9-2018

Resonance attacks on load frequency control of smart grids

Yongdong WU
Institute for Infocomm Research

Zhuo WEI
Huawei International Pte Ltd

Jian WENG
Jinan University - China

Xin LI
Sinocloud Wisdom Company Ltd

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

DOI: https://doi.org/10.1109/TSG.2017.2661307

Published in IEEE Transactions on Smart Grid, Sep. 2018, Volume: 9, Issue: 5, pp. 4490-4502.
https://doi.org/10.1109/TSG.2017.2661307

Resonance Attacks on Load Frequency Control of Smart Grids

Yongdong Wu, Zhuo Wei, Jian Weng, Xin Li, and Robert H. Deng, *Fellow, IEEE*

***Abstract*—Load frequency control (LFC) is widely employed to regulate power plants in modern power generation systems of smart grids. This paper presents a simple and yet powerful type of attacks, referred to as resonance attacks, on LFC power generation systems. Specifically, in a resonance attack, an adversary craftily modifies the input of a power plant according to a resonance source (e.g., rate of change of frequency) to produce a feedback on LFC power generation system, such that the state of the power plant quickly becomes instable. Extensive computer simulations on popular LFC power generation system models which consist of linear, non-linear, and/or high-order items clearly demonstrate the effectiveness of the proposed attacks. As the attack has very low computational cost and communication overhead, it is easy to launch in resource-limited devices such as intelligent electronic devices. In our simulations, the attacker keeps modified input within the normal operating range so as to invade plausibility and consistency based attack detection methods and yet the modifications can quickly drive the system beyond the admissible boundary. Another interesting finding is that by maliciously modifying the input such as power load and tie-line signal over multi-area interconnection channels, a multi-area LFC power generation system could become unreliable more quickly than a single-area system. Finally, we propose countermeasures on the proposed attacks.**

***Index Terms*—Load frequency control (LFC), rate of change of frequency (RoCoF), cyber-physical system (CPS) security, false data injection (FDI), system stability.**

I. Introduction

SMART grids are reliable, sustainable and safe thanks to ICC (Information, Communication and Control) technologies which enable real-time exchange of system control information among grid subsystems and consumers. However, the open communication architecture of ICC also makes smart grids vulnerable to cyber-attacks with potentially catastrophic consequences. For instance, an experimental cyber attack on a replica of a power plant's control system caused a generator to self-destruct [1].

In order to ensure electricity equipments to work properly, frequency of the electric power must be stable [2]. However, as the amount of actual load changes from time to time in practice,[1] it is hard to stabilize power frequency [3]. In spite of load dynamics, both electricity frequency $f(t)$ and its RoCoF (Rate of Change of Frequency) $\dot{f}(t) = \frac{df}{dt}$ should remain within their admissible intervals all the time according to the grid code for safe, secure, economic and proper functioning of the electricity system [5].

A good solution to power frequency stabilization takes the interests of both power providers and customers into consideration. To this end, load management technologies have been deployed to achieve load peak clipping, valley filling, peak shifting [6]–[9]. Although load management schemes are able to reduce equipment damage or prolonged imbalance that could lead to cascading failures and massive blackouts, the customers in disconnected regions may suffer significant loss of comfort or money, and even personal safety [10].

Different from load management which simply sheds or curtails power load, LFC (Load Frequency Control) shares the power regulation burden or capacity via the tie-lines in interconnected power systems to ensure the balance of load and frequency. As its heterogenous and dynamic power systems have to exchange information and power in real-time, a multi-area LFC is more complex than load management, such that unreliability and instability of one LFC area could quickly propagate to all the other interconnected areas.

To ensure reliability and stability of an entire LFC system, two major technologies have been proposed or even adopted in smart grids: (1) generator collaboration mechanism which deals with the measured tie-line frequencies in a multi-area LFC system with different technologies [11]–[13]; (2) Wide-area monitoring system which is supported by a network of devices deployed over a vast geographical area [14]–[17].

Manuscript received April 13, 2016; revised April 15, 2016, July 4, 2016, October 29, 2016, and December 23, 2016; accepted January 22, 2017. Date of publication January 30, 2017; date of current version August 21, 2018. This work was supported in part by the Energy Innovation Research Programme, Singapore, through Energy Market Authority under Award NRF2014EWT-EIRP002-040, in part by the Guangdong Innovative and Entrepreneurial Research Team Program under Grant 2014ZT05D238, and in part by the National Natural Science Foundation of China under Grant 61402199, Grant U1636209, and Grant 61373170. Paper no. TSG-00473-2016.

Y. Wu is with the System Security Department, Institute for Infocomm Research, Singapore (e-mail: wuyd007@qq.com).

Z. Wei is with the Shield Laboratory, Central Research Institute, Huawei International Pte Ltd., Singapore (e-mail: phdzwei@gmail.com).

J. Weng is with the Department of Computer Science, Jinan University, Guangdong 510630, China (e-mail: cryptjweng@gmail.com).

X. Li is with Sinocloud Wisdom Company Ltd., Beijing 100176, China (e-mail: li.xin@yunkouan.com).

R. H. Deng is with the School of Information Systems, Singapore Management University, Singapore (e-mail: robertdeng@smu.edu.sg).

[1]For instance, based on real loading data published by Electric Reliability Council of Texas (ERCOT) which schedules power on an electric grid that connects more than 43,000 miles of transmission lines and 550 generation units, the actual hourly load varies within the interval [35,993MWh, 45,056MWh] on 11 Jan. 2016 [4].

The above stabilization technologies work well when they are deployed in protected and/or benign environments. However, they may perform poorly or even fail to function in malicious situations when smart grids suffer from a variety of cyber attacks, such as TDS (Time-Delay Switch) attack [18], DOS (Denial-of-Service) attack [19], FDI (False Data Injection) at breaker [20], FDI at controller [21] and FDI at sensor [22]. In particular, false load attack attempts to cause circuit overflow at the most vulnerable areas of the electric grid, and hence is very effective and convenient [23]–[25] even if the adversary is restricted to simply tamper with the signals in a specified range of their allowed values. To protect LFC systems against this kind of attacks, the approaches in [26]–[28] integrate monitoring mechanisms and data analysis technologies to check the plausibility and consistency of data flows. In these countermeasures, a load disturbance model is used to check the soundness of load measurement such as [29]. Once the measurement deviates from the model beyond a predefined boundary, the controller of the LFC system raises a load-tampering alarm.

Based on the resonance principle, this paper introduces a new type of attacks which is able to defeat the plausibility and consistency based attack detection techniques mentioned above. Specifically, in a resonance attack, an attacker alters power load according to a resonance source RoCoF such that the modified load is kept within an admissible interval. Although the load changes are too small to be identified by detection methods, they could lead to abnormal frequency and/or RoCoF in the power system. Alternatively, the internal states of a power plant, power frequency and their delayed values can be used as resonance sources too. For a multi-area interconnected LFC system, the resonance attack can also be launched by altering tie-line signal besides load. To demonstrate effectiveness of the resonance attacks, we conduct digital simulations on single-area and multi-area LFC system models which consist of linear/non-linear items, one-order/high-order items, AVR (Automatic Voltage Regulator) and PSS (Power System Stabilizer). The simulation results show that the damage of attacks on LFC in one area can propagate to other interconnected areas. Finally, we address countermeasures to the attacks by invalidating the resonance.

The reminder of this paper is organized as follows. Section II presents the novel resonance attack and applies it on the simple linear model of LFC power systems, including single-area LFC and multiple-area LFC. Section III addresses the alternative resonance attacks and Section IV examines the attacks on complex models of LFC power systems. Section VI discusses the attack feasibility, countermeasures and comparison with the existing attacks. Section VI draws conclusions and remarks on future research topics.

II. Resonance Attack on LFC

In any modern power system, a large frequency deviation can damage equipments, degrade load performance, cause overload of transmission lines, and ultimately lead to an unstable condition for the power system. For example, violation of frequency control requirements was known as a main reason for Italy power grid blackouts.[2] Thus frequency (f) and RoCoF ($\dot{f}$) are two important electricity power parameters, and must remain stable all the time. As the divergency of RoCoF often results in the divergency of frequency, and there are many works on the stability of frequency, the following sections will focus on RoCoF only unless otherwise stated.

Typical RoCoF protection relay in a power system has a boundary $[B_0, B_1] = [0.1, 1.0]$ Hz/s, depending on the inertia of the power system [30], *e.g.*, the required RoCoF boundary is 0.5 Hz/s in Ireland [31]. As a consequence, if an adversary is able to attack a power system such that its RoCoF is beyond the predefined boundary, the RoCoF relays may trip to protect the electricity equipments. If there are many relay trips, the power system may go blackout. This section will propose a novel resonance attack on LFC system to cause RoCoF relay trips by craftily manipulating the load of the power system.

A. LFC Model

As a major function of AGC (Automatic Generation Control), LFC is able to balance load and frequency, and is one of the important control mechanisms in power system design and operation. Generally, a power system may consist of several LFC areas. We provide a brief description of the LFC model below. For more details, please refer to [32].

Fig. 1 shows the dynamic model of the ith LFC area in a multi-area LFC system. The model consists of a plant $G(s)$ and an outer controller, where the plant $G(s)$ further consists of three modules and an inner speed regulator. The three modules are governor, turbine and generator respectively. Denote $\hat{P}_{v_i}$, $\hat{P}_{t_i}$, and $\hat{f}_i$ as the deviation of the governor output, the deviation of the turbine output, and the deviation of system output frequency, respectively. The regulator is used to adapt to local load deviations. When the system frequency deviates from the nominal frequency f_0, either over frequency or under frequency, the frequency deviation is fed back as an ACE (Area Control Error) signal which is used to generate the outer control signal based on a control algorithm. Currently, PI (Proportional Integral) controller is commonly used as an outer controller in LFC system [33]. It aims to drive frequency f_i to nominal frequency f_0 in tens of seconds whenever a step-load perturbation $\hat{L}_i$ is applied to the power system [2].

In a multi-area power system, the generation units are connected over inter-area transmission lines so as to automatically balance the dynamic load among power areas. To this end, the frequency signals from all the connected LFC areas are exchanged via tie-lines among LFC areas and used in the outer controller. Denote $\hat{P}_{tie_i}$ as the deviation of tie-line signal in the ith area. With reference to Fig. 1, it is easy to show that

$$\hat{P}_{tie_i}(s) = \left(T_{ii}\hat{f}_i(s) - \sum_{j=1, j\neq i}^{J} T_{ij}\hat{f}_j(s) \right) \times \frac{2\pi}{s} \qquad (1)$$

where $\hat{f}_i = f_i - f_0$, $T_{ij} = T_{ji}$ is the connectivity strength between area i and area j, and $T_{ii} = \sum_{j=1, j\neq i}^{J} T_{ji}$, $i, j = 1, 2, \ldots, J$ for a power system having J LFC areas. In the ideal situation, the LFC power system is perfectly managed, *i.e.,* deviation of

[2] http://www.rae.gr/old/cases/C13/italy/UCTE_rept.pdf

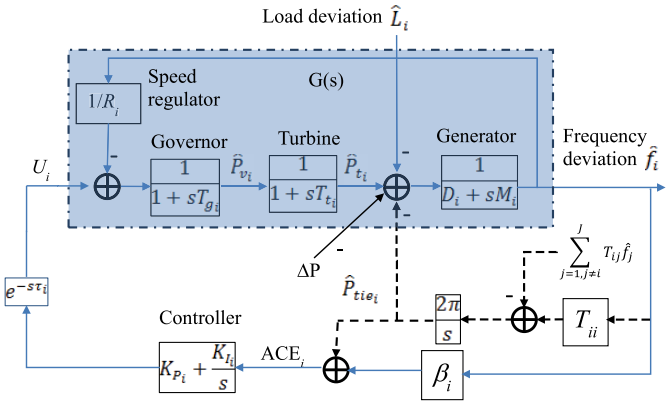


Fig. 1. The ith control area in a multi-area LFC system including non-reheat steam unit, where $G(s)$ (within the dotted-dash box) is the close-loop transfer function of the plant and dotted lines represent the inter-area connection, $\hat{P}_{v_i}$ and $\hat{P}_{t_i}$ are the change of valve position for controlling mechanical force and the change of the generator mechanical output respectively, and ΔP is the output from AVR (see Section IV-B). Adapted from [32].

tie-line signal $\hat{P}_{tie_i} = 0$ and frequency deviation $\hat{f}_i = 0$. In practice, the controllers aim to minimize $\hat{f}_i$ and $\hat{P}_{tie_i}$ for all the LFC areas in case of load fluctuation.

B. Security Model

Fig. 2 is a simplified power system architecture marked with several possible attack points. Because electric power can not be stored on a large scale, a power generation system attempts to produce electricity according to customers' load demand L_i in real-time. Therefore, after receiving the customers' power load request via a network, the control center instructs the power plant to generate the demanded power by adjusting the amount of external energy such as the rate of burning oil in the power generator (*e.g.*, Siemens Air-Cooled Generators SGen-100A-4P Series). However, in a malicious situation, the customers' equipment, the control center and their communication channels are vulnerable to data modification or injection attacks. In addition, for a power system consisting of generators distributed over several areas, input signals such as frequency signal f_j transmitted among the power generation areas may be tampered with by the attacker too.

By maliciously manipulating the input signals[3] such as aggregated load L_i or individual customer load L_{ik}, an attacker aims to drive the power grid to undesirable or dangerous states. To this end, the attacker is assumed to be able to

(1) Observe the parameters of power system output (*e.g.*, electricity frequency);
(2) Stealthily modify the input without being detected.

The first assumption means the attacker knows the system output all the time. In practice, it is not hard to measure system output because electricity produced by any power generator is usually delivered to customers over open areas. For example, the electricity voltage and frequency can be easily measured by anyone. The second assumption assumes that the attacker is

[3]For ease of exposition, we assume that the attacker manipulates the digital signal of the load. In Section V-B, we will elaborate how the attacker can tamper with the actual load for the same purpose.

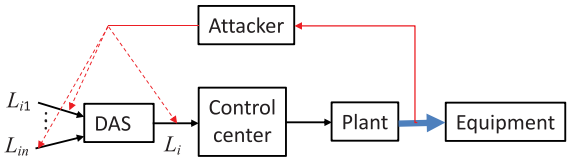


Fig. 2. A simplified power system architecture, where DAS (Demand Aggregation System) in a control center is used to aggregate customers' input. Thick blue line indicates power flow, solid black line indicates information flow, and dash line indicates that the attacker tampers with the load signals.

able to modify or inject input data within a range. For example, using the power load altering methods in [34], the faked input $|x(t)| < x_{max}$ for any time t, where x_{max} is some predefined constant. As the modification is too small to be detected, the attack is stealth. Considering the load dynamic range [4] and mandatory redundancy, we choose $x_{max} = 0.3$ pu (per unit) which will be enforced by the plant.

C. Attack Method

In a nutshell, to launch a resonance attack on a target power grid, an attacker slightly modifies or fakes input so that the input resonates with a resonance source, usually the system output or a function of the system output. Specifically, the attack process proceeds as follows.

(1) The attacker samples the output of the target power grid such as power frequency, then modifies/fakes an input based on a chosen resonance source;
(2) The attacker sends the bogus input to the power generator system;
(3) The generator system checks on the plausibility of the input. If the input is within the plausibility range, the input will be accepted by the power system for regulating the target power generator;
(4) The generator produces electricity power which is transmitted over the power grid;
(5) As the protection relay periodically measures the electricity power, it will trip automatically as long as the measured RoCoF is beyond the admissible boundary. Simultaneously, the attacker also samples the electricity power, and decides whether the attack is successful or not. If not, he repeats the above process.

In the attack process, RoCoF protection relay is not directly controlled by the attacker. The next subsections will elaborate how the attacker indirectly controls the RoCoF protection relay in single-area LFC and multi-area LFC.

D. Attack on Single-Area LFC

Suppose the adversary samples the electricity frequency at a rate 1,000 Hz,[4] and selects $x_i = \hat{L}_i$ as the attacking input which is no more than $x_{max} = 0.3$ pu. Furthermore assume the system delay is $\tau_1 = 0.25$s according to the system stability interval [0, 0.348] specified in [33]. The attacker uses RoCoF

[4]GOOSE (Generic Object Oriented Substation Event) enables IEC 61850 based devices to quickly exchange critical data (*e.g.*, a trip signal to a circuit breaker) less than 4 milliseconds, over the Ethernet based communication [35]. Due to Nyquist-Shannon sampling theorem, we choose 1,000Hz sampling frequency.

TABLE I
SYSTEM PARAMETERS IN THE iTH LFC AREA [33]

Parameter $\mathcal{V}$	Value
Time constant of the turbine T_{t_i}	0.3 s
Time constant of the governor T_{g_i}	0.1s
Speed drooping R_i	0.05 Hz/pu
Damping coefficient of the generator D_i	1.0 pu/Hz
Moment of inertia of the generator M_i	10 pu s
Area feedback β_i	21 pu/Hz
Proportional K_{p_i}	-1.0 s
Integral K_{I_i}	-1.0 s

$y_i = \dot{\hat{f}}_i = \frac{d\hat{f}_i}{dt}$ to measure whether the attack is successful or not. That is, if RoCoF is beyond the boundary, the attacked LFC power system will be disconnected from the power grid. Furthermore, we adopt the LFC system parameters shown in Table I.

This subsection investigates the stability of the single-area LFC of area 1, where $\hat{P}_{tie_1} = 0$. According to the attack method presented in Section II-C, an attacker attempts to fake the load input $x_1(t)$ such that RoCoF becomes unstable. To demonstrate the attack effect, with regard to Fig. 1, the power generation system with the parameters in Table I is modeled as

$$\begin{cases} ACE_1 = 21\hat{F}_1 \\ U_1 = \left(-1.0 + \frac{-1.0}{s}\right)e^{-\tau_1 s}ACE_1 \\ \hat{P}_{v_1} = \left(U_1 - \frac{\hat{F}_1}{0.05}\right)\frac{1}{1+0.1s} \\ \hat{P}_{t_1} = \frac{1}{1+0.3s}\hat{P}_{v_1} \\ \hat{F}_1 = \left(\hat{P}_{t_1}e^{-\lambda_1 s} - X_1\right)\frac{1}{1+10s} \\ Y_1 = s\hat{F}_1 \end{cases} \tag{2}$$

assume AVR output $\Delta P = 0$, where λ_1 is the delay of governor-turbine module such as DEGOV/DEGOV1 [37], the upper-case variable is the Laplace transform of the lower-case (time-domain) variable, *e.g.*, $Y_1(s)$ is the Laplace transform of $y_1(t)$. For simplicity, we omit the variable s in the Laplace formulas, *i.e.,* $Y_1(s)$ is written as Y_1. Assume $\lambda_1 = 0$, the transfer function of the single-area LFC can be written as

$$\begin{aligned} \frac{Y_1}{X_1} &= \frac{-s^2(1+0.1s)(1+0.3s)}{s(1+0.1s)(1+0.3s)(1+10s)+21(s+1)e^{-\tau_1 s}} \\ &= -\frac{0.03s^4+0.4s^3+s^2}{0.3s^4+4.03s^3+10.4s^2+21(s+1)e^{-\tau_1 s}} \end{aligned} \tag{3}$$

Clearly, as shown in Fig. 3.a, the step response of system Eq. (3) is stable if there is no attack. However, when the system is attacked with input $x_1(t) = -0.3 \times sign(y_1(t-0.25))$pu, where function $sign(a) = \begin{cases} 1 & a > 0 \\ -1 & a \le 0 \end{cases}$, its RoCoF goes beyond the boundary quickly. As a result, the attacked LFC power plant will be disconnected from the whole power system, which can cause shortage of power supply and overload of other LFC areas. More seriously, power blackout may happen as more and more LFC power plants are disconnected from the grid.

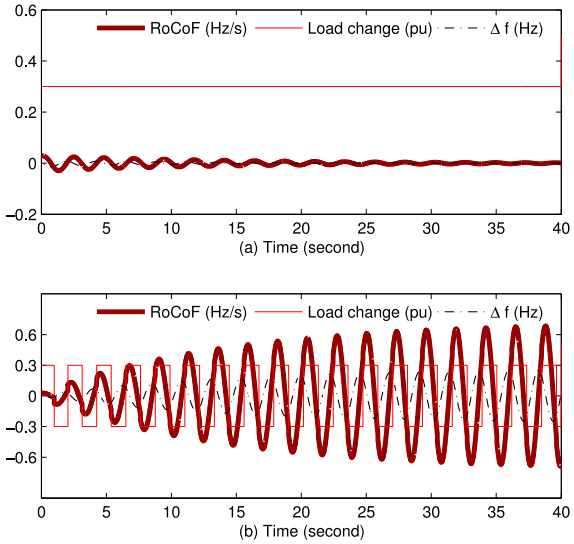


Fig. 3. Response of a single-area LFC. (a) No attack, (b) Resonance attack on a single-area LFC. The RoCoF (thick line) goes beyond 0.6 Hz/s and the frequency derivation (dashed line) does not converge when the plant is attacked with the faked input $x_1(t)$. $\Delta f = \hat{f} = f - f_0$ is the derivation of power frequency f from the nominal frequency f_0.

E. Attack on Multi-Area LFC

In a multi-area LFC, each generator needs to handle local load deviation as well as tie-line deviations from other areas in order to regulate its local and global load balances. However, this interconnection due to tie-line input can be exploited by attackers. As we show below, an attacker may need to attack only one LFC area in order to cause the blackout of the whole power grid. For simplicity, we assume that all the LFC areas have the same set of parameters given in Table I, and the correlation matrix is

$$\mathbf{T} = \{T_{ij}\}, T_{ij} = \begin{cases} 0.2 \text{ pu/Hz} & i \neq j \\ \sum_{k=1,k\neq i}^{J} T_{ik} & i = j \end{cases}$$

As a concrete example, let's consider a two-area LFC system, whose step response RoCoF and tie-line signal $\hat{P}_{tie_1}$ of area 1 are shown in Fig. 4. Obviously, the step response is convergent and hence the non-attacked LFC plant system is stable. However, if the attacker changes the load of area 1 to $x_1(t) = -0.3 \times sign(y_1(t-0.25))$ and its inter-connected frequency deviation $\hat{f}_2$ to $0.3 \times sign(y_1(t))$, the frequency and RoCoF of area 1 will become divergent as shown in Fig. 5.a and Fig. 5.b respectively, and the tie-line signal P_{tie_1} is shown in Fig. 5.c. Comparing with the result shown in Fig. 3.b, we know that the tie-line signal can be exploited to cause higher RoCoF of area 1 in a two-area LFC system. More seriously, when area 1 is attacked, the non-attacked area 2 becomes instable too, as shown in Fig. 5.d.

Fig. 6 shows the performance of attack on a four-area LFC system when both the load input and all the inter-connected signals $\hat{f}_j$ $(j = 2, 3, 4)$ of the first LFC area are tampered with. By comparing the attack effects shown in Fig. 3.b, Fig. 5.b and Fig. 6, we conclude that resonance attacks are more powerful as the number of LFC areas increases. Thus, although inter-connected infrastructure improves system performance in general, it increases the attack surface and makes the overall system more vulnerable.

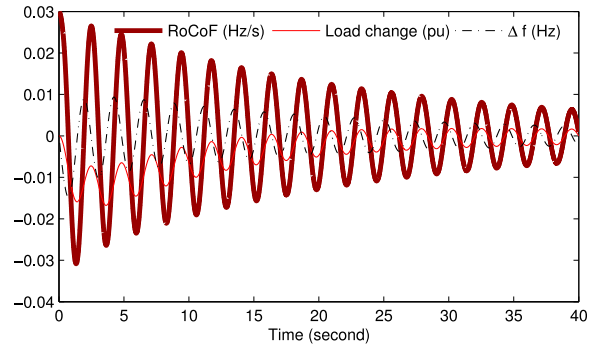


Fig. 4. Step response in a two-area LFC. The interconnected area is still stable when there is a tie-line between two LFC areas.

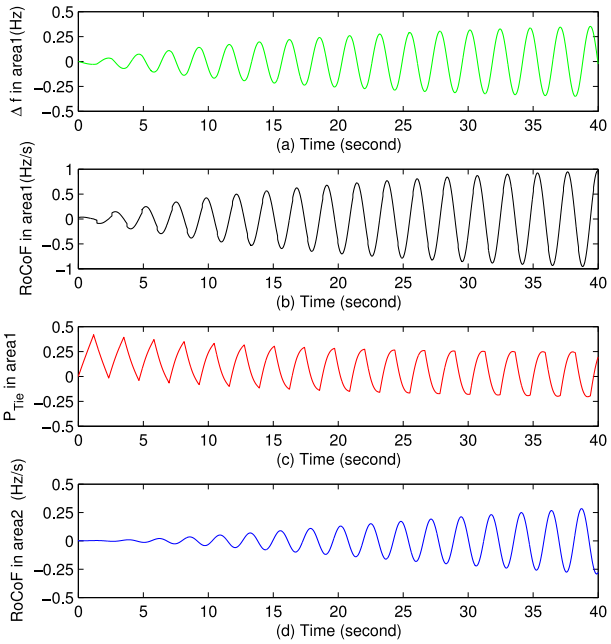


Fig. 5. Resonance attack to a two-area LFC. In an interconnected LFC power system, if area 1 is attacked directly, area 2 will be attacked indirectly.

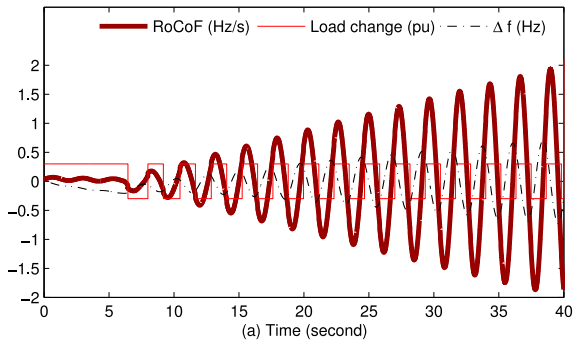


Fig. 6. Resonance attack on a four-area LFC. When both the load x_1 and all the inter-connected signals $\hat{f}_j$ $(j = 2, 3, 4)$ are tampered with, the amplitude of RoCoF (thick line) increases significantly.

III. Alternative Attacks

Section II introduces the idea of resonance attacks on LFC power generation system. In the attack, an attacker can easily fake an attack input $x_i(t) = -0.3 \times sign(y_i(t-\gamma))$ for some delay time γ after measuring the resonance source RoCoF.

TABLE II
Results of Various Resonance Sources

Resonance source	Period	Launch	Attack effect
Internal state derivation	Middle	Difficult	Best
Frequency derivation	Long	Easy	Good
RoCoF	Short	Easy	Good

In this section, we will extend the resonance attacks to other resonance sources and the stealth attack which aims to avoid detection.

A. Alternative Resonance Sources

The resonance attack aims to fake a load input as a feedback of the LFC generator so as to drive RoCoF out of the admissible boundary. Besides RoCoF, an attacker can employ generator internal states and frequency derivation as resonance sources to fake input.

1) Internal State as a Resonance Source: Given that the plant internal state is known to the attack, a more powerful attacker is able to modify the load according to the (estimated) internal states. Fig. 7.a and Fig. 7.b show the attack results given that the loads are faked based on the governor output $P_{v_1}(t)$ and the turbine output $P_{t_1}(t)$ respectively.

2) Frequency Derivation as a Resonance Source: It is easy for an attacker to measure the frequency derivation, and use it as a resonance reference, *i.e.,* the adversary is able to fake an attack input $x_i(t) = -0.3 \times sign(\hat{f}_i(t))$. As shown in Fig. 7.c, this bogus input also degrades the quality of RoCoF quickly.

Table II summarizes the performance of attacks using different resonance sources. The second column indicates that the RoCoF-based attack takes less time than others, i.e., shortest period in Fig. 7. In the third column, the attack using internal state is difficult to start as it needs to know the internal state of the plant. But it merely performs slightly better than the other attacks, as indicated in the last column. Therefore, attack using RoCoF or frequency derivation as resonance source is adopted in this paper because it has good attack performance and is easy to launch.

As resonance attack takes effect as long as the bogus input correlates with the target output, we expect that the input delay will also have impact on the attack performance. In fact, Fig. 7.d $\sim$ 7.f and Fig. 3.b demonstrate that delayed source can also be used for attacks, and different delay $\gamma \in [0, 0.5s]$ incurs only a little difference in terms of attack performance.

B. Stealthy Resonance Attack

In the above attack experiments, the load change is not continuous, and hence may alert plausibility-based detectors. To invade this kind of detectors, an attacker may modify the load value smoothly, *e.g.*, by filtering the bogus inputs $x_i(t)$ into a continuous signal $\tilde{x}_i(t) = \alpha \times (-0.3 \times sign(y_i(t))) + (1-\alpha)\bar{x}_i(t)$, the resonance attack effect represented by RoCoF maximum is shown in Fig. 8, where $\bar{x}_i$ is the mean of function $x_i(t')$ for $t < t'$, $\alpha \in [0, 1]$.

According to Fig. 8, the attacker can choose $\alpha = 0.005$ to have the best attack effect (maximal RoCoF). As shown in

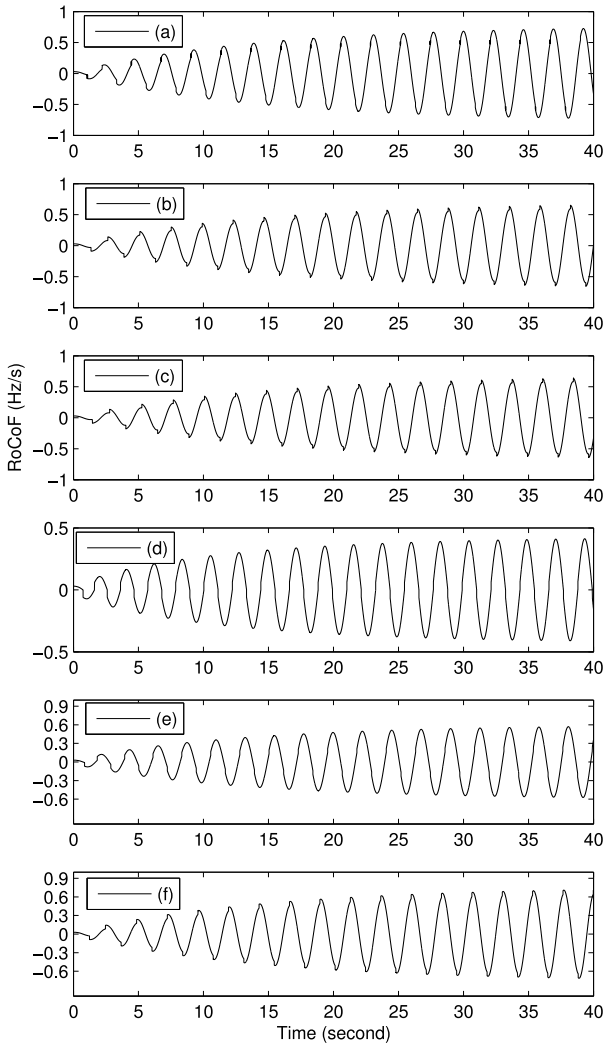


Fig. 7. Resonance attacks on single-area LFC model using different resonance sources. (a) $x_i(t) = 0.3 \times sign(\hat{P}_{v_i}(t))$; (b) $x_i(t) = 0.3 \times sign(\hat{P}_{l_i}(t))$; (c) $x_i(t) = -0.3 \times sign(\hat{f}_i(t))$; (d) $x_i(t) = -0.3 \times sign(y_i(t))$; (e) $x_i(t) = -0.3 \times sign(y_i(t - 0.125))$; (f) $x_i(t) = -0.3 \times sign(y_i(t - 0.5))$.

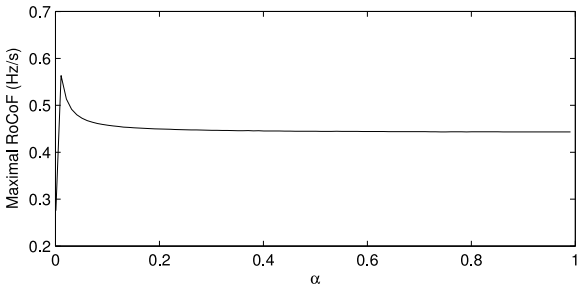


Fig. 8. Stealthy resonance attack effect on a single-area LFC.

Fig. 9, after the faked load in Fig. 3.b is filtered to be smooth and then sent to the plant, the resonance attack is still viable.

IV. Attacks on Plant Variants

Presently, there are roughly 7,000 and 3,000 synchronous generator models in the typical planning cases of Eastern Interconnection and WECC (Western Electricity Coordinating

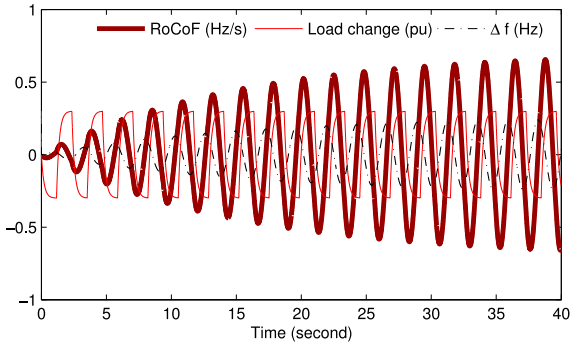


Fig. 9. Stealth resonance attack effect on a single-area LFC, $\alpha = 0.005$. The load change is filtered such that the attack is stealthy.

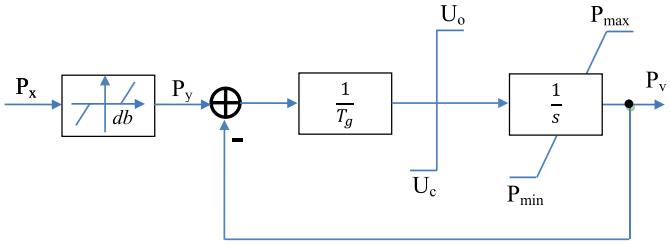


Fig. 10. The governor model with non-linear items, where $P_x = U_i - \frac{\hat{f}_i}{R_i}$ with reference to Fig. 1.

Council) respectively [36]. Apparently, it is difficult and not very useful to present the attacks to all the models here. Instead, it may be sufficient to investigate the stability of the governor-turbine models including basic physical constraints when they are attacked with the method in Section II.

A. Variant of Governor-Turbine

In a practical conventional electricity plant, the governor has some restriction items including dead band, rate limiter and power limiter as shown in Fig. 10, where *db* is the dead band, Uo is the maximum of valve opening rate, Uc is the maximum of valve closing rate, Pmax is the maximum of valve position and Pmin is the minimum of valve position. In addition, it may be more accurate to describe turbine with high-order models.

1) Dead Band: The dead band of a governor is defined as the total magnitude *db* of a sustained speed change, within which there is no resulting change in valve position [32]. Mathematically, a dead band function is

$$P_y = \begin{cases} P_x - db & P_x > db \\ P_x + db & P_x < -db \\ 0 & \text{otherwise} \end{cases} \quad (4)$$

Usually, a dead band may change the frequency control performance, and hence may impact the attack performance too. To simulate the attack performance, we choose a sufficiently large dead band $db = 0.1$ pu. If there is no attack, the power plant is stable as shown in Fig. 11.a. However, when the proposed attack is applied to the plant, the system output is changed into Fig. 11.b. Clearly, the attack is still effective even if the governor-turbine has dead band.

2) Rate Limiter: If the electricity power is generated from the conventional energy source, e.g., thermal energy or

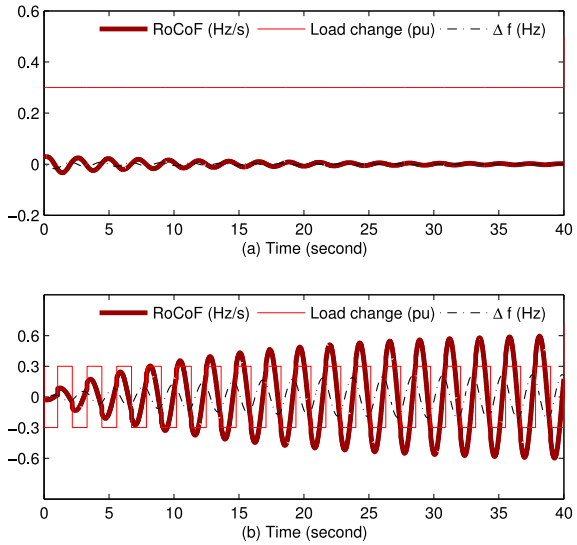


Fig. 11. Response of a single-area LFC plant where dead band $db = 0.1$ pu. (a) No attack; (b) Resonance attack.

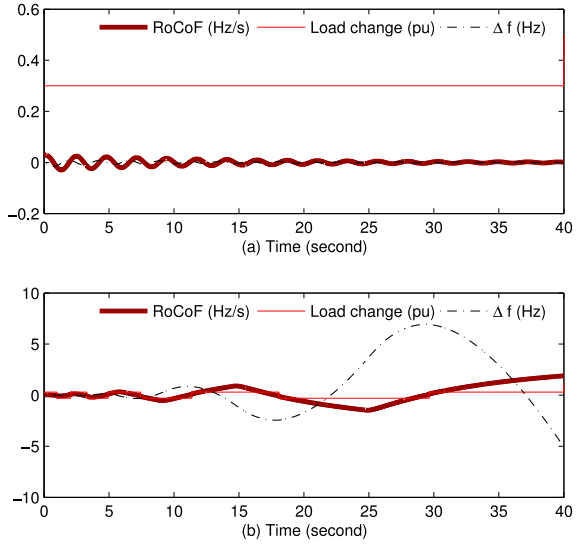


Fig. 12. Response of a single-area LFC plant whose governor has a rate limiter. (a) No attack; (b) Resonance attack.

mechanical energy, the change rate of power generation is slow. Thus, the governor is not required to change the valve quickly. In many governor-turbine models such as TGOV5 and IEEEG1, rate limiter is a mandatory item in order to improve the accuracy of long-term dynamic studies [36].

As shown in Fig. 12.a, it is stable for a power plant whose rate limiter is $2R_L$, where $R_L = 1.43$ is the maximal valve rate of the step response shown in Fig. 3.a. However, when the proposed attack is applied to the plant whose governor has the valve rate limiter, the system output is instable as shown in Fig. 12.b. In comparison with Fig. 3.b, Fig. 12.b shows much higher RoCoF and/or frequency deviation, and larger vibration period. Further experiments show that the output of the attacked plant is divergent if its rate limiter is within an interval $(0, 15R_L)$.

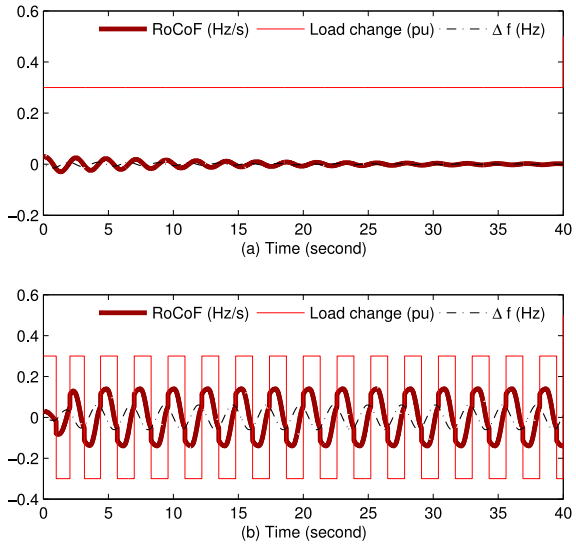


Fig. 13. Response of a plant whose governor has a power limiter 1.2pu. (a) No attack; (b) Resonance attack on single-area LFC power system.

According to the experiments on governor with/without rate limiter, we have two findings: (1) rate limiter dramatically decreases the attack resilience capability of the plant; (2) if the governor-turbine has a rate limiter, the attack has impact on long-period (e.g., tens of seconds) LFC, otherwise, it has impact on short-period (e.g., several seconds) primary frequency control as shown in Fig. 3.b.

3) Power Limiter: Due to restriction of energy source, a power generator usually has a limited capacity to produce power. That is to say, power limiter determines the capacity and scalability of the power generator, and is related to the valve position controlled by the governor.

Assume governor's power limiter is 1.2pu (Turbine-GAST model in [37]), Fig. 13.a shows that the step response of the power plant with power limiter become zero quickly when there is no attack. However, when the resonance attack is applied on the plant, the system output fluctuates as Fig. 13.b. In comparison with Fig. 3.b, Fig. 13.b has lower RoCoF and frequency deviation. Thus, power limiter can alleviate the risk of the present attack. Nonetheless, the RoCoF of the attacked plant is still beyond the lower boundary $B_0 = 0.1Hz/s$ and hence the attack may incur potential risk on some power grids.

More importantly, the present attack may have significant impact on a special kind of LFC plants. This kind of plants includes several governor-turbine units in one area [32] and each governor has a power limiter. It is stable when there is no attack as shown in Fig. 14.a, but becomes instable as shown in Fig. 14.b due to the present attack because the actual power restriction on each generation unit is reduced.

4) High-Order Turbine Model: In reality, a real turbine is much more complicated than a one-order model in Fig. 1. In order to assess the accuracy of the attack, we perform simulations on a high-order turbine model shown in Fig. 15 [36]. According to typical parameters for steam turbine models in [38], the high-order turbine model has a time constant tuple $\{T_{VH}, T_H, T_I, T_L\} = \{0.3, 8, 8, 0.4\}$ in seconds. If we perform the attack simulation on the plant with a high-order

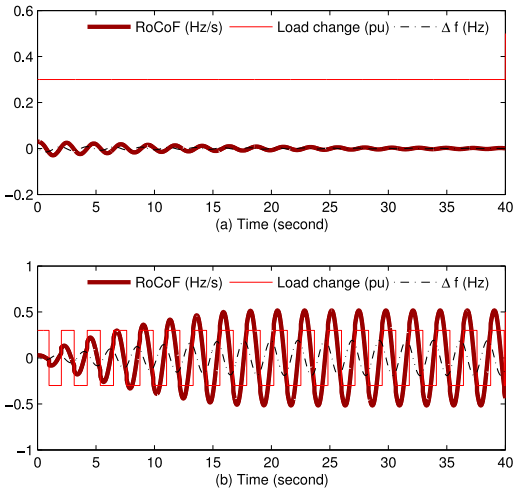


Fig. 14. Response of a plant consisting of five identical generation units. Each unit has power limiter 1.2pu and participation factor 0.2. (a) No attack; (b) Resonance attack.

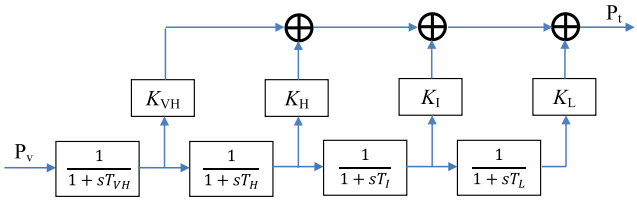


Fig. 15. A high-order turbine model in the standard IEEEG1 model, where $K_{\mathrm{VH}} + K_{\mathrm{H}} + K_{\mathrm{I}} + K_{\mathrm{L}} = 1$.

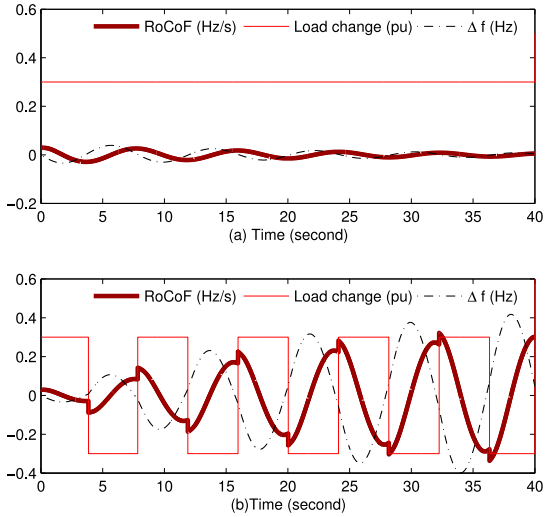


Fig. 16. Response of single-area LFC plant with high-order turbine model, the gain tuple $\{K_{\mathrm{VH}}, K_{\mathrm{H}}, K_{\mathrm{I}}, K_{\mathrm{L}}\} = \{0.15, 0.50, 0.20, 0.15\}$. (a) No attack; (b) Resonance attack.

turbine model, the attack is weakened. However, if there is a delay factor in the governor-turbine model, the attack will still be effective, e.g., if the delay $\lambda_1 = 0.1$s, Fig. 16.a shows that RoCoF converges quickly when there is no attack, but Fig. 16.b shows that RoCoF is beyond the boundary when the plant is attacked.

5) Integrated Governor-Turbine Model: As shown in Sections IV-A and IV-A4, dead band has minor impact on the attack effect, rate limiter enhances the effect, while power limiter and high-order turbine model weaken the effect. As each of them exists in a real governor-turbine system, we perform the present attack on the integrated governor-turbine system which includes all of them. The non-attack system runs well as shown in Fig. 17.a, but becomes instable if it is attacked as shown in Fig. 17.b. In particular, the frequency change of the integrated governor-turbine model exceeds 1 Hz in 2 minutes when the faked load fluctuates within [-0.3, 0.3] pu only.

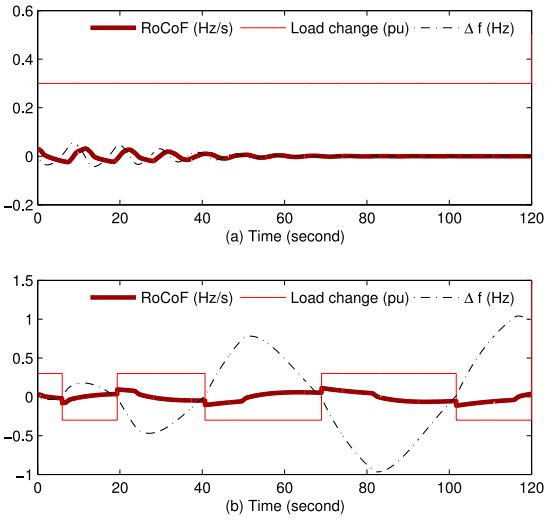


Fig. 17. Response of single-area LFC with integrated governor-turbine model (single generation unit, and $\lambda_1 = 0$). (a) No attack; (b) Resonance attack.

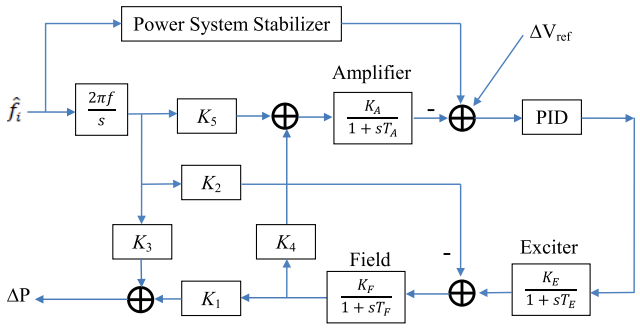


Fig. 18. Block diagram of AVR, where $\Delta \mathrm{V}_{\mathrm{Ref}} = 0.091$ is the reference terminal voltage deviation [39], [40].

B. Combined Model of LFC and AVR

With reference to [39] and [40], AVR (Automatic Voltage Regulator) loop is used to regulate the voltage and the reactive power in the power plant. As shown in Fig. 18, it consists of PSS (Power System Stabilizer), amplifier, AVR controller, and exciter, where PSS has a transfer function

$$\phi_{PSS} = K_{PSS} \times \frac{sT_w}{1+sT_w} \times \frac{1+sT_1}{1+sT_2} \tag{5}$$

for some constant K_{PSS}. When the proposed attack is applied to a power plant enhanced with AVR, the attack effect is shown in Fig. 19. Clearly, AVR does not increase the defense capability of a power plant.

TABLE III
AVR PARAMETERS

Parameter values for PSS [40]					
K_{PSS}	T_w	T_1	T_2		
1.853	0.1632	0.3457	1.0304		
Parameter values for AVR loop [40]					
K_F	K_A	K_E	T_E	T_A	T_F
0.3794	1	20	0.05	0.05	2.9441
Gain values for AVR loop [40]					
K_1	K_2	K_3	K_4	K_5	
1.853	0.1632	0.3457	1.0304	0.0674	
PID for AVR loop [41]					
k_P	k_I	k_D			
0.6871	7.9162	0.0688			

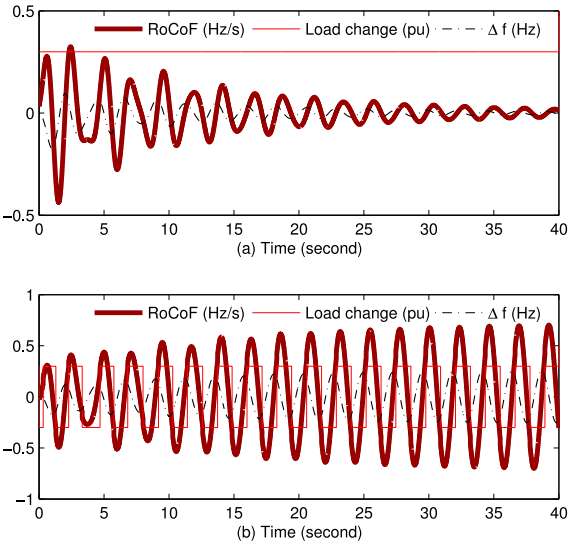


Fig. 19. Response of a single-area LFC plant which has an AVR item, where the AVR parameters are listed in Table III. (a) No attack; (b) Resonance attack.

C. PID Output Saturation

PID controller saturation is used to stabilize a plant by restricting the control signal within an interval. Its disadvantage is that it decreases the system response speed. When the proposed attack is applied to a power plant whose control signal is limited to 1.2pu, Fig. 20.b shows that the attack effect is weakened but still effective. Especially, in an LFC power system which consists of multiple governor-turbine generation units, the PID output limiter shall be increased to adapt to wide load dynamics. Suppose the PID output limiter is increased according to the number of generation units in one area, but only a portion of generation units is in operation, the PID saturation may not reduce the attack performance as shown in Fig. 20.c.

V. DISCUSSION

In this section, we will discuss random attack, parameter sensitivity, and countermeasures to resonance attacks addressed in Section II. For simplicity, this section focuses on single-area LFC systems. For multi-area LFC systems, similar conclusions can be drawn.

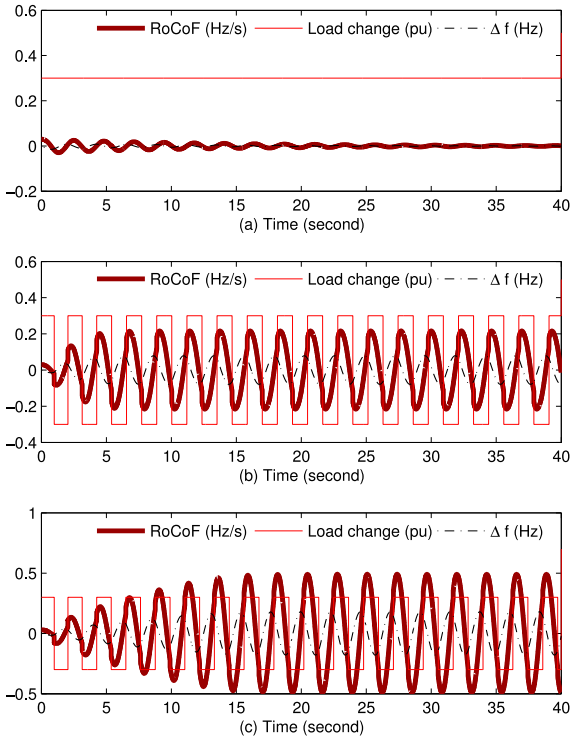


Fig. 20. Response of single-area LFC plant with PID output saturation. (a) No attack; (b) Resonance attack on a generator (single generation unit), (c) Resonance attack on a plant which has three generation units, but only one in operation.

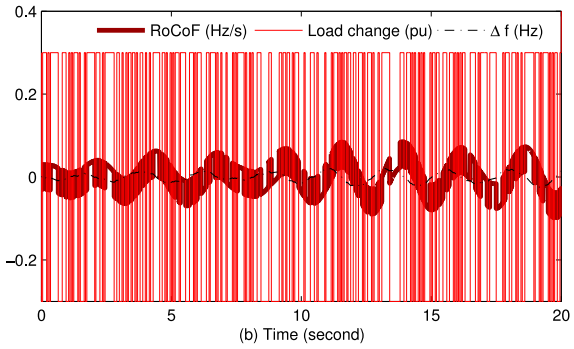


Fig. 21. Random manipulation effect on a single-area LFC system when the load is randomly changed per 50ms.

A. Random Attack

When the input x_1 is changed over set {-0.3pu, 0.3pu} randomly, RoCoF fluctuation shown in Fig. 21 is much smaller than that in Fig. 3.b. Hence the resonance attack clearly performs much better than random load manipulation.

B. Attack Feasibility

In the present attacks, the adversary has to tamper with the actual load directly or indirectly. If the load management process is performed over data networks, the adversary can tamper with the traffic such that the load management system increases or decreases the actual load. Otherwise, he will modify the actual load by compromising the devices such as smart

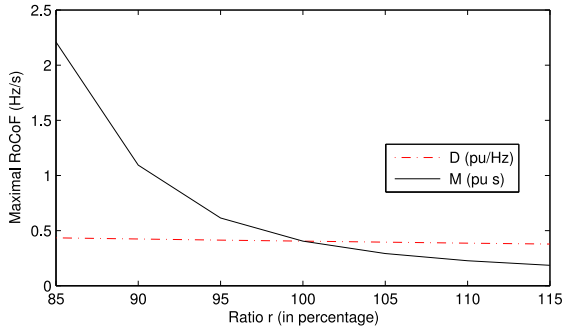


Fig. 22. Attack effect on a single-area LFC regarding generator parameters, where y-axis is the maximal RoCoF over 40s simulation period for each r.

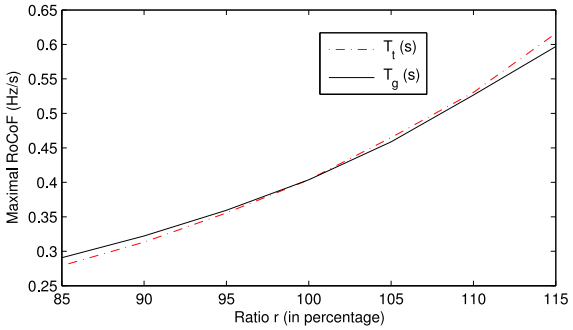


Fig. 23. Attack effect on a single-area LFC regarding governor-turbine time constants.

meters. Concretely, according to the characteristics of the target power system, the attacker can realize the different attack strategies as follows.

1) Indirect Modification: In some power systems, ELC (Electronic Load Controller) [42] is used to match load demand with the generators' output. Hence, if an adversary is able to fake the load input of ELC or its customers, he can achieve actual instantaneous load control as ELC will adjust (i.e., switch on/off) the actual load based on the faked input. In other words, if the attacker can indirectly manipulate a portion of actual load via ELC, he is able to start the resonance attack to threat the entire power grid.

2) Direct Modification: With the advance of smart grids, electrical devices with grid friendly controller are recommended by U.S. Department of Energy to support power grid reliability [43], [44] and realize dynamic demand control [45], [46]. Thus, an adversary is able to achieve actual instantaneous load control if he can compromise a portion of gridwise friendly devices with malicious codes and then directly manipulate the device loads (i.e., switch on/off the devices).

C. Sensitivity Analysis

In order to study the robustness of the proposed attack using RoCoF as resonance source, we assume that the system parameter is changed at ratio $r = \frac{\mathcal{V}}{\mathcal{V}_i} \in [85\%, 115\%]$, where $\mathcal{V}_i$ is the value for parameter $\mathcal{V}$ in Table I.

As shown in Fig. 22, different moment of inertia M results in different resilience effect on the attack, i.e., if the power system has higher moment of inertia M, it will be more stable (i.e., lower RoCoF maximum). However, the damping coefficients D does not have obvious effect on attack resilience.

Fig. 23 shows the attack resilience of the governor time constant T_g. Clearly, when the governor time constant is increased, the attack effect is more significant. Similarly, attack performance increases with turbine time constant T_t too.

As shown in Fig. 24, when the PI controller coefficient Kp or K_I is changed at any ratio $r > 85\%$, the output of the attacked system is beyond the admissible boundary, and high PI coefficients may enhance the attack effect. Therefore, it should be cautious to choose PI coefficients for stabilizing the generator in a malicious situation.

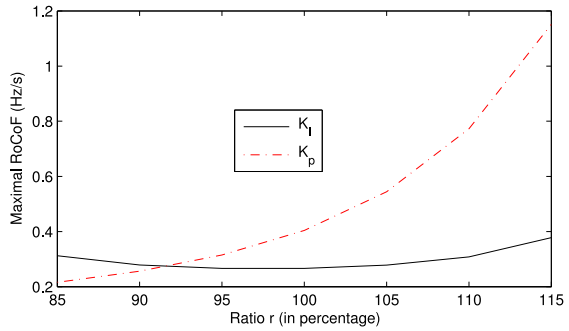


Fig. 24. Attack effect on a single-area LFC system regarding PI controller coefficients.

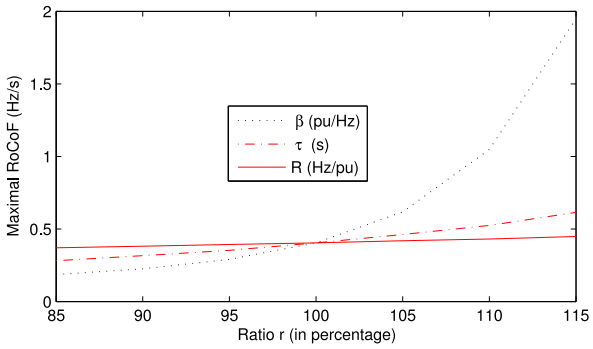


Fig. 25. Attack effect on a single-area LFC system regarding system parameters.

With reference to Fig. 25, the larger the parameters including area feedback gain β, speed drooping parameter R and controller loop delay τ, the higher attack performance. Especially, the system feedback gain β has the most significant impact on attack resilience.

D. Countermeasure

Two prerequisites of resonance attacks are that the attacker is able to access a resonance source such as the system output and is able to modify or inject input data which resonates with the resonance source. The output of most power generation systems such as electric frequency is publicly available, hence protecting the input data is the only viable countermeasure to resonance attacks. The problem of protecting data integrity to prevent both data modification and data injection is well

studied in the network security community and many effective solutions have been proposed in the literature. Most of the solutions employ cryptographic techniques together with timestamps/sequence numbers to ensure data authenticity and freshness [47]. In fact, there are security standards such as IEC 62351 for protecting smart grids by specifying cipher suites (authentication, integrity protection and encryption algorithms) for end-to-end security [48]. For instance, IEC 62351-6 specifies VLAN (Virtual Local Area Network) to be mandatory for IEC 61850 GOOSE, where IEC 61850 is mainly used for delivering data (status, sampled value and command) among IEDs (Intelligent Electronic Devices) to substation automation controllers.

Although existing network security solutions, which use cryptographic techniques to protect data integrity, can be very effective in defeating the data modifications/injection attacks, deployment of such techniques calls for an upgrade of all the existing power generation systems. Definitely, the upgrade is not only costly, but also has significant impact on the continuous operations of these systems, and may encounter interoperability problem [49]. In addition, it is unable to prevent the attack using direct load manipulation introduced in Section V-B2. Thus, alternative protection methods need to be considered, especially for legacy systems.

The attacks presented in this paper take effect due to resonance effect. Hence, if the tampered input is reshaped (e.g., average), the resonance effect will be weakened such that the attack fails. Fig. 26 shows the mitigation result when the tampered input is averaged every 2 seconds.[5] Fig. 26.b is the load change faked by a resonance attacker. After the faked load is reshaped by the power plant, it is changed as Fig. 26.c. Clearly, as both RoCoF and frequency derivative in Fig. 26.a are very small, the protected system is stable even if it is attacked.

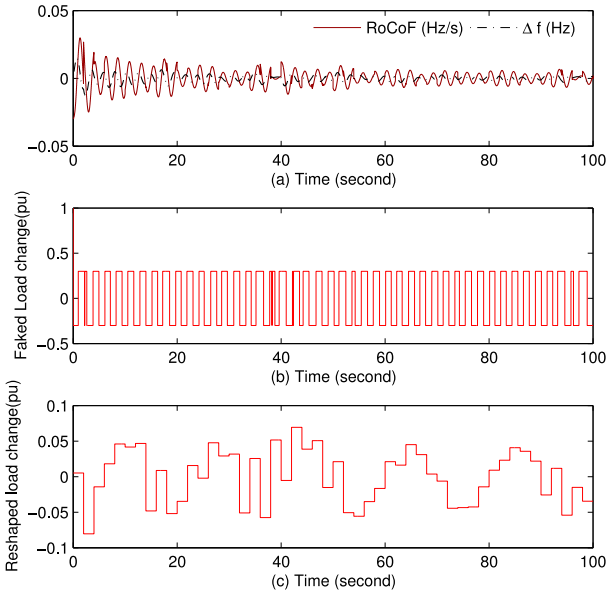


Fig. 26. Countermeasure on resonance attack by using the average value of load change within 2 seconds.

TABLE IV
COMPARISON OF ATTACK SCHEMES

Scheme	Model	Point	Computation	Anti-Crypto
TDS [18]	LTI	Cin	Simple	Yes
DOS [19]	LTI	Cin	Simple	Yes
FDI_b [20]	LTI	Load	Optimization	No
FDI_c [21]	(Non)linear	Cin/Cout	Optimization	No
FDI_s [22]	LTI	Cin	Optimization	No
Present	(Non)linear	Load	Simple	∼Yes

FDI_b, FDI_c, FDI_s : FDI at breaker, controller, sensor respectively
Cin/Cout: Controller input/output.

E. Comparison of LFC Attacks

As the stability and security of power grid is very important in modern societies, it is a hot topic in power research community. Table IV lists the comparison result among LFC attacks.

The second column shows that the system models used in the works. Both scheme FDI_c (False Data Injection at controller) [21] and the present one are applicable to linear and non-linear plant models, while the rest focus on LTI (Linear Time Invariant) model only.

The third column is the comparison of attack points. Both scheme FDI_s (False Data Injection at sensor) [19] and the present one manipulate the load, while other schemes manipulate the controller input (Cin) or output (Cout). Generally, the controller signals, especially the controller output, are protected with dedicated channels, hence it is hard for an adversary to manipulate them.

The fourth column shows the computational cost for the attacker. Schemes FDI_x [20]–[22] require complicated optimization processes for every attack operation and are very time-consuming, while TDS, DOS and ours do not require computation process and hence can be launched from resource-restricted devices, e.g., circuit breaker and smart meter.

The last column illustrates whether the attacks are applicable to cryptographically protected power systems. As TDS attack and DOS attack do not change the communication traffic, cryptographic protection technologies can not be used to defeat them, but schemes FDI_x [20]–[22] can be defeated with integrity protection as they depend on traffic manipulation. As elaborated in Section V-D, if load manipulation is realized directly, cryptographic protection schemes are invalid in defeating the present attacks.

VI. CONCLUSION

In this paper we presented resonance attacks in which attackers slightly modify the load input such that LFC in existing electric power generation systems becomes ineffective in stabilizing the system. The effectiveness of the resonance attacks are verified and demonstrated by simulating the attacks on LFC systems which are one of the most critical sub-systems in smart grids. Based on the simulation results, the proposed attacks can destabilize both single-area LFC and multi-area

[5]If the attacker modifies the actual load as Section V-B2 introduces, the power system is able to reshape the actual load with transformers, response delay and electricity storage.

LFC systems. In order to defeat the resonance attack, we proposed a countermeasure which reshapes the faked load.

The stability of a close-loop cyber-physical system is tightly related to its parameters whether it is under attack or not. Although the present countermeasure is able to stabilize the system by invalidating the resonance effect, it may be vulnerable to advanced attacks. Hence, how to further improve the countermeasure is interesting. In addition, as renewable energy resources (e.g., wind, solar or electric vehicles) are more and more important, and their models are different from the governor-turbine model, their security and countermeasure are interesting topics too.

REFERENCES

[1] J. Meserve. *Staged Cyber Attack Reveals Vulnerability in Power Grid*. Accessed on Sep. 26, 2007. [Online]. Available: http://edition.cnn.com/2007/US/09/26/power.at.risk/

[2] Y. W. Law, T. Alpcan, and M. Palaniswami, "Security games for risk minimization in automatic generation control," *IEEE Trans. Power Syst.*, vol. 30, no. 1, pp. 223–232, Jan. 2015.

[3] S. F. Bush, *Smart Grid: Communication-Enabled Intelligence for the Electric Power Grid*. Chichester, U.K.: Wiley, Jan. 2014, p. 570.

[4] *Hourly Real-Time Load vs. Actual Report*. Accessed on Jan. 11, 2016. [Online]. Available: http://www.ercot.com/mktinfo/rtm/index.html

[5] *Indian Electricity Grid Code*, Central Elect. Regul. Comm., New Delhi, India, Apr. 2010. [Online]. Available: http://cercind.gov.in/2010/ORDER/February2010/IEGC_Review_Proposal.pdf

[6] Q. Dong, D. Niyato, P. Wang, and Z. Han, "Deferrable load scheduling under imperfect data communication channel," *Wireless Commun. Mobile Comput.*, vol. 15, no. 17, pp. 2049–2064, Dec. 2015.

[7] Q. Cui, X. Wang, X. Wang, and Y. Zhang, "Residential appliances direct load control in real-time using cooperative game," *IEEE Trans. Power Syst.*, vol. 31, no. 1, pp. 226–233, Jan. 2016.

[8] X. Lou, D. K. Y. Yau, H. H. Nguyen, and B. Chen, "Profit-optimal and stability-aware load curtailment in smart grids," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1411–1420, Sep. 2013.

[9] A. Mahmood, N. Javaid, M. A. Khan, and S. Razzaq, "An overview of load management techniques in smart grid," *Int. J. Energy Res.*, vol. 39, no. 11, pp. 1437–1450, 2015.

[10] H. H. Nguyen, R. Tan, and D. K. Y. Yau, "Safety-assured collaborative load management in smart grids," in *Proc. Int. Conf. Cyber Phys. Syst.*, Berlin, Germany, 2014, pp. 151–162.

[11] L. Wu and J. M. Yang, "Load frequency control of area power system with multi-source power generation units based on differential games tracking control," in *Proc. IEEE PES Asia–Pac. Power Energy Eng. Conf.*, Hong Kong, 2013, pp. 1–6.

[12] H. A. Yousef, K. AL-Kharusi, M. H. Albadi, and N. Hosseinzadeh, "Load frequency control of a multi-area power system: An adaptive fuzzy logic approach," *IEEE Trans. Power Syst.*, vol. 29, no. 4, pp. 1822–1830, Jul. 2014.

[13] H. Chen, R. Ye, X. Wang, and R. Lu, "Cooperative control of power system load and frequency by using differential games," *IEEE Trans. Control Syst. Technol.*, vol. 23, no. 3, pp. 882–897, May 2015.

[14] M. Qiu, W. Gao, M. Chen, J.-W. Niu, and L. Zhang, "Energy efficient security algorithm for power grid wide area monitoring system," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 715–723, Dec. 2011.

[15] J. Ree, V. Centeno, J. S. Thorp, and A. G. Phadke, "Synchronized phasor measurement applications in power systems," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 20–27, Jun. 2010.

[16] M. Chenine, J. Ullberg, L. Nordström, Y. Wu, and G. N. Ericsson, "A framework for wide-area monitoring and control systems interoperability and cybersecurity analysis," *IEEE Trans. Power Del.*, vol. 29, no. 2, pp. 633–641, Apr. 2014.

[17] J. Kim and L. Tong, "On phasor measurement unit placement against state and topology attacks," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Vancouver, BC, Canada, 2013, pp. 396–401.

[18] A. Sargolzaei, K. Yen, and M. N. Abdelghani, "Time-delay switch attack on load frequency control in smart grid," *J. Adv. Commun. Technol.*, vol. 5, pp. 55–64, Nov. 2014.

[19] S. Liu, X. P. Liu, and A. El Saddik, "Denial-of-service (dos) attacks on load frequency control in smart grids," in *Proc. IEEE PES Innov. Smart Grid Technol.*, Washington, DC, USA, 2013, pp. 1–6.

[20] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 2, pp. 273–285, Dec. 2013.

[21] M. Vrakopoulou, P. M. Esfahani, K. Margellos, J. Lygeros, and G. Andersson, "Cyber-attacks in the automatic generation control," in *Cyber Physical Systems Approach to Smart Electric Power Grid*. Heidelberg, Germany: Springer, 2015, pp. 303–328.

[22] R. Tan *et al.*, "Optimal false data injection attack against automatic generation control in power grids," in *Proc. ACM/IEEE 7th Int. Conf. Cyber Phys. Syst.*, Vienna, Austria, 2016, pp. 1–10.

[23] K. C. Sou, H. Sandberg, and K. H. Johansson, "On the exact solution to a smart grid cyber-security analysis problem," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 856–865, Jun. 2013.

[24] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1731–1738, Sep. 2012.

[25] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1665–1676, Jul. 2014.

[26] A. Rosich, H. Voos, and M. Darouach, "Cyber-attack detection based on controlled invariant sets," in *Proc. Eur. Control Conf. (ECC)*, Strasbourg, France, 2014, pp. 2176–2181.

[27] M. Krotofil, J. Larsen, and D. Gollmann, "The process matters: Ensuring data veracity in cyber-physical systems," in *Proc. 10th ACM Symp. Inf. Comput. Commun. Security, (ASIA CCS)*, Singapore, 2015, pp. 133–144.

[28] S. Ntalampiras, "Detection of integrity attacks in cyber-physical critical infrastructures using ensemble modeling," *IEEE Trans. Ind. Informat.*, vol. 11, no. 1, pp. 104–111, Feb. 2015.

[29] B. Shah, A. Bose, and A. Srivastava, "Load modeling and voltage optimization using smart meter infrastructure," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. (ISGT)*, Washington, DC, USA, 2013, pp. 1–6.

[30] H. K. Kargar and J. Mirzaei, "New method for islanding detection of wind turbines," in *Proc. IEEE 2nd Int. Power Energy Conf.*, Johor Bahru, Malaysia, 2008, pp. 1633–1637,

[31] *The Commission for Energy Regulation, Rate of Change of Frequency (Rocof) Modification to the Grid Code, Reference*, CER/14/081, Apr. 4, 2014. [Online]. Available: http://www.cer.ie/docs/000260/CER14081%20ROCOF%20Decision%20Paper%20-%20FINAL%20FOR%20PUBLICATION.pdf

[32] H. Bevrani, *Robust Power System Frequency Control*. New York, NY, USA: Springer, 2009, ch. 2.

[33] L. Jiang, W. Yao, Q. H. Wu, J. Y. Wen, and S. J. Cheng, "Delay-dependent stability for load frequency control with constant and time-varying delays," *IEEE Trans. Power Syst.*, vol. 27, no. 2, pp. 932–941, May 2012.

[34] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed Internet-based load altering attacks against smart power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 667–674, Dec. 2011.

[35] J. Hong, Y. Chen, C.-C. Liu, and M. Govindarasu, "Cyber-physical security testbed for substations in a power grid," in *Cyber Physical Systems Approach to Smart Electric Power Grid*. Heidelberg: Springer, 2015, pp. 261–301.

[36] P. Pourbeik *et al.*, "Dynamic models for turbine-governors in power system studies," IEEE Power Energy Soc., Piscataway, NJ, USA, Tech. Rep. PES-TR1, Jan. 2013. [Online]. Available: http://sites.ieee.org/fw-pes/files/2013/01/PES_TR1.pdf

[37] NEPLAN AG. *Turbine-Governor Models: Standard Dynamic Turbine-Governor Systems in NEPLAN Power System Analysis Tool*. Accessed on Feb. 20, 2017. [Online]. Available: http://www.neplan.ch/wp-content/uploads/2015/08/Nep_TURBINES_GOV.pdf

[38] R. T. Byerly *et al.*, "Dynamic models for steam and hydro turbines in power system studies," *IEEE Committee Rep. Trans. PAS*, vol. 92, no. 6, pp. 1904–1915, Nov./Dec. 1973.

[39] E. Rakhshani and J. Sadeh, "Application of power system stabilizer in a combined model of LFC and AVR loops to enhance system stability," in *Proc. Int. Conf. Power Syst. Technol.*, Hangzhou, China, 2010, pp. 1–5.

[40] S. Satyanarayana, R. K. Sharma, Mukta, and A. K. Sappa, "Automatic generation control in power plant using PID, PSS and fuzzy-PID controller," in *Proc. Int. Conf. Smart Elect. Grid (ISEG)*, Guntur, India, 2014, pp. 1–8.

[41] M. Mahdavian, G. Shahgholian, M. Janghorbani, S. Farazpey, and M. Azadeh, "Analysis and simulation of PID-PSS design for power system stability improvement," in *Proc. 13th Int. Conf. Elect. Eng. Electron. Comput. Telecommun. Inf. Technol. (ECTI-CON)*, 2016, pp. 1–6.

[42] O. Thapar, *Modern Hydroelectric Engineering Practice in India: Electro-Mechanical Works*. Accessed on Feb. 20, 2017. [Online]. Available: http://www.iitr.ac.in/departments/AH/pages/Publications_Downloads+Modern_Hydroelectric_Engg_Practice_by_Prof_OD_Thapar.html

[43] D.J. Hammerstrom *et al.*, *Pacific Northwest GridWise™ Testbed Demonstration Projects: Part II. Grid Friendly™ Appliance Project*, Pac. Northwest Nat. Lab., Richland, WA, USA, Oct. 2007. [Online]. Available: http://www.pnl.gov/main/publications/external/technical_reports/PNNL-17079.pdf

[44] K. Kalsi *et al.*, *Distributed Smart Grid Asset Control Strategies for Providing Ancillary Services*, Pac. Northwest Nat. Lab., Richland, WA, USA, Sep. 2013. [Online]. Available: http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-22875.pdf

[45] S. A. Pourmousavi and H. Nehrir, "Introducing dynamic demand response in the LFC model," *IEEE Trans. Power Syst.*, vol. 29, no. 4, pp. 1562–1572, Jul. 2014.

[46] J. A. Short, D. G. Infield, and L. L. Freris, "Stabilization of grid frequency through dynamic demand control," *IEEE Trans. Power Syst.*, vol. 22, no. 3, pp. 1284–1293, Aug. 2007.

[47] C. Kaufman, R. Perlman, and M. Speciner, *Network Security: Private Communication in a Public World*. Englewood Cliffs, NJ, USA: Prentice-Hall, 2002.

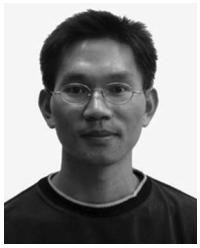
[48] S. Fries, H. J. Hof, and M. Seewald, "Enhancing IEC 62351 to improve security for energy automation in smart grid environments," in *Proc. 5th Int. Conf. Internet Web Appl. Services*, Barcelona, Spain, 2010, pp. 135–142,

[49] ENISA. *Smart Grid Security Certification in Europe: Challenges and Recommendations*. Accessed on Dec. 19, 2014. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/smart-grid-security-certification-in-europe-challenges-and-recommendations

Yongdong Wu received the B.Eng. and M.S. degrees from Beihang University, the Ph.D. degree from the Institute of Automation, Chinese Academy of Science, and the Master for Management of Technology degree from the National University of Singapore. He is currently a Senior Scientist with Infocomm Security Department, Institute of Infocomm Research, Agency for Science Technology, and Research (A*STAR), Singapore. He is also an Adjunct Associate Professor with the Singapore Management University. He has published over 100 papers and 7 patents. His research interests include multimedia security, cyber-physical system security, IoT security, and network security. His research results and proposals was incorporated in the ISO/IEC JPEG 2000 Security Standard 15444-8 in 2007. He was a recipient of the Best Paper Award of IFIP Conference on Communications and Multimedia Security 2012.

Zhuo Wei received the B.A. degree from Jilin University, China, and the M.S. and Ph.D. degrees from the Huazhong University of Science and Technology, China.

He is currently a Research Scientist with Huawei International Company, Singapore. His interests include image processing and video processing. He was a recipient of the Best Paper Award of CMS 2012.



Jian Weng received the Ph.D. degree from Shanghai Jiaotong University, Shanghai, China, in 2008.

He is currently a Professor and the Dean with the School of Information Technology, Jinan University, Guangzhou, China. He has published over 60 papers in cryptography conferences and journals. He was a recipient of a number of awards including the 2014 Chinese Association for Cryptographic Research Cryptographic Innovation Award, the 2011 Symposium on Cryptography and Information Security Best Paper Award, and the 8th International Conference on Provable Security Best Student Award in 2014.

Xin Li received the B.Eng. degree from Xi'an Jiaotong University, China, in 1992.

He is a Guest Professor of Zheng Zhou University, China. His research interests include computer image processing, pattern recognition, public safety and security, and cloud computing. He is the Founder and the CEO of Sinocloud Wisdom Company Ltd.

Robert H. Deng (F'16) received the B.Eng. degree from the National University of Defense Technology, China, in 1981, and the M.Sc. and Ph.D. degrees from the Illinois Institute of Technology, Chicago, IL, USA, in 1983 and 1985, respectively.

He is a Professor of Information Systems, the Director of Secure Mobile Center, and the Dean of Postgraduate Research Programme, Singapore Management University. His research interests include data security and privacy, multimedia security, network, and system security. He was a recipient of the University Outstanding Researcher Award from the National University of Singapore in 1999 and the Lee Kuan Yew Fellow for Research Excellence from the Singapore Management University in 2006. He has served/is serving on the editorial boards of many international journals in security, such as the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, the IEEE SECURITY & PRIVACY, and the *Journal of Computer Science and Technology*. He is the Chair of the Steering Committee of the ACM Asia Conference on Computer and Communications Security. He was named Community Service Star and Showcased Senior Information Security Professional by $(ISC)^2$ under its Asia–Pacific Information Security Leadership Achievements Program in 2010.