}$, $\bar{\boldsymbol{B}}_{\boldsymbol{d}}$ are constant matrices; $\bar{c}$ is a constant vector.

2) Stochastic System Model Considering D-LAA: Based on (3), $\boldsymbol{P_d}$ herein is thus expressed by:

$$d\boldsymbol{P_d} = \boldsymbol{\mu}\left(t, \boldsymbol{P_d}\right) dt + \boldsymbol{\sigma}\left(t, \boldsymbol{P_d}\right) d\boldsymbol{B_t} \tag{7}$$

Since $\boldsymbol{P}_d$ is a non-zero attack vector, by dividing both sides of (7) by dt and letting $\boldsymbol{P_d}$ be the $(n+2)^{th}$ to $(n+p+1)^{th}$ extended states. (6) can be rewritten by:

$$\begin{cases} \dot{\boldsymbol{z}} = \boldsymbol{A_z}\boldsymbol{z} + \boldsymbol{B_z}\boldsymbol{\xi} \\ y = c_z^T \boldsymbol{z} \end{cases} \tag{8}$$

where $\boldsymbol{z} = \begin{bmatrix} \bar{\boldsymbol{x}}^T & \boldsymbol{P_d}^T \end{bmatrix}^T$,

$$\boldsymbol{A_z} = \begin{bmatrix} \bar{\boldsymbol{A}} & \bar{\boldsymbol{B}}_{\boldsymbol{d}} \\ \boldsymbol{0} & \boldsymbol{\mu}\left(\boldsymbol{t}, \boldsymbol{P_d}\right)/\boldsymbol{P_d} \end{bmatrix}$$

$\boldsymbol{B_z} = \begin{bmatrix} \boldsymbol{0} & \boldsymbol{\sigma}^T\left(t, \boldsymbol{P_d}\right) \end{bmatrix}^T$, $\boldsymbol{\xi} = d\boldsymbol{B_t}/dt$, $c_z^T = \begin{bmatrix} \bar{c}^T & \boldsymbol{0} \end{bmatrix}^T$. From (8), it can be learned that the volatile $\boldsymbol{P_d}$ is considered as the combination of exogenous disturbance ($\boldsymbol{\xi}$ and $\boldsymbol{\sigma}\left(t, \boldsymbol{P_d}\right)$) and endogenous disturbance ($\boldsymbol{\mu}\left(t, \boldsymbol{P_d}\right)$) for the SFC system.

C. Dynamic System Model Considering D-FDIA

1) Deterministic System Model Considering D-FDIA: By ignoring the normal load variation, the attack system model considering D-FDIA can be written by:

$$\begin{cases} \dot{\boldsymbol{x}} = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{B_u}\boldsymbol{u} \\ y = c^T\boldsymbol{x} + F_d \end{cases} \tag{9}$$

As with (5), let $\varepsilon = k_i/r \int (c^T\boldsymbol{x} + F_d)dt$; supposing that $\boldsymbol{u} = \begin{bmatrix} \varepsilon & \varepsilon & \cdots & \varepsilon \end{bmatrix}^T \in \mathbb{R}^{r\times 1}$, let the extended state be $x_{n+1} = r\varepsilon$, (9) can be transformed into:

$$\begin{cases} \dot{\bar{\boldsymbol{x}}} = \bar{\boldsymbol{A}}\bar{\boldsymbol{x}} + \bar{\boldsymbol{G}}_{\boldsymbol{d}} F_d \\ y_r = \bar{c}^T\bar{\boldsymbol{x}} \end{cases} \tag{10}$$

where y_r is the actual frequency; $\bar{\boldsymbol{G}}_{\boldsymbol{d}} = \begin{bmatrix} \boldsymbol{0} & 1 \end{bmatrix}^T$, and the rest of the matrices are the same as (6).

2) Stochastic System Model Considering D-FDIA: Based on (3), F_d is thus expressed by:

$$dF_d = \mu\left(t, F_d\right) dt + \sigma\left(t, F_d\right) dB_t \tag{11}$$

Let F_d be x_{n+2}, (10) can be rewritten as:

$$\begin{cases} \dot{\boldsymbol{\varsigma}} = \boldsymbol{A_\varsigma}\boldsymbol{\varsigma} + \boldsymbol{B_\varsigma}\xi \\ y = c_\varsigma^T\boldsymbol{\varsigma} \end{cases} \tag{12}$$

$\boldsymbol{\varsigma} = \begin{bmatrix} \bar{\boldsymbol{x}}^T & F_d^T \end{bmatrix}^T$,

$$\boldsymbol{A_\varsigma} = \begin{bmatrix} \bar{\boldsymbol{A}} & \bar{\boldsymbol{G}}_{\boldsymbol{d}} \\ 0 & \mu\left(t, F_d\right)/F_d \end{bmatrix}$$

$\boldsymbol{B_\varsigma} = \begin{bmatrix} \boldsymbol{0} & \sigma^T\left(t, F_d\right) \end{bmatrix}^T$, $\xi = dB_t/dt$, $c_\varsigma^T = \begin{bmatrix} \bar{c}^T & 0 \end{bmatrix}^T$.

Based on the above derived attack models (6), (8), (10) and (12), it can be seen that the introduction of stochastic process makes the system subject to the exogenous and endogenous disturbances, while the time-varying deterministic FDIA can be treated as exogenous disturbances.

IV. Stability Evaluation of Dynamic Attacks on Secondary Frequency Control

Based on the compromised SFC models in Section III, the stability is evaluated. Since the system frequency is the main interested variable in SFC, the influence of the attack input u_a upon y is studied.

A. Stability Evaluation of Deterministic Attack System

As for the mild attack mode that corresponds to the small-signal model with bounded attack inputs, the following principle holds.

Theorem 1. *The deterministic attack systems (6) and (10) are bounded-input-bounded-output (BIBO) stable.*

Proof. The S-domain representation of (6) and (10) can be expressed by:

$$Y\left(s\right) = \boldsymbol{G}\left(s\right)\boldsymbol{U_a}\left(s\right) \tag{13}$$

The impulse response $g_j(t)$ from the j^{th} input to the output can be calculated by:

$$\begin{aligned} g_j\left(t\right) &= \mathcal{L}^{-1}\left\{G_j\left(s\right)\right\} \\ &= \mathcal{L}^{-1}\left\{\sum_{i=1}^{n+1}\sum_{j=1}^{q_i}\frac{\varphi_i}{(s-\lambda_i)^j}\right\} \\ &= \sum_{i=1}^{n+1}\sum_{j=1}^{q_i} t^{j-1}e^{\lambda_i t} \end{aligned} \tag{14}$$

where λ_i is the eigenvalue of $\boldsymbol{G}(s)$ or $\bar{\boldsymbol{A}}$; q_i is the multiplicity index of λ_i; φ_i is the time-domain coefficient. For the tuned control power system model, $Re(\lambda_i) < 0$ is satisfied. Based on L'Hopital's rule, $t^{j-1}e^{\lambda_i t}$ converges to zero over time. Hence, $\int_0^\infty |g_j\left(t\right)|\, dt < M < \infty$, and $g_j(t)$ is absolutely integrable. Then the system is BIBO stable. □

Since both (6) and (10) are BIBO stable by Theorem 1, what are the differences between deterministic D-LAA and D-FDIA? Note that the extended state x_{n+1} in (10) is $x_{n+1} = k_i \int (c^T\boldsymbol{x} + F_d)dt$, BIBO stability means that x_{n+1} is bounded and $c^T\boldsymbol{x} + F_d$ is absolutely integrable:

$$c^T x\left(t\right) + F_d\left(t\right) = F\left(t\right), t \in \ominus \tag{15}$$

where F represents a nonzero value; $\ominus$ represents the finite time set. It means that the frequency $y_r = c^T x$ will be the opposite of $F_d(t)$ in most of the time. Similarly, x_{n+1} in (6) is the integration of the frequency. The boundedness of x_{n+1} means that $y_r = c^T x$ is asymptomatically stable and irrespective of $\boldsymbol{P_d}$.

The above description presents the quasi-steady state long-term stability analysis. In the following, the dynamic responses of y concerning different deterministic attack signals in subsection II-C are derived. the solution of (6) is written by:

$$\bar{\boldsymbol{x}}\left(t\right) = e^{\bar{\boldsymbol{A}}t}\bar{\boldsymbol{x}}\left(0\right) + e^{\bar{\boldsymbol{A}}t}\int_0^t e^{-\bar{\boldsymbol{A}}\tau}\bar{\boldsymbol{B}}_{\boldsymbol{d}}\boldsymbol{P_d}\left(\tau\right)d\tau \tag{16}$$

The homogeneous state response $\bar{\boldsymbol{x}}_{\boldsymbol{h}}(t) = e^{\bar{\boldsymbol{A}}t}\bar{\boldsymbol{x}}\left(0\right)$ converges to zero and is not considered. The forced state response $\bar{\boldsymbol{x}}_{\boldsymbol{f}}(t)$ is determined by $\boldsymbol{P_d}$. For convenience of analysis, P_{di} from one certain input channel i is investigated. The remaining channels can achieve similar conclusions.

1) Pulse Attack: In this context, one has:

$$\begin{aligned} \bar{\boldsymbol{x}}_{\boldsymbol{fi}}\left(t\right) = {} & e^{\bar{\boldsymbol{A}}t}\int_0^{t_1} e^{-\bar{\boldsymbol{A}}\tau}\bar{\boldsymbol{B}}_{\boldsymbol{di}}0d\tau + e^{\bar{\boldsymbol{A}}t}\int_{t_1}^{t_2} e^{-\bar{\boldsymbol{A}}\tau}\bar{\boldsymbol{B}}_{\boldsymbol{di}}P_{di}d\tau \\ & + e^{\bar{\boldsymbol{A}}t}\int_{t_2}^{t} e^{-\bar{\boldsymbol{A}}\tau}\bar{\boldsymbol{B}}_{\boldsymbol{di}}0d\tau \end{aligned} \tag{17}$$

where t_1 and t_2 are the boundaries of time interval. (17) can be rewritten by:

$$\bar{\boldsymbol{x}}_{\boldsymbol{fi}}(t) = e^{\bar{\boldsymbol{A}}t} \int_{t_1}^{t_2} e^{-\bar{\boldsymbol{A}}\tau} \bar{\boldsymbol{B}}_{\boldsymbol{di}} P_{di} d\tau \tag{18}$$

The integration in (18) is bounded by M_b, it means that $\|\bar{\boldsymbol{x}}_{\boldsymbol{fi}}(t)\| \leq \left\|e^{\bar{\boldsymbol{A}}t}\right\| M_b$. Hence $\lim_{t\to\infty} \bar{\boldsymbol{x}}_{\boldsymbol{fi}}(t) = 0$ and $\lim_{t\to\infty} \bar{\boldsymbol{x}}_{\boldsymbol{f}}(t) = \lim_{t\to\infty} \sum_i \bar{\boldsymbol{x}}_{\boldsymbol{fi}}(t) = 0$. It indicates that not only y but also all the other states are not affected by the pulse attack in the long term operation.

2) Step Attack: For the convenience of analysis, supposing that the attack occurs at $t = 0s$, it follows that:

$$\bar{\boldsymbol{x}}_{\boldsymbol{fi}}(t) = e^{\bar{\boldsymbol{A}}t} \int_{0}^{t} e^{-\bar{\boldsymbol{A}}\tau} \bar{\boldsymbol{B}}_{\boldsymbol{di}} P_{di} d\tau \tag{19}$$

By ignoring the multiplicity of the eigenvalues and expanding (19), it follows that:

$$\bar{\boldsymbol{x}}_{\boldsymbol{fi}}(t) = \boldsymbol{E}\boldsymbol{\Gamma}\boldsymbol{E}^{-1}\bar{\boldsymbol{B}}_{\boldsymbol{di}} P_{di} \tag{20}$$

where

$$\boldsymbol{\Gamma} = \begin{bmatrix} \frac{1}{-\lambda_1}\left(1 - e^{\lambda_1 t}\right) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \frac{1}{-\lambda_{n+1}}\left(1 - e^{\lambda_{n+1} t}\right) \end{bmatrix}$$

$\boldsymbol{E}$ is the square $(n+1)\times(n+1)$ matrix whose i^{th} column is eigenvector $\boldsymbol{q_i}$ of $\bar{\boldsymbol{A}}$. Hence, y can be ultimately expressed by the weighted sum of $-1/\lambda_i\left(1 - e^{\lambda_i t}\right)$. Since (6) is BIBO stable, x_{n+1} is bounded. Then $y = \bar{c}^T\bar{\boldsymbol{x}}$ is absolutely integrable and $\lim_{t\to\infty} y(t) = 0$. In other words, the dynamic response of y takes the form of damped oscillation before it achieves the exponential stability.

3) Ramp Attack: Unlike the constant P_{di} in (19), P_{di} herein is $P_{di} = Rt$, where R is the ramping rate. (20) can thus be transformed into:

$$\bar{\boldsymbol{x}}_{\boldsymbol{fi}}(t) = e^{\bar{\boldsymbol{A}}t} \int_{0}^{t} e^{-\bar{\boldsymbol{A}}\tau} \bar{\boldsymbol{B}}_{\boldsymbol{di}} R t d\tau \tag{21}$$

(21) can be solved as:

$$\bar{\boldsymbol{x}}_{\boldsymbol{fi}}(t) = \boldsymbol{E}\boldsymbol{\Psi}\boldsymbol{E}^{-1}\bar{\boldsymbol{B}}_{\boldsymbol{di}} R \tag{22}$$

where

$$\boldsymbol{\Psi} = \begin{bmatrix} \left(-\frac{t\lambda_1+1}{\lambda_1^2}e^{-\lambda_1 t}\right) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & -\frac{t\lambda_{n+1}+1}{\lambda_{n+1}^2}e^{-\lambda_{n+1} t} \end{bmatrix}$$

The exponential divergence of $e^{-\lambda_i t}$ leads to the the divergence of y. In practice, since the ramp attack signal Rt eventually 'breaks' the boundary of the stability region. Hence it is the nonlinear model rather than the linearized small-signal one that will be applied in this case. The dynamic responses are still divergent but more complex.

4) Periodic Attack: Since all the periodic signals can be written by a weighted sum of sinusoids, for convenience of analysis, the periodic attack signal is assumed to be the sinusoidal function $P_{di} = a\sin(wt)$, where a and w represent the amplitude and angular frequency. The phase lag is set zero for brevity. (20) can thus be transformed into:

$$\bar{\boldsymbol{x}}_{\boldsymbol{fi}}(t) = e^{\bar{\boldsymbol{A}}t} \int_{0}^{t} e^{-\bar{\boldsymbol{A}}\tau} \bar{\boldsymbol{B}}_{\boldsymbol{di}} a sin(wt) d\tau \tag{23}$$

(23) can be solved as:

$$\bar{\boldsymbol{x}}_{\boldsymbol{fi}}(t) = \boldsymbol{E}\mathbf{T}\boldsymbol{E}^{-1}\bar{\boldsymbol{B}}_{\boldsymbol{di}} P_{di} \tag{24}$$

$$\mathbf{T} = \begin{bmatrix} \eta_1\cos(wt) + \rho_1\sin(wt) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \eta_{n+1}\cos(wt) + \rho_{n+1}\sin(wt) \end{bmatrix}$$

$$\eta_i = \frac{aw}{w^2 + \lambda_i^2}, \rho_i = \frac{a\lambda_i}{w^2 + \lambda_i^2}$$

Hence, y can be expressed by:

$$y = \sum\nolimits_i \kappa_i \left(\eta_i \cos(wt) + \rho_i \sin(wt)\right) \tag{25}$$

Since κ_i and λ_i are fixed, y is affected by adjusting a and w. (25) can be transformed into:

$$y = \sum\nolimits_i \kappa_i \frac{a}{\sqrt{w^2 + \lambda_i^2}} \cos(wt + \vartheta_i) \tag{26}$$

where $\cos\vartheta_i = w \Big/ \sqrt{w^2 + \lambda_i^2}$. When w is very small, ϑ_i is considered approximately $\vartheta_i = \pi/2 + 2k\pi$. Therefore $\cos\sqrt{w^2 + \lambda_i^2}$ is approximately zero. Then the magnitude of $a \Big/ \sqrt{w^2 + \lambda_i^2}$ decreases by increasing w, while the magnitude of $cos(wt + \vartheta_i)$ increases by increasing w. Note that the increase weighs more than the decrease for y, meaning that the magnitude of y increases w.r.t. w. When w continues to grow beyond the critical value, this increase weighs much less than the decrease. In this case, y is equivalent to $a \Big/ \sqrt{w^2 + \lambda_i^2} v$, which monotonically decreases w.r.t. w. That is to say, the attacker will try in vain to deteriorate the system response by more frequently changing the periodic attack signal.

The dynamic responses of y for (10) can be similarly derived under different attack signals. The details are omitted for brevity.

B. Stability Evaluation of Stochastic Attack System

The differential equations of (8) and (12) can be uniformly expressed by:

$$\dot{\boldsymbol{\psi}} = \boldsymbol{A}_{\boldsymbol{\psi}}\boldsymbol{\psi} + \boldsymbol{B}_{\boldsymbol{\psi}}\boldsymbol{\xi} \tag{27}$$

Note that (3) only gives the general definition of the stochastic process. The discrete-time stochastic processes (with finite elements in the index set) usually do not change the inner system dynamics, which indicates that they have no influence on system stability. Hence we use two classic continuous-time stochastic processes to model the attack input:

- *Geometric Brownian processes*:

$$d\boldsymbol{u_a} = \boldsymbol{\mu u_a} dt + \boldsymbol{\sigma u_a} d\boldsymbol{B_t} \tag{28}$$

where $\boldsymbol{\mu} \in \mathbb{Z}^p$; $\boldsymbol{\sigma} \in \mathbb{Z}^p$. In these processes, both the short-term growth and variability are dependent upon the stochastic states $\boldsymbol{u_a}$.

- *Ornstein-Uhlenbeck processes*:

$$d\boldsymbol{u_a} = \boldsymbol{\mu u_a} dt + \boldsymbol{\sigma} d\boldsymbol{B_t} \tag{29}$$

In these processes, only the short-term growth is dependent upon $\boldsymbol{u_a}$.

Supposing that (28) is considered, (27) can be transformed into:

$$\dot{\boldsymbol{\psi}} = \boldsymbol{A_\psi \psi} + \boldsymbol{B_a \psi \xi} \tag{30}$$

where

$$\boldsymbol{B_a} = \begin{bmatrix} \boldsymbol{0_{n\times n}} & 0 & \cdots & 0 \\ 0 & \sigma_1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \sigma_p \end{bmatrix}$$

By using Ito's formula, the time-domain solution of (30) $\boldsymbol{\psi}(t) = \boldsymbol{f}(t, \boldsymbol{B_t})$ can be expanded as:

$$\begin{aligned} d\boldsymbol{\psi}(t) = &\left[\boldsymbol{f_t}(t, \boldsymbol{B_t}) + \tfrac{1}{2}\boldsymbol{f_{BB}}(t, \boldsymbol{B_t})\right] dt \\ &+ \boldsymbol{f_B}(t, \boldsymbol{B_t})\, d\boldsymbol{B_t} \end{aligned} \tag{31}$$

where partial derivatives of $\boldsymbol{f}$ w.r.t. t are denoted by $\boldsymbol{f_t}$; $\boldsymbol{f_B}$ represents partial derivatives w.r.t. $\boldsymbol{B_t}$. Based on (30) and (31), the solution should satisfy the following conditions:

$$\boldsymbol{A_\psi \psi} = \boldsymbol{f_t}(t, \boldsymbol{B_t}) + \frac{1}{2}\boldsymbol{f_{BB}}(t, \boldsymbol{B_t}) \tag{32}$$

$$\boldsymbol{B_a \psi} = \boldsymbol{f_B}(t, \boldsymbol{B_t}) \tag{33}$$

Based on (33), it follows that:

$$\boldsymbol{\psi}(t) = e^{(\boldsymbol{B_a B_t} + \boldsymbol{\gamma}(t))} \tag{34}$$

By differentiating (34) w.r.t. t and $\boldsymbol{B_t}$ (twice), one has:

$$\boldsymbol{A_\psi \psi} = \boldsymbol{\psi}\boldsymbol{\gamma}'(t) + \frac{1}{2}\boldsymbol{B_a^2 \psi} \tag{35}$$

$$\boldsymbol{\gamma}(t) = \left(\boldsymbol{A_\psi} - \frac{1}{2}\boldsymbol{B_a^2}\right) t \tag{36}$$

From (34) and (36), the solution can be expressed as:

$$\boldsymbol{\psi}(t) = e^{\left[\left(\boldsymbol{A_\psi} - 0.5\boldsymbol{B_a^2}\right)t + \boldsymbol{B_a B_t}\right]} \boldsymbol{\psi_0} \tag{37}$$

Theorem 2. *In the i^{th} attack input channel, let $\mu_i - 0.5\sigma_i^2 < 0, \forall i \in p$ for the geometric Brownian processes-based stochastic attack signal. Then, the system in (8) or (12) is stochastically mean stable.*

Proof. Based on (37), it is seen that the stability of the stochastic attack system is dependent upon $\boldsymbol{B_a}$ or σ_i, $\left(\boldsymbol{A_\psi} - 0.5\boldsymbol{B_a^2}\right)$ is:

$$\begin{bmatrix} \boldsymbol{\bar{A}_{n\times n}} & \boldsymbol{W_1} & \cdots & \boldsymbol{W_p} \\ 0 & \mu_1 - 0.5\sigma_1^2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \mu_p - 0.5\sigma_p^2 \end{bmatrix}$$

TABLE I. Stability evaluation results under different attack scenarios

Stability Check Table		
Attack Signal	Deterministic Attack System	Stochastic Attack System
Pulse attack	BIBO stable	N/A
Step attack	BIBO stable	N/A
Ramp attack	unstable	N/A
Periodic attack	BIBO stable	N/A
Geometric Brownian process	N/A	conditionally stochastically mean stable
Ornstein-Uhlenbeck process	N/A	conditionally stochastically mean stable

Its eigenvalues are those of the diagonal block matrix. Since the eigenvalues of $\boldsymbol{\bar{A}}$ lie in the open left half plane (OLHP). If $\mu_i - 0.5\sigma_i^2 < 0, \forall i \in p$, the eigenvalues of $\left(\boldsymbol{A_\psi} - 0.5\boldsymbol{B_a^2}\right)$ lie in the OLHP, $e^{\left(\boldsymbol{A_\psi} - 0.5\boldsymbol{B_a^2}\right)t}$ converges to zero. Also, $E\left(e^{\boldsymbol{B_a B_t}}\right)$ is bounded. It is proved that $\lim_{t\to\infty} E\left\|\boldsymbol{\psi}(t)\right\| = 0$. □

As for Ornstein-Uhlenbeck processes in (29), (27) can be transformed into:

$$\dot{\boldsymbol{\psi}} = \boldsymbol{A_\psi \psi} + \boldsymbol{B_e \xi} \tag{38}$$

where

$$\boldsymbol{B_e} = \begin{bmatrix} \boldsymbol{0} & \cdots & \boldsymbol{0} \\ \sigma_1 & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \ddots & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \sigma_p \end{bmatrix}$$

For the convenience of analysis, it is supposed that B_{it} is the same for all the attack input channels. Hence the solution of (38) is:

$$\boldsymbol{\psi}(t) = e^{\boldsymbol{A_\psi} t}\left[\boldsymbol{\psi_0} + \int_o^t e^{-\boldsymbol{A_\psi} s}\boldsymbol{B_e} dB_s\right] \tag{39}$$

Theorem 3. *In the i^{th} attack input channel, let $\mu_i < 0, \forall i \in p$ for the Ornstein-Uhlenbeck processes-based stochastic attack signal. Then, (8) or (12) is stochastically mean stable.*

Proof. When $\mu_i < 0, \forall i \in p$, $\boldsymbol{A_\psi}$ is asymptotically stable and $\lim_{t\to\infty} e^{\boldsymbol{A_\psi} t}\boldsymbol{\psi_0} = 0$. It can be proved that $E\left[\int_o^t e^{-\boldsymbol{A_\psi} s}\boldsymbol{B_e} dB_s\right] = 0$, and then $\lim_{t\to\infty} E\left\|\boldsymbol{\psi}(t)\right\| = 0$ holds. □

In this section, the stability is evaluated for both deterministic and stochastic attack systems. Table I summarizes the above results. From Table I, it is learned that BIBO stability can be guaranteed for most of the time-varying deterministic attack systems except for those that suffer from ramp attacks. As for deterministic attack systems, the stochastic attack signals which satisfy either Theorem 2 or 3 can guarantee the stochastic mean stability.

For those attack signals that can destabilize the system, e.g., the ramp attack, some stochastic processes, they all diverge over time. From the perspective of transient stability, these divergent disturbances will force the kinetic energy of power systems to exceed the critical value. The kinetic energy cannot be converted to the potential energy, which leads to the loss of

synchronization and the divergence of system responses. Since the dynamic attack signals considered herein are exogenous, a viable solution is to screen out these signals in a timely manner.

V. Case Studies

Two benchmark systems are used to validate the results. Kundur's 4-unit-13-bus system is used to demonstrate the deterministic attack systems. The IEEE 68-bus system is used to demonstrate the stochastic attack system.

A. Simulations of Deterministic Attack Systems

As for the Kundur's system, it is supposed that the load on bus 4 is attacked in D-LAA. The attacker can arbitrarily change the load within a certain boundary (P_{dl}, P_{du}) by considering the capacity limit of the available load. The nominal load is $9.8p.u.$ and (P_{dl}, P_{du}) is set $(5, 15)$. Similarly, $F_d \in (-0.5, 0.5)$.

1) Pulse Attack: As for D-LAA, it is assumed that the pulse attack occurs at $t = 10s$ and endures for $0.5s$ with the amplitude $P_d = 3$. As for D-FDIA, it is assumed that the pulse attack occurs at $t = 10s$ and endures for $0.5s$ with the amplitude $F_d = 0.5$.

2) Step Attack: As for D-LAA, it is assumed that the step attack occurs at $t = 10s$ with the amplitude $P_d = 3$. As for D-FDIA, it is assumed that the step attack occurs at $t = 10s$ with the amplitude $F_d = 0.5$. The dynamic responses of COI frequency under the pulse and step attacks defined above are illustrated in Fig. 4. It is shown in Fig. 4a that the pulse attack only causes an abrupt fluctuation before the system frequency is recovered to the equilibrium. Based on (15), it is learned that $c^T x$ should be the opposite of F_d in most of the time. Hence the red response curve in Fig. 4b shows that D-FDIA using the step signal can lead to the long-term deviation, the value of which is exactly the opposite of 0.5. Also, from Fig. 4c it is seen that the pulse attack only causes the pulse-like change of the control efforts while the step attack leads to enduring control effort change. Whatever the dynamic responses are under these two types of attacks, the BIBO stability holds, which validates the results in Table I.

3) Periodic Attack: It is assumed that the periodic D-LAA $asin(wt)$ occurs at $t = 10s$. First, the amplitude a is fixed to 1. w is chosen from the geometric sequence starting from 0.1 and ending at 62.5 (the common ratio is set as 5). Second, the angular rotation speed is fixed to 1. a is chosen from the arithmetic sequence starting from 0.5 and ending at 3 (the common difference is set as 0.5). The periodic D-FDIA $0.1sin(wt)$ occurs at $t = 10s$. w is chosen from the geometric sequence starting from 0.1 and ending at 62.5 (the common ratio is set as 5). Fig. 5. depicts the dynamic COI frequency responses. It is noted in Fig. 5a that the magnitude of y increases from $w = 0.1$ to $w = 0.5$ significantly. Then it slightly decreases when $w = 2.5$ before significantly decreasing from $w = 12.5$ to $w = 62.5$, which validates the analysis about the dynamic responses of y in subsection IV-A4. Also, from Fig. 5b it is learned that the magnitude of y increases with a. As for the simulation results of periodic D-FDIA in Fig. 5c, the magnitude of y just decreases as w increases from 0.1 to 62.5. It means that the critical value for D-FDIA is smaller than D-LAA. The reasons can be interpreted as follows. The input channels of D-LAA and D-FDIA are different, leading to different sets of $\{\lambda_i\}$ that contributes to y. These two different $\{\lambda_i\}$ in return cause the difference of the critical values.

B. Simulations of Stochastic Attack Systems

The schematic diagram of IEEE 16-unit-68-bus system is shown in Fig. 6. It contains the complete electromechanical models of generators, controllers (e.g., the power system stabilizer and automatic voltage control) and the network model.

1) Ornstein-Uhlenbeck Process-Based Attack: The stochastic D-LAA occurs at load buses 55, 56, 59, and 60 when $t = 5s$, $t = 10s$, $t = 15s$, and $t = 20s$, respectively. μ in (29) for the attack inputs in these four channels are set as $\mu = -0.5, -1, -1.5$, and -2, respectively. All of values of μ satisfy Theorem 3. It is assumed that $\sigma = 0.01$ in (28), while the mean of the stochastic process is set as 0.5. The stochastic attack input for D-FDIA has the same setting except that the mean is set as 0. 1000 simulations are implemented to obtain the statistical features (the mean value) of the system frequency.

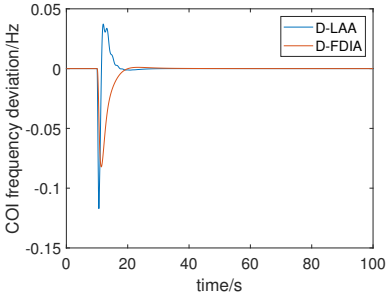
2) Geometric Brownian Process-Based Attack: As for the stochastic attack input for D-LAA, it is also supposed that it occurs at load buses 55, 56, 59, and 60 when $t = 5s$, $t = 10s$, $t = 15s$, and $t = 20s$, respectively. The parameters in (28) for these four attack signals are set as $\mu = 0.001, \sigma = 0.1$, $\mu = 0.0015, \sigma = 0.15$, $\mu = 0.002, \sigma = 0.2$, and $\mu = 0.0025, \sigma = 0.25$. All satisfy $\mu - 0.5\sigma^2 < 0$ in Theorem 2. 1000 simulations are implemented to obtain the statistical features (the mean value) of the system frequency.

The dynamic frequency responses under these three attack scenarios are shown in Fig. 7. As can be seen from the yellow dashed line in Fig. 7a and 7b, when $\mu < 0$ satisfies Theorem 3 for these four stochastic attack signals, attack systems considering both D-LAA and D-FDIA are stochastically mean stable. $E(y)$ converges to zero when the Ornstein-Uhlenbeck process-based attack is implemented in both the load input and controlled output channel. Similarly, when Theorem 2 is satisfied in Fig. 7c, the stochastic mean stability is guaranteed.

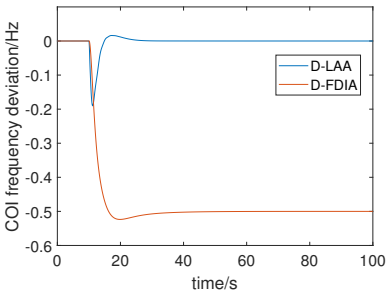
C. Simulations of Coordinated Attack Systems

Subsections V-A and V-B only consider unilateral attack activities (either LAA or FDIA). Attackers may also implement coordinated attacks by attacking loads and frequency data simultaneously. The principle of coordination is: *Perform LAA and FDIA simultaneously. LAA's influence should better not offset FDIA's.* For example, when attackers inject positive false data to cause the positive control errors, generators will reduce production (which corresponds to negative control errors) under SFC control, causing the frequency drop. If attackers simultaneously decrease loads (negative load change), this temporary frequency increase under LAA will offset the frequency drop under FDIA.

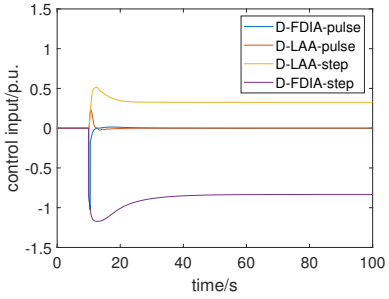
Since compromised system models in Section III belong to the small-signal models; based on the superstition principle



(a) Dynamic COI frequency deviation excursion under the pulse attack

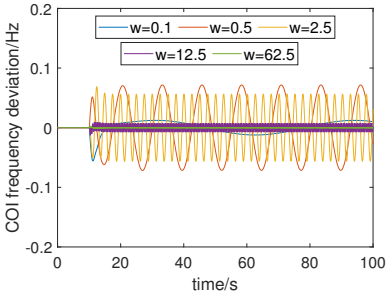


(b) Dynamic COI frequency deviation excursion under the step attack

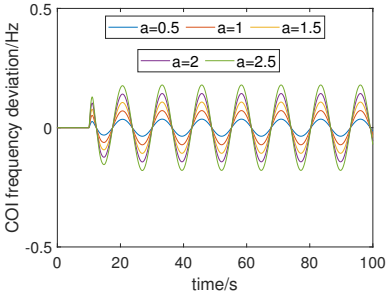


(c) Control efforts under the pulse and step attacks

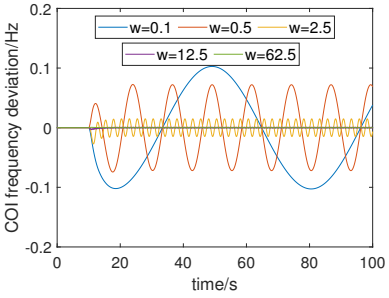
Fig. 4. Simulation results under the pulse and step attack using Kundur's 4-unit-13-bus system



(a) Dynamic COI frequency deviation excursion under the periodic D-LAA with different w



(b) Dynamic COI frequency deviation excursion under the periodic D-LAA with different a



(c) Dynamic COI frequency deviation excursion under the periodic D-FDIA with different w

Fig. 5. Simulation results under the periodic attack using Kundur's 4-unit-13-bus system

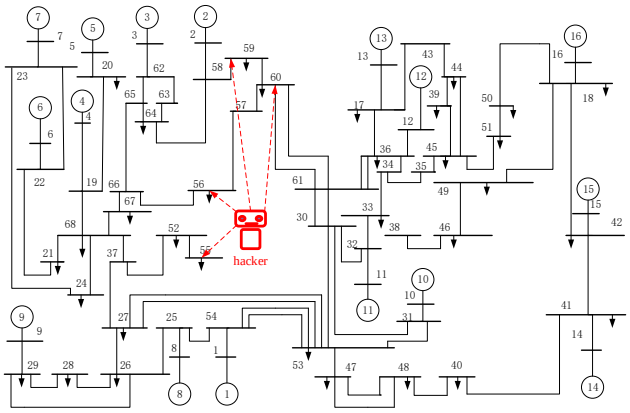


Fig. 6. Schematic diagram of IEEE 16-unit-68-bus system

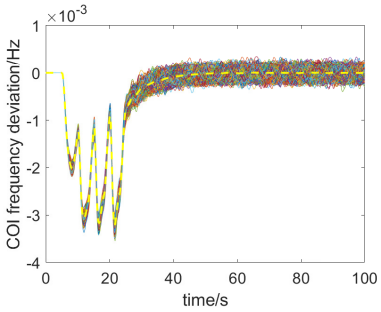
[33], compromised systems under coordinated attacks are BIBO stable. To validate this conclusion, we simulate three coordinated attack scenarios: 1) coordinated pulse attacks; 2) coordinated step attacks, and 3) coordinated stochastic attacks. In each attack scenario, we randomly simulate 100 pairs of LAA and FDIA, and Fig. 8 validates the BIBO stability under coordinated attacks.

VI. Conclusions and Future Work

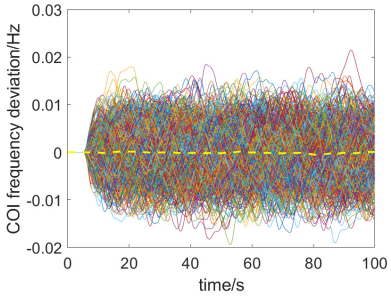
This paper answers the basic question of how dynamic cyber attacks, in the form of false data or load injection, affect SFC stability. Based on the theoretical and simulation analyses in Section IV and V, the following conclusions can be drawn:

- As for the SFC system under deterministic time-varying attack signal, whatever it is D-LAA or D-FDIA, the system is mathematically proved to be BIBO stable. The main differences concerning different attack signals lie in the dynamic response of the interested variable as well as the boundary of the frequency excursions when the system suffers D-FDIA.
- As for the stochastic attack, whatever it is D-LAA or D-FDIA, all attack systems are stochastically mean stable as long as the attack input signal satisfies Theorem 2 and 3, which can be easily satisfied, as long as the attacker is not aggressive and inject some exorbitant divergent stochastic signals into the systems.

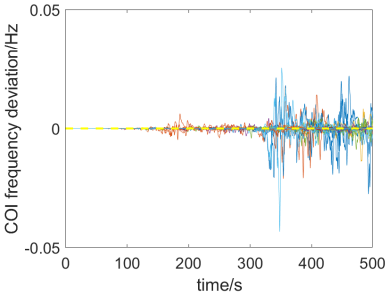
As for the deterministic D-LAA or D-FDIA, it can also be found that the pulse attack barely affects the system frequency. While the step attack can enduringly change the system frequency in D-FDIA (though the BIBO stability still holds). More interesting conclusions come from the periodic attack, which will decrease the magnitude of oscillated system frequency when the frequency surpasses certain threshold values. In future work, we will focus on the "aggressive" dynamic attacks that lead to emergency frequency control instead of SFC. Though stealthy attackers would not readily switch to this aggressive mode, they may at times opt for it to cause the grid instantaneous huge damage. Since it will take some time to achieve the detection and isolation. We need to investigate post-attack stability analyses regarding with 1) how "big" the attack signal can be and 2) when to cut off



(a) Dynamic COI frequency deviation excursion considering Ornstein-Uhlenbeck process-based D-LAA

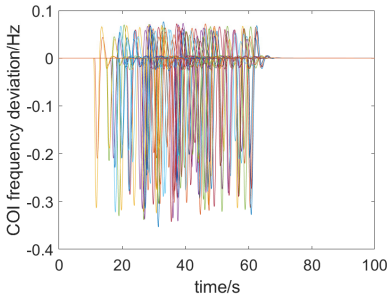


(b) Dynamic COI frequency deviation excursion considering Ornstein-Uhlenbeck process-based D-FDIA

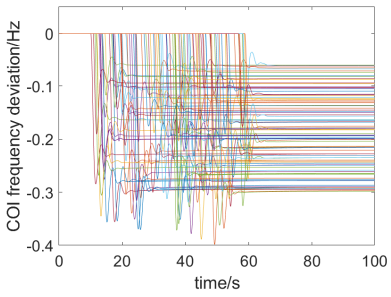


(c) Dynamic COI frequency deviation excursion considering geometric Brownian process-based D-LAA

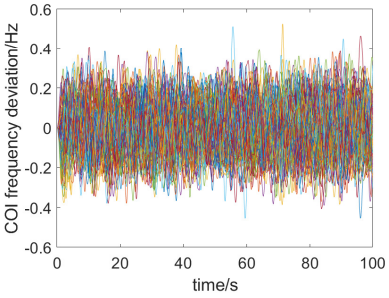
Fig. 7. Simulation results under the stochastic attack using IEEE 16-unit-68-bus system



(a) Dynamic COI frequency deviation excursion under coordinated pulse attacks



(b) Dynamic COI frequency deviation excursion under coordinated step attacks



(c) Dynamic COI frequency deviation excursion under coordinated stochastic attacks

Fig. 8. Simulation results under coordinated attacks using Kundur's 4-unit-13-bus system

the attack signal to prevent the instability. The magnitude of these "intensive" attack signals exceeds the stability region and feedback control-based small-signal frequency control model in this paper demands complete reformation. Energy-based stability criteria will be studied to assess the post-attack system stability after these "intensive" attack signals are detected and cut off.

REFERENCES

[1] X. Yu and Y. Xue, "Smart grids: A cyber–physical systems perspective," *Proc. IEEE*, vol. 104, no. 5, pp. 1058–1070, 2016.

[2] F. Farivar, M. S. Haghighi, A. Jolfaei, and M. Alazab, "Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT," *IEEE Trans. Ind. Informa.*, vol. 16, no. 4, pp. 2716–2725, 2019.

[3] A. Sawas, H. Khani, and H. Farag, "On the resiliency of power and gas integration resources against cyber-attacks," *IEEE Trans. Ind. Informa.*, 2020. in press.

[4] T. Khan and I. Tomic, "Securing industrial cyber-physical systems: A run-time multi-layer monitoring," *IEEE Trans. Ind. Informa.*, 2020. in press.

[5] M. Cui, J. Wang, and M. Yue, "Machine learning-based anomaly detection for load forecasting under cyberattacks," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5724–5734, 2019.

[6] S. Xiao, Q.-L. Han, X. Ge, and Y. Zhang, "Secure distributed finite-time filtering for positive systems over sensor networks under deception attacks," *IEEE Trans. Cybern.*, vol. 50, no. 3, pp. 1220–1229, 2019.

[7] X. Liu, Y. Song, and Z. Li, "Dummy data attacks in power systems," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1792–1795, 2019.

[8] A. Ameli, A. Hooshyar, E. F. El-Saadany, and A. M. Youssef, "An intrusion detection method for line current differential relays," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 329–344, 2019.

[9] H. Xu, Y. Lin, X. Zhang, and F. Wang, "Power system parameter attack for financial profits in electricity markets," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3438–3446, 2020.

[10] M. Cui and J. Wang, "Deeply hidden moving-target-defense for cyber-secure unbalanced distribution systems considering voltage stability," *IEEE Trans. Power Syst.*, 2020. early access.

[11] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: A distributed and trusted authentication system," *IEEE Trans. Ind. Informa.*, vol. 16, no. 3, pp. 1972–1983, 2019.

[12] K. Gai, Y. Wu, L. Zhu, Z. Zhang, and M. Qiu, "Differential privacy-based blockchain for industrial internet-of-things," *IEEE Trans. Ind. Informa.*, vol. 16, no. 6, pp. 4156–4165, 2019.

[13] Z. Guan, J. Li, L. Zhu, Z. Zhang, X. Du, and M. Guizani, "Toward delay-tolerant flexible data access control for smart grid with renewable energy resources," *IEEE Trans. Ind. Informa.*, vol. 13, no. 6, pp. 3216–3225, 2017.

[14] K. Wang, J. Wu, X. Zheng, A. Jolfaei, J. Li, and D. Yu, "Leveraging energy function virtualization with game theory for fault-tolerant smart grid," *IEEE Trans. Ind. Informa.*, 2020. in press.

[15] H. Davarikia and M. Barati, "A tri-level programming model for attack-resilient control of power grids," *J. Mod. Power Syst. Clean Energy*, vol. 6, no. 5, pp. 918–929, 2018.

[16] C. Chen, M. Cui, X. Fang, B. Ren, and Y. Chen, "Load altering attack-tolerant defense strategy for load frequency control system," *Appl. Energy*, vol. 280, p. 116015, 2020.

[17] J. Duan, H. Xu, W. Liu, J.-C. Peng, and H. Jiang, "Zero-sum game based cooperative control for onboard pulsed power load accommodation," *IEEE Trans. Ind. Informa.*, vol. 16, no. 1, pp. 238–247, 2019.

[18] M. Khalaf, A. Youssef, and E. El-Saadany, "Joint detection and mitigation of false data injection attacks in AGC systems," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 4985–4995, 2018.

[19] J. Liu, Y. Gu, L. Zha, Y. Liu, and J. Cao, "Event-triggered H_∞ load frequency control for multiarea power systems under hybrid cyber attacks," *IEEE Trans. Syst. Man Cyber.*, vol. 49, no. 8, pp. 1665–1678, 2019.

[20] Z. Wu, H. Mo, J. Xiong, and M. Xie, "Adaptive event-triggered observer-based output feedback $\mathcal{L}_\infty$ load frequency control for networked power systems," *IEEE Trans. Ind. Informa.*, vol. 16, no. 6, pp. 3952–3962, 2019.

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

[22] T. Huang, B. Satchidanandan, P. Kumar, and L. Xie, "An online detection framework for cyber attacks on automatic generation control," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6816–6827, 2018.

[23] A. Ameli, A. Hooshyar, E. F. El-Saadany, and A. M. Youssef, "Attack detection and identification for automatic generation control systems," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4760–4774, 2018.

[24] C. Chen, Y. Chen, J. Zhao, K. Zhang, M. Ni, and B. Ren, "Data-driven resilient automatic generation control against false data injection attacks," *IEEE Trans. Ind. Informa.*, 2021. early access.

[25] R. Tan, H. H. Nguyen, E. Y. Foo, D. K. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 7, pp. 1609–1624, 2017.

[26] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2862–2872, 2016.

[27] H. Huang and F. Li, "Sensitivity analysis of load-damping characteristic in power system frequency regulation," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1324–1335, 2012.

[28] S. Ntalampiras, "Detection of integrity attacks in cyber-physical critical infrastructures using ensemble modeling," *IEEE Trans. Ind. Informa.*, vol. 11, no. 1, pp. 104–111, 2014.

[29] F. Milano and R. Zárate-Miñano, "A systematic method to model power systems as stochastic differential algebraic equations," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 4537–4544, 2013.

[30] Z. Zhu, G. Geng, and Q. Jiang, "Power system dynamic model reduction based on extended Krylov subspace method," *IEEE Trans. Power Syst.*, vol. 31, no. 6, pp. 4483–4494, 2016.

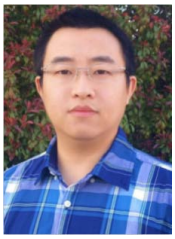
[31] X.-F. Wang, Y. Song, and M. Irving, *Modern power systems analysis*. Springer Science & Business Media, 2010.

[32] C. Huang, K. Zhang, X. Dai, and Q. Zang, "Robust load frequency controller design based on a new strict model," *Electric Power Components and Systems*, vol. 41, no. 11, pp. 1075–1099, 2013.

[33] W. Ma, Y. Zhang, Y. Tang, and J. Tu, "Hirota bilinear equations with linear subspaces of solutions," *Appl. Math. Comput.*, vol. 218, no. 13, pp. 7174–7183, 2012.

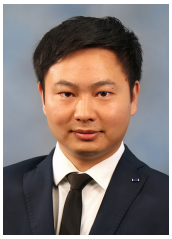
Chunyu Chen received the Ph.D. degree from Southeast University, Nanjing, China, in 2019. From 2017 to 2018, he was a Visiting Student with Southern Methodist University, Dallas, TX, USA. His research interests include power system control, and power system cyber security.

Xiao Zhang received the Ph.D. degrees in electrical engineering from China University of Mining and Technology (CUMT), Xuzhou, China, in 2012. From 2013 to 2014, he was a visiting scholar with Longya Xu in the Ohio State University. His research interests include power system operation and control, power electronics, power quality compensation systems,and electrical drive. Prof. Zhang received two prestigious Second Class Prizes of The State Science and Technology Progress Award, in 2009 and 2017 respectively.



Mingjian Cui received the B.S. and Ph.D. degrees in electrical engineering and automation from Wuhan University, Wuhan, Hubei, China, in 2010 and 2015, respectively. From 2017 to 2020, he was a Research Assistant Professor with Southern Methodist University, Dallas, TX, USA. He was also a Visiting Scholar from 2014 to 2015 with the Transmission and Grid Integration Group, National Renewable Energy Laboratory (NREL), Golden, CO, USA. His research interests include renewable energy, power system operation, power system cybersecurity, power system data analytics, and machine learning. He has authored/coauthored more than 60 peer-reviewed publications. He has served as Editors for journals of IEEE Transactions on Power Systems, IET Generation, Transmission & Distribution, and IEEE Open Access Journal of Power and Energy since 2020. He is Best Reviewers of IEEE Transactions on Smart Grid 2018, IEEE Transactions on Sustainable Energy 2019 and 2020.

Kaifeng Zhang received the Ph.D. degree from Southeast University, Nanjing, China, in 2004. From 2013 to 2014, he was a visiting scholar with Lehigh University. He was also a visiting scholar with Energy Systems Division, Argonne National Laboratory, in 2016. His research interests include power system dispatch and control, wind power and nonlinear control.



Junbo Zhao received the Ph.D. degree from Virginia Tech, Blacksburg, the USA, in 2018. He has published three book chapters and more than 100 peer-reviewed journal and conference papers, where more than 60 appear in IEEE Transactions. He has served as the Editor of IEEE Transactions on Power Systems, IEEE Transactions on Smart Grid, Associate Editor of International Journal of Electrical Power & Energy Systems, Journal of Modern Power System and Clean Energy, and subject editor of IET Generation, Transmission & Distribution, and CSEE Journal of Power and Energy Systems. He received the 2020 IEEE PES Outstanding Engineer Award, the CEEPE 2021-Young Scientist Award, and the 2021 IEEE PES Outstanding Volunteer Award. His research interests include cyber-physical power system modeling, state/parameter estimation, and power system dynamics and stability.

Fangxing Li received the B.S. and M.S. degrees in electrical engineering from Southeast University, Nanjing, China, in 1994 and 1997, respectively, and the Ph.D. degree from Virginia Tech, Blacksburg, VA, USA, in 2001. From 2001 to 2005 he served as a Senior Engineer and then a Principal Engineer at ABB Electrical System Consulting (ESC), a.k.a. ABB Consulting, in Raleigh, NC. His editing services has spanned flagship journals of various IEEE societies. He has served as editors for IEEE Transactions on Power Systems, IEEE Transactions on Sustainable Energy, IEEE Transactions on Smart Grid, IEEE Transactions on Industrial Informatics, etc. He has served the IEEE PES Power System Operation, Planning and Economics (PSOPE) Committee as a chair since 2020. He has been a chair/orgnaizer of numerous panel sessions at a number of international conferences. As the Principal Investigator (PI), Prof. Li received the prestigious R&D 100 Award in 2020. He also received many research-oriented and service-oriented awards in his professional society.