IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 14, 2020, accepted October 21, 2020, date of publication October 26, 2020, date of current version November 6, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3033566

Coordinated False Data Injection Attacks in AGC System and Its Countermeasure

XI HE[1], (Member, IEEE), XUAN LIU[2], (Member, IEEE), AND PENG LI[3]
[1]Department of Electrical and Information Engineering, Hunan Institute of Technology, Hengyang 421002, China
[2]Department of Electrical and Information Engineering, Hunan University, Changsha 410006, China
[3]Digital Research Institute, China Southern Power Grid, Guangzhou 510663, China

Corresponding author: Xi He (forevermau@163.com)

This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFB0902900, in part by the Provincial Educational Department Fund for Excellent Young Scholars under Grant 19B137, in part by the National College Students Innovative and Entrepreneurship Training Scheme under Grant S202011528005, and in part by the Provincial College Teaching Reform and Research Project under Grant HNJG-2020-1062.

ABSTRACT The Automatic Generation Control (AGC) system is vital for power system frequency stability. The frequency and tie-line power flow are measured and transmitted to the control room to form Area Control Error (ACE), which is then sent to each generator for power generation adjustment. Due to the vulnerability of the Inter-Control Center Communication (ICCP) protocol, which is used for data transmission, many attacks such as Denial of Service, timing de-synchronization, and False Data Injection (FDI) attack can be inflicted upon the compromised system. In this paper, we investigated the attacking mechanism and the impact of the coordinated FDI attack. Compared with the single attack model, the coordinated FDI attack has a smaller Time to Emergency (TTE) value and wider parameter ranges. Therefore, it is stealthier and more harmful to the AGC system. However, it is found that the pattern of the corrupted ACEs (attacked by a specific coordination FDI attack) follows a specific fashion. Therefore, we proposed a self-learning and evolving approach to detect this stealthy attack. The real data from an electric company helps to train and test the pattern recognition model. The coordinated attack is simulated and compared in a 3-area AGC system, while the proposed detection method is verified via the IEEE 39-bus test system.

INDEX TERMS False data injection attack, automatic generation control (AGC), pattern recognition, area control error (ACE).

NOMENCLATURE

AGC	Automatic Generation Control
ACE	Area Control Error
EDC	Economic Dispatch Control
RoCoF	Rate of Change of Frequency
UFLS	under-frequency load shedding
FDI	False Data Injection
TTE	Time to Emergency
ICCP	Inter-Control Center Communication
DNP3	Distributed Network Protocol 3.0
PJM	Pennsylvania-New Jersey-Maryland Cooperation
λ_s	attacking factor of the scale attack
λ_r	attacking factor of the ramp attack
λ_p	attacking factor of the pulse attack
τ_T	turbine time constant

The associate editor coordinating the review of this manuscript and approving it for publication was Yassine Maleh.

τ_g	governor time constant
R	speed regulation
D	frequency sensitivity load coefficient
K_{I}	AGC integrator gain
H	inertial constant
P_s	synchronizing power coefficient
$a_1 \sim a_6$	six injected attack vectors
ΔP_{ij}	tie-line power flow deviation from the scheduled value
$\Delta\omega_i$	angular frequency deviation from the nominal value
B_i	frequency bias factor
δ_i	the set of areas that area i is connected to
a_{tie}	tie-line attack vector
a_f	frequency attack vector
$\boldsymbol{H}$	state-space matrix
$p(x\|C_k)$	class-conditional densities
$p(C_k)$	class priors

$p(C_k\|x)$	posterior probabilities
$\sigma(\mathrm{a})$	*logistic sigmoid* function
$y(x)$	recognition function

I. INTRODUCTION

In the power system, Automatic Generation Control (AGC) is regarded as the most critical function among three power control measures, i.e., the control via synchronous generator's governor, AGC, and EDC (Economic Dispatch Control) [1]–[3]. It is responsible for the load fluctuation cycling from 10s to 2-3min, which is no longer suitable for governor control. The primary purpose of AGC is to maintain the nominal power system frequency and minimizes the tie-line power deviation. The former function is for safety purposes, while the latter is mainly due to economic consideration. Basically, AGC is a closed-loop feedback control system that uses frequency and tie-line power measurements to form the control signal, i.e., Area Control Error (ACE). The formed ACE signal is sent to each generator to adjust its output, and this process repeats every 2-5 seconds [4]–[6].

However, as deepening integration and coupling between the physical power system and cyber system, the AGC system faces severe security challenges. Malware infection, eavesdropping, False Data Injection (FDI) attack, Denial-of-Service (DoS), password pilfering, and de-synchronization threaten the safety and integrity of the power system. The AGC system's vulnerability can be categorized into two aspects: measurement data tampering and control data tampering. Fig. 1 illustrates a 3-area interlinked system and its vulnerabilities.

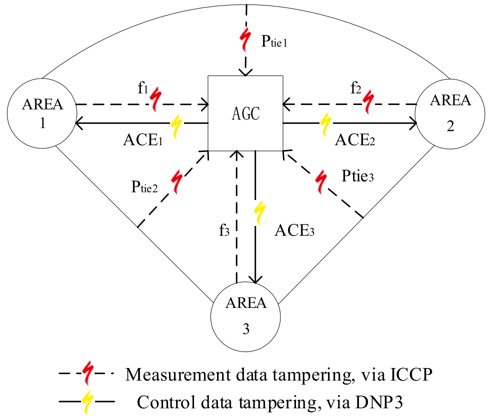

Ptie1
f1
f2
AREA 1
AGC
AREA 2
ACE1
ACE2
Ptie2
Ptie3
f3
ACE3
AREA 3
Measurement data tampering, via ICCP
Control data tampering, via DNP3

FIGURE 1. A 3-area interlinked system and its vulnerabilities.

The measurement data tampering can be achieved by a false data injection attack first investigated by Liu *et al.* [7]. By stealthily injecting false data into the measurements, the perpetrator can affect ACE value to sabotage the frequency stability and economic power dispatch. On the other hand, the control attack is to alter or block the computed ACE corrections, which is supposed to be sent to the generators. It can be realized by FDIA or Denial of Service (DoS) attack. In most scenarios, the control signal is sent to the Balancing Area (BA) via Distributed Network Protocol 3.0 (i.e., DNP3) [8]. There are existing IEEE standards (such as IEEE 1815-2012) and loads of secure authentications for DNP3 security [9]. While for the measurement data transmission, the widely deployed Inter-Control Center Communication Protocol (ICCP) is vulnerable to many cyber attacks, such as data manipulation, Denial of Service (DoS), timing de-synchronization, and false data injection attacks [10]. In this paper, we focus on the false data injection attack during measurement data collection.

False data injection attack is a major threat to the security of the power system. It falsifies the original measurement data by hacking into the compromised Intelligent Electronic Devices (IEDs) or transmission devices. FDI attack affects not only the AGC system, but also other important functions, such as power system state estimation, power economic dispatch, and the integration of renewable energy [11]–[13]. The impact of FDI attacks on AGC systems has been investigated using different methodologies, such as model-based analysis [15] and state estimation [21].

Normally, there are simple bad data detection algorithms to deter adversaries' actions. A straightforward bad data checking algorithm in the AGC system can be formed as the following expression:

$$\left|\frac{ACE_{i,t} - ACE_{i,t+T}}{T}\right| < \varepsilon \tag{1}$$

where $ACE_{i,t}$ is the calculated ACE at time t, T is the processing interval, which is 2-5 seconds, ε is the threshold. In the power system state estimation function, the Chi-square χ^2 distribution is used for bad data detection and identification. The square of the measurement residual will have a χ^2 distribution with N degrees of freedom, i.e.

$$\sum_{i=1}^{N}(x_i - \hat{x}_i)^2 \sim \chi^2 \tag{2}$$

where x_i and $\hat{x}_i$ is the measurement and estimated measurement, respectively.

Attacks can be classified as brute-force attacks or intelligent coordinated attacks. The brute-force attack is simple and straightforward yet easy to be detected. An example of this attack is a line-tripping attack. On the other hand, a coordinated attack requires a deep understanding of the system and sophisticated hacking skills. This attack pattern can cause severe damage to the system because it nullifies power system defenses and penetrates stealthily. A good example to illustrate the coordinated attack is the Ukraine cyber-induced power outage in 2015 [14]. The highly structured and resourced perpetrator was co-adaptive and demonstrated varying tactics/techniques to match the defenses of the three impacted distribution grids. What's more, the attack was conducted in an orderly fashion that is hard for the defense system to react.

This paper investigates the mechanism of coordinated FDI attack in the AGC system and its impact; afterward, a novel detection method based on pattern recognition is proposed. The comparison of the coordinated attack and single attack is simulated based on a 3-area AGC system, and the effectiveness of the proposed countermeasure is verified by the IEEE 39-bus test system. The contribution of this paper can be summarized as follows:

- The attack mechanism of the coordinated attack is thoroughly studied. Unlike other studies that merely focus on single attack models, i.e., the scale/ramp/pulse/random attack, the proposed coordinated attack is a combination of several attack templates. Therefore, its Time-to-Emergency (TTE) value and parameter ranges (λ_s, λ_r, λ_p) are quite different from its counterparts.
- An artificial intelligence-based method is proposed to tackle the sophisticated, coordinated attack. Different from many studies in which attack detection involves either state estimation or load forecast, the proposed countermeasure is a pure statistics approach that embodies self-learning and evolving.
- A 3-area AGC system is simulated to compare four different scenarios. It shows severer damage can be caused yet hard to detect. Meanwhile, the IEEE 39-bus test system, which can be regarded as a specific real 3-area AGC system, is simulated to find the attacked ACE patterns for coordinated attack detection.

The rest of the paper is organized as follows. Section II conducts a brief literature review. Section III explains the AGC system and single attack templates. Section IV elaborates on the coordinated attack, including injected measurement coordination and attack model coordination. In section V, the pattern recognition-based attack detection method is proposed. Finally, Section VI concludes the paper.

II. RELATED WORK

Attacks can be classified as brute-force attacks or intelligent coordinated attacks. The cyber attack on the Ukrainian power grid is a typical coordinated attack that involves false data injection attack, spear-phishing emails, BlackEnergy3 malware, credential cracking, denial-of-service, KillDisk modification, etc. [14]. Normally, the research of the coordinated FDI attack against the AGC system is based on the single attack models presented by Sridhar *et al.* in 2014 [15]. In [16], the authors derived an optimal attack, which is a combination of a series of false data injections. It also showed that, based on eavesdropped sensor data and a few feasible-to-obtain system constants, the attacker could learn the attack impact model and achieve the optimal attack in practice. Other optimized or coordinated related FDI attacks against the AGC system can be found in [17]–[19].

For its countermeasures, the authors used an unknown input observer (UIO) to estimate the states of the load frequency control system and then calculate the UIO's residual function for anomaly detection in [20]. In [21], a machine learning-based algorithm was proposed to tackle the stealthy FDI attack. The authors used Neural Network, namely Long Short-Term Memory (LSTM), to train and forecast the ACE value, and used Fast Fourier Transform (FFT) to covert the moving average data from a time domain to a frequency domain for scale attack detection. However, it is only suitable for a single attack scenario, whose pattern period is about 50 AGC cycles. There are other literature works looking into the application of machine learning or artificial intelligence technology in this territory [5], [22], [23]. Deb Roy *et al.* investigated the unique feature of low inertial AGC systems, such as the system with lots of renewable generations. Low inertial grid experiences larger frequency fluctuation during any perturbation due to the lack of rational inertia [24]. Ashok *et al.* investigate the PowerCyber CPS testbed for experimental evaluation of cyber attacks on the AGC system at Iowa State University. Two types of cyber attacks, namely, measurement attack and control attack, are performed, and its impacts on system frequency and load supply, are investigated [25]. There are other testbeds for Supervisory Control And Data Acquisition (SCADA) or Wide-Area Monitoring, Protection and Control (WAMPAC) system, such as the National SCADA Testbed (NSTB) [26], Virtual Control System Environment (VCSE) testbed in Sandia National Laboratory [27], Virtual Power System Testbed (VPST) in University of Illinois [28], etc.

III. SYSTEM DESCRIPTION AND ATTACK MODELING

In an interlinked power transmission system, generators are equipped with Load Frequency Control (LFC) and Automatic Voltage Regulator (AVR). The LFC has a preset frequency and constantly monitors the tiny variation of the frequency and active power output. Base on this, the steam turbines' valve is controlled. Similarly, the AVR has a preset voltage and constantly monitors the tiny variation of the voltage and reactive power output. Base on this, the field current is regulated. The time constant of the excitation system is much smaller than that of the turbine, so the transient damping of the AVR is much faster than that of the LFC. In this sense, the two control loops can be decoupled and analyzed separately.

AGC is the most important LFC method in the power system. The control block diagram of the 3-area AGC system is depicted in Appendix A, and the system parameters, as well as its assumed value in each area, are stated in Table 1.

In the control block diagram, six additional inputs ($a_1 \sim a_6$) are added to model the false data injection attack. The six attack vectors are injected to tamper the frequency bias measurement in area 1, 2, and 3 (Δf_1, Δf_2, and Δf_3), and the tie-line power flow measurement ($\Delta P_{tie1\text{-}2}$, $\Delta P_{tie1\text{-}3}$, and $\Delta P_{tie2\text{-}3}$). Therefore, the compromised measurements can be denoted as $\Delta\omega_n + a_n$ ($n = 1, 2, 3$) and $\Delta P_{ij} + a_m$ ($m = 4, 5, 6$). According to [15], there are three attack templates:

i) Scaling Attack. This attack vector is formed by scaling the true measurements.

$$a = (1 + \lambda_s)^* z \tag{3}$$

TABLE 1. Parameters of the 3-area system.

Parameters	Description	Area 1	Area 2	Area 3
τ_T	Turbine time constant	0.5(s)	0.4(s)	0.3(s)
τ_g	Governor time constant	0.25(s)	0.2(s)	0.15(s)
R	Speed regulation	0.04(p. u.)	0.035(p.u.)	0.030(p.u.)
D	Frequency sensitivity load coefficient	1.2	1.4	1.6
K_I	AGC integrator gain	0.5	0.5	0.5
H	Inertial constant	8(s)	7(s)	6(s)
P_s	Synchronizing power coefficient	1.5	1.4	1.3
B_i	Frequency bias factor $B_i = \frac{1}{R_i} + D_i$	26.20	29.97	34.93

where λ_s is the scaling factor, and z is the true measurement.

ii) *Ramp Attack*. This attacking vector is formed by adding a ramp function that gradually increases with time.

$$a = z + \lambda_r{}^{*}t \tag{4}$$

iii) *Random Attack*. This attacking vector is formed by adding a random positive value to the true measurement.

$$a = z + rand(x, y) \tag{5}$$

iv) *Pulse Attack*. This attack involves the addition of a very short period pulse to the true measurement. We regard this attack as a special kind of random attack.

The ACE signal of area *i* is:

$$ACE_i = \sum_{j\in\delta_i} \Delta P_{ij} + B_i \Delta\omega_i \tag{6}$$

where ΔP_{ij} is the tie-line power flow deviation from the scheduled value, $\Delta\omega_i$ is the angular frequency deviation from the nominal value, i.e., 100π (50Hz power system) or 120π (60Hz power system). B_i is the frequency bias factor that determines the reciprocity of the two connected areas during a disturbance. δ_i is the set of areas that area *i* is connected to.

The various attack models can be integrated into the ACE expression to obtain the compromised $ACE_{i.c}$,

$$ACE_{i.c} = \sum_{j\in\delta} (\Delta P_{ij} + a_{tie}) + \beta_i(\Delta\omega_i + a_f) \tag{7}$$

where a_{tie}, a_f represent the tie-line attack and frequency attack, respectively. The perpetrator can target either type of measurement or even both.

IV. COORDINATED FALSE DATA INJECTION ATTACK

A. INJECTED MEASUREMENTS COORDINATION

The AGC system has a simple validation mechanism to verify the input measurements' credibility and calculated ACEs. An alarm will raise if any of the following situations happens:

- The Rate of Change of Frequency (RoCoF) exceeds a certain value, e.g., if the frequency exceeds 1Hz during a 15-second time window, an alarm will be raised [20].
- The definite value of the system frequency, tie-line power, or ACE signal exceeds a predefined limit, e.g., the system frequency exceeds ±0.1Hz, or the ACE signal exceeds ±0.05 p.u..
- Other situations, such as the ACE signal does not return to around zero within 10 minutes; the average value of the ACE signal during a specific consecutive time window exceeds the threshold, etc.

However, this primitive approach is susceptible to the coordinated FDI attack. Still using the 3-area system illustrated in Appendix A, the mathematic state description is

$$\dot{x}(t) = x(t) + u(t) + Ca(t) + \omega(t) \tag{8}$$

where $x = [\Delta f_1, \Delta f_2, \Delta f_3, \Delta P_{g1}, \Delta P_{g2}, \Delta P_{g3}, \Delta P_{T1}, \Delta P_{T2}, \Delta P_{T3}, \Delta P_{tie12}, \Delta P_{tie13}, \Delta P_{tie23}, \mathrm{ACE}_1, \mathrm{ACE}_2, \mathrm{ACE}_3]^T$, $u(t) = [u_1(t), u_2(t)]$ is the load disturbance, $a(t) = [a_1(t), a_2(t), a_3(t), a_4(t), a_5(t), a_6(t)]$ is the attack vector, and $\omega(t)$ denotes the process noise. The coefficient C is a constant used for scaling the coordinated attack vector. The state space matrices of the 3-area AGC system can be obtained. For simplicity, only the state variables of area 1 is stated here as follows:

$$\begin{aligned}\Delta\dot{f}_1 &= \frac{-D_1}{2H_1}\Delta f_1 + \frac{1}{2H_1}\Delta P_{T1} - \frac{1}{2H_1}\Delta P_{tie12} \\ &\quad - \frac{1}{2H_1}\Delta P_{tie13} - \frac{1}{2H_1}u_1 + \frac{1}{2H_1}a_1 \end{aligned} \tag{9}$$

$$\Delta\dot{P}_{T1} = \frac{-1}{T_{T1}}\Delta P_{T1} + \frac{1}{T_{T1}}\Delta P_{g1} \tag{10}$$

$$\Delta\dot{P}_{g1} = \frac{-1}{R_1 T_{g1}}\Delta f_1 - \frac{1}{T_{g1}}\Delta P_{g1} + \frac{1}{T_{g1}}ACE_1 \tag{11}$$

The three tie-line power are related to the connected areas' frequency deviation, as well as the corresponding attacks.

$$\Delta\dot{P}_{tie12} = P_s\Delta f_1 - P_s\Delta f_2 + a_4 \tag{12}$$

$$\Delta\dot{P}_{tie13} = P_s\Delta f_1 - P_s\Delta f_3 + a_5 \tag{13}$$

$$\Delta\dot{P}_{tie23} = P_s\Delta f_2 - P_s\Delta f_3 + a_6 \tag{14}$$

The three ACEs are related to the frequency deviation, connected areas' tie-line power deviation, and the corresponding attacks.

$$\begin{aligned}\dot{ACE}_1 &= -K_{I1}B_1\Delta f_1 - K_{I1}\Delta P_{tie12} - K_{I3}\Delta P_{tie13} \\ &\quad + K_{I1}B_1 a_1 + K_{I1}a_4 \end{aligned} \tag{15}$$

$$\begin{aligned}\dot{ACE}_2 &= -K_{I2}B_2\Delta f_2 + K_{I2}\Delta P_{tie12} - K_{I3}\Delta P_{tie23} \\ &\quad + K_{I2}B_2 a_2 + K_{I2}a_5 \end{aligned} \tag{16}$$

$$\begin{aligned}\dot{ACE}_3 &= -K_{I3}B_3\Delta f_3 - K_{I3}\Delta P_{tie13} - K_{I3}\Delta P_{tie23} \\ &\quad + K_{I3}B_3 a_3 + K_{I3}a_6 \end{aligned} \tag{17}$$

where

$$B_i = \frac{1}{R_i} + D_i, \quad i = 1, 2, 3 \tag{18}$$

Therefore, the state-space matrix can be obtained. The full matrix is given in Figure 2.

We assume that the attacker has access to *k* specific meters in different areas. According to [7], the attack vector should

$$
\begin{bmatrix}
\frac{-D_1}{2H_1} & 0 & 0 & 0 & 0 & 0 & \frac{1}{2H_1} & 0 & 0 & \frac{1}{2H_1} & \frac{1}{2H_1} & 0 & 0 & 0 & 0 \\
0 & \frac{-D_2}{2H_2} & 0 & 0 & 0 & 0 & 0 & \frac{1}{2H_2} & 0 & \frac{1}{2H_2} & 0 & \frac{1}{2H_2} & 0 & 0 & 0 \\
0 & 0 & \frac{-D_3}{2H_3} & 0 & 0 & 0 & 0 & 0 & \frac{1}{2H_3} & 0 & \frac{1}{2H_3} & \frac{1}{2H_3} & 0 & 0 & 0 \\
\frac{-1}{R_1T_{g1}} & 0 & 0 & -\frac{1}{T_{g1}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{T_{g1}} & 0 & 0 \\
0 & \frac{-1}{R_2T_{g2}} & 0 & 0 & -\frac{1}{T_{g2}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{T_{g2}} & 0 \\
0 & 0 & \frac{-1}{R_3T_{g3}} & 0 & 0 & -\frac{1}{T_{g3}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{T_{g3}} \\
0 & 0 & 0 & \frac{1}{T_{T1}} & 0 & 0 & \frac{-1}{T_{T1}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \frac{1}{T_{T2}} & 0 & 0 & \frac{1}{T_{T2}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \frac{1}{T_{T3}} & 0 & 0 & \frac{1}{T_{T3}} & 0 & 0 & 0 & 0 & 0 & 0 \\
P_s & -P_s & & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & P_s & -P_s & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & P_s & -P_s & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-K_{I1}B_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & K_{I1} & -K_{I3} & 0 & 0 & 0 & 0 \\
0 & -K_{I2}B_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & K_{I2} & 0 & -K_{I3} & 0 & 0 & 0 \\
0 & 0 & -K_{I3}B_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -K_{I3} & -K_{I3} & 0 & 0 & 0
\end{bmatrix}
$$

FIGURE 2. **The full state-space matrix of the AGC system.**

satisfy the equation $\boldsymbol{a} = \boldsymbol{H} \cdot \boldsymbol{c}$, where $\boldsymbol{H}$ is the state-space matrix calculated in Fig. 2, and $\boldsymbol{c}$ is the injected error. Normally, $\boldsymbol{c}$ could be any arbitrary number. For a random FDI attack, the attack vector doesn't have to consider the injected error vector, provided it complies with the equation $\boldsymbol{B} \cdot \boldsymbol{a} = \mathbf{0}$, where $\boldsymbol{B} = \boldsymbol{H}(\boldsymbol{H}^{\mathbf{T}}\boldsymbol{H})\boldsymbol{H}\text{-}\boldsymbol{I}$. The purpose of a coordinated attack is to utilize all the available resources to launch a stealthy and malicious attack that can cause significant damage to the power system. In this sense, the error injected into the AGC system should be carefully chosen. Two criteria must be guaranteed by vector $\boldsymbol{c}$ for a successful stealthy attack:

(i) The injected error could not exceed the alarming threshold;

(ii) $\boldsymbol{c_s} = \boldsymbol{H_s^{-1}}(\boldsymbol{a} - \boldsymbol{b})$.

In (ii), $\boldsymbol{H_s}$ is the sub-matrix of $\boldsymbol{H}$ containing columns, whose indices are not corrupted. $\boldsymbol{c} = [\boldsymbol{c_j}, \boldsymbol{c_s}]$, $\boldsymbol{c_j}$ denotes the targeted state variables with specific error, and $\boldsymbol{c_s}$ denotes the uncompromised state variables.$\boldsymbol{b} = \sum_{j\in\Phi attack} \boldsymbol{h_j}c_j$, where $\boldsymbol{h_j}$ is the indices of $\boldsymbol{H_j}$ representing the corrupted sub-matrix. The physical meaning of (ii) is that in order to launch a stealthy targeted attack, the selection of $\boldsymbol{c}$ should keep the non-attacking region remain unchanged. It means the tie-line power flow and the state variables of the boundary nodes in the non-attacking region should be uninterrupted.

To prove the second requirement, we decompose the attack vector to

$$\boldsymbol{a} = \sum_{i\notin\Phi attack} \boldsymbol{h_s}c_s + \sum_{i\in\Phi attack} \boldsymbol{h_j}c_j = \boldsymbol{H_s}\boldsymbol{c_s} + \boldsymbol{b} \tag{19}$$

Therefore, $\boldsymbol{c_s} = \boldsymbol{H_s^{-1}}(\boldsymbol{a} - \boldsymbol{b})$.

B. ATTACK MODELS COORDINATION

For a 3-area interlinked system, there are six measurements can be tampered. Therefore, the coordinated attack is a congregation of the three attack models. For simplicity, we first investigate the attack mechanism of each type. The 3-area system depicted in Fig. 1 and Appendix A is used for illustration, and its tie-line power flow is stated in Table 2.

TABLE 2. **Tie-line power flow of the 3-area system.**

Lines	Power flow(p.u.)	Direction
Tie-line 1-2	0.2155	From Area 1 to Area 2
Tie-line 1-3	0.1088	From Area 3 to Area 1
Tie-line 2-3	0.0403	From Area 3 to Area 2

Assuming the attacker launches a scale attack on tie-line 1-2 with λ_s equals 0.1. Therefore, the compromised tie-line power flow from Area 1 to Area 2 is 0.2371. For this injected data changed the real power flow measurement between Area 1 and Area 2, the false frequency measurement needs to be calculated according to

$$\Delta F = \frac{-(1+\lambda_s)^k z(t)}{\sum\limits_{i=1}^{n} (\frac{1}{R_i} + D_i)} = 0.012\ (\text{Hz}) \tag{20}$$

where R and D denote speed regulation and frequency sensitivity load coefficient. Here, the baseline value of the tie-line power flow is assumed as 100MW. The outcome ΔF means that it does not exceed the 0.1 Hz threshold.

With the falsified power flow and frequency measurements, the ACE is computed to a value of 0.0083 p.u.. As a result, the generator in Area 1 will ramp down and end up with a deficiency of power supply. As we mentioned at the beginning of this section, the sudden definite change of ACE cannot exceed 0.05 p.u.. Otherwise, the detection system will raise the alarm. On the other hand, the ACE has to be big enough to trigger the under-frequency load shedding (UFLS) or over-frequency disconnecting action. For example, the ULFS will be initiated when the system frequency is below 59 Hz.

It is worth noting that the FDI attack is not a once for all action but an itinerated process. So, the single attack takes several iterations to launch a successful malicious attack. For the above case, the single scale attack takes approximately 20 cycles (i.e., 100s) to cause the ULFS damage. Another prevalent attack is to target the electricity market. By modifying the power flow between two areas, a specific plant can gain benefits. In this case, there is only upper boundary of ACE value, while no lower boundary is required.

For the ramp attack and random attack, the attack mechanism is the same. However, it is worth noting that the time-to-emergency (TTE) value of the ramp attack is larger than those of the two other attacks. TTE is defined as the time from the onset of an attack to the instant when the system takes emergency action. Intuitively, the injected false data of the ramp attack is increasing gradually with time, so it shall take a while to make an impact.

We assume that there are three different attacks inflicted into three different areas, i.e., the scale attack on Tie-line 1-2, the ramp attack on Tie-line 2-3, and the random attack on the frequency in Area 3. As we mentioned above, if the tie-line is under attack, the false injected frequency value of the corresponding area has to be calculated using (20). In order to compare the coordinated attack with single attack, we deliberately use a larger scale and ramping factor. The scale factor λ_s of the scale attack on Tie-line 1-2 is set to 0.3, which exceeds the maximum boundary (0.2922) in the single scale attack scenario, while the ramping factor λ_r of the ramp attack on Tie-line 2-3 is set to 0.1, which also exceeds the maximum boundary (0.0824) in the single ramp attack scenario. The falsified measurements, calculated false frequency deviation, and ACE of the scale attack types are stated in Appendix B.

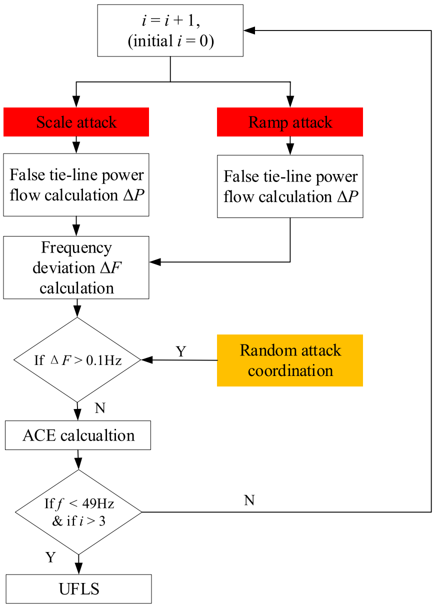

$i = i + 1$,
(initial $i = 0$)
Scale attack
Ramp attack
False tie-line power flow calculation ΔP
False tie-line power flow calculation ΔP
Frequency deviation ΔF calculation
If $\Delta F > 0.1$Hz
Y
Random attack coordination
N
ACE calcualtion
If $f < 49$Hz & if $i > 3$
N
Y
UFLS

FIGURE 3. The process of attack types coordination.

The random attack on the frequency of Area 3 is not yet determined because it is used to coordinate with the scale and ramp attack. If the calculated instant frequency deviation exceeds the threshold, i.e., 0.1Hz, the random attack will be launch for compensation. This process is to guarantee the stealth of the attack. The entire process of the coordinated attack is shown in Fig. 3. The scale attack and ramp attack are firstly introduced by the attackers, and random attack acts as an adjustment to compensate for the deviation of the sudden frequency change. It is worth noting that the itineration of a stealthy attack causing UFLS damage must be bigger than three because the Rate of Change of Frequency (RoCoF) is not allowed to exceed 0.3Hz/15s. If so, the detection system of AGC will raise the alarm. The attack model coordination is elaborated by a 3-area system in this paper. However, the procedure and basic principle hold for a more complicated system, and the attack model combination can be numerous.

C. SIMULATION RESULTS

The coordinated attack, as well as the three different single attacks, are simulated and compared in a 3-area system. Among the three single attacks, we use the pulse attack instead of the random attack, which requires a long time to take effect. In all four scenarios, the power system will act as soon as the system frequency is under 59Hz. We mainly focus on the TTE value and the attack parameters (i.e., λ_s, λ_r, λ_p) in each scenario. The system parameters and tie-line power flows were stated in Table 1 and Table 2.

Scenario 1: A scale attack with a scaling factor of 0.25 is applied to tie-line 1-2, and the magnitude of the attacking vector is shown in Fig. 4(a). After the AGC control, the three tie-line power flow will deviate from its scheduled values, as shown in Fig. 4(b). Fig. 4(c) shows that after about 63.2s, the frequency of area 1 descends to 59Hz.

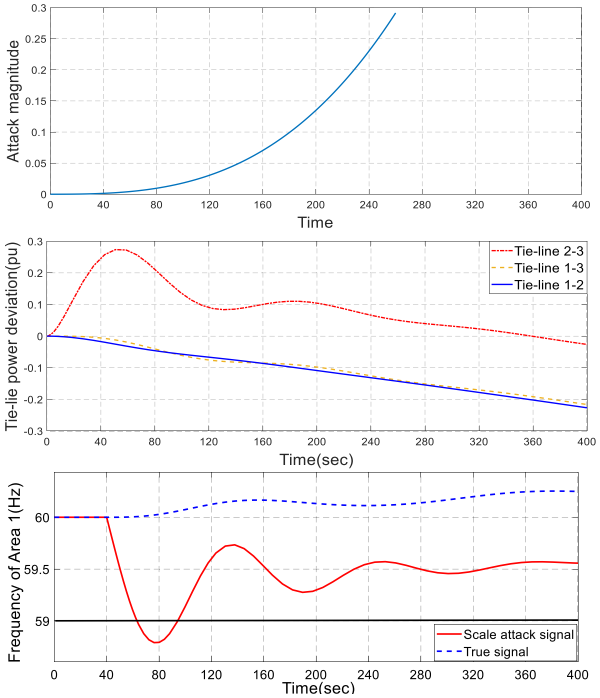


FIGURE 4. The effects of scale attack. (a) Scale attack with a scaling factor 0.25. (b) Tie-line power deviation. (c) Frequency of area 1.

Scenario 2: A ramp attack with a ramping factor of 0.07 is applied to the tie-line 1-2, and the magnitude of the attacking vector is shown in Fig. 5(a). Fig. 5(c) shows that after about 101.9s, the frequency of area 1 descends to 59Hz. The TTE value of a ramp attack with $\lambda_r = 0.07$ is much bigger than the TTE value of a scale attack with $\lambda_s = 0.25$. The reason behind this is that the injected false data of the ramp attack is increasing gradually with time, so it takes a much longer time to make an impact. It is worth noting that both the scaling factor and ramping factor are chosen carefully so that they match with each other in their own ranges.

Scenario 3: A pulse attack with a magnitude of 0.8 is applied to the tie-line 1-2, and the attacking period is from 0-15 seconds. The TTE value of the pulse attack is 12.4s, which is less than three cycles. Therefore, the detection system will raise the alarm.

Scenario 4: In this scenario, a coordinated attack is conducted. Specifically, a scale attack with $\lambda_s = 0.3$ is inflicted upon the tie-line 1-2 power measurement, and a ramp attack

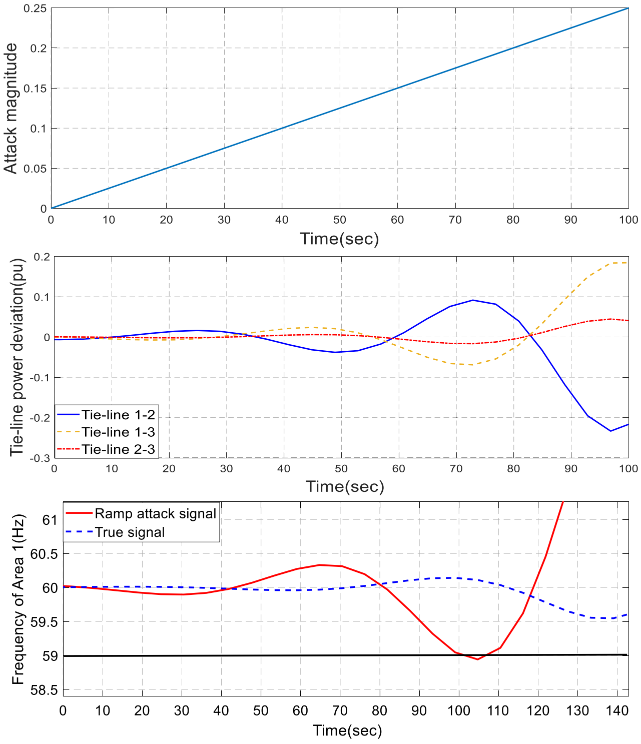


FIGURE 5. The effects of ramp attack. (a) Ramp attack with a ramping factor 0.07. (b) Tie-line power deviation. (c) Frequency of area 1.

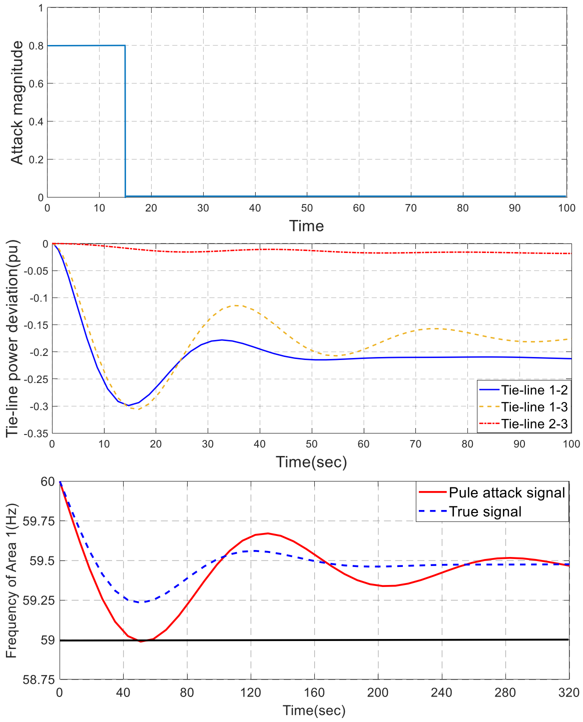


FIGURE 6. The effects of pulse attack. (a) Pulse attack with a magnitude of 0.8. (b) Tie-line power deviation. (c) Frequency of area 1.

with $\lambda_r = 0.1$ is inflicted upon the tie-line 1-3 power measurement. Besides, in order to keep the instant frequency deviation below 0.1Hz, a pulse attack with $\lambda_p = -0.04$ is conducted as an adjustment. Fig. 7(a) shows that after about 17.9s, the frequency will drop to 59Hz. Thus the UFLS will be initiated.

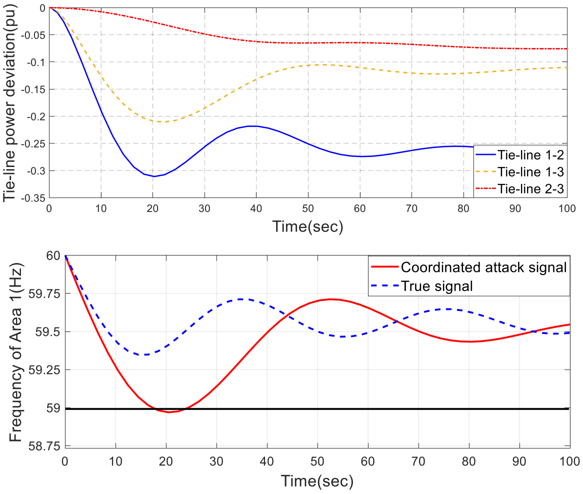


FIGURE 7. The effects of a coordinated attack. (a) Tie-line power deviation. (b) Frequency of area 1.

TABLE 3. The comparison of single attack and coordinated attack.

Attack types	parameters	Lower boundary	Upper boundary	Least TTE
Single attack	λ_s	0.1581	0.2922	10 cycles
	λ_r	0.0477	0.0824	17 cycles
Coordinated attack	λ_s	0.0225	0.4220	3 cycles
	λ_r	0.0130	0.1717	

Table 3 compares the parameter ranges and the least TTE of each attack, from which we can draw the conclusion that the coordinated false data injection attack not only shortens the TTE but also widen the range of the attack parameters. For example, in scenario 4, λ_s is set to 0.3, which is beyond the upper boundary of the scaling factor value for a single scale attack, but it is viable for a coordinated attack. This is the case for λ_r as well (which is set to 0.1 in scenario 4, and its upper boundary is 0.0824 for single ramp attack), providing the adjusting frequency attack is well designed to keep the instant frequency change below the threshold. It can also be seen from Table 3 that the least TTE value of the coordinated attack (only three cycles) is much shorter than the single attacks.

V. THE COUNTERMEASURE

From the analysis of coordinated attack, we can see that the coordinated attack is a combination of various single attacks. Therefore, it is difficult or even impossible to verify every single measurement fed into the AGC system, and even the system has this computational power, the outcome may well be incorrect because the adjusting attack keeps the checking points within its boundaries. A better way to investigate this problem is to analyze the pattern of the Area

Control Error (ACE) because it is the ultimate output of all the available measurements in the AGC system.

The expression of ACE is depicted in formula (7), from which it can be seen that ACE is linear to frequency deviation ($\Delta\omega_i$) and tie-line power flow (ΔP_{ij}). The parameter B_i is the frequency bias factor that determines the reciprocity of the two connected areas during the disturbance, and it is constant for a long period of time. Therefore, no matter how many measurements are falsified, the ACEs still follow a certain modification trend because of the linearity. For example, if a scale attack is inflicted upon the tie-line power flow, the pattern of ACE is just translational displaced, and the shape of it remains the same. However, for a coordinated attack, the attacked ACE pattern may change significantly because of the combination of multiple single attacks, and because of the uncertainty of the combination, many patterns need to be considered.

A. ATTACKED ACE PATTERN RECOGNITION

Pattern recognition is concerned with the automatic discovery of regularities to classify the data into different categories or differentiate individual behaviors. The basic idea is to find a function $y(x)$, which is determined by training, to decide which category of the new input belongs to. Here we use linear models for classification. For generative approach, we model the class-conditional densities $p(x|C_k)$ and class priors $p(C_k)$. The posterior probabilities $p(C_k|x)$ can be obtained using Bayes' Theorem, which is

$$\begin{aligned} p(C_1|x) &= \frac{p(x|C_1)p(C_1)}{p(x|C_1)p(C_1)+p(x|C_2)p(C_2)} \\ &= \frac{1}{1+\exp(-a)} = \sigma(a) \end{aligned} \tag{21}$$

where $a = \ln\frac{p(x|C_1)p(C_1)}{p(x|C_2)p(C_2)}$ and $\sigma(a)$ is the *logistic sigmoid* function.

For the case of $K > 2$, the posterior probabilities $p(C_k|x)$ can be written as

$$\begin{aligned} p(C_k|x) &= \frac{p(x|C_k)p(C_k)}{\sum_i p(x|C_k)p(C_i)} \\ &= \frac{\exp(-a)}{\sum_i \exp(a_i)} \end{aligned} \tag{22}$$

where $a_k = \ln p(x|C_k)p(C_k)$. $p(C_k|x)$ is also known as the *normalized exponential* and can be regarded as a multiclass generalization. Normally, the training data only comprises a small fraction of all possible inputs. Thus it is vital for the recognition model to identify every new input correctly. Generalization signifies the ability of a pattern recognition algorithm to correctly categorize new inputs that differ from the training set and is a key feature for the pattern recognition algorithm to be precise. The normalized exponential is also known as *softmax function* as it represents a smoothed version of the "max" function because, if $a_k \gg a_i$ for all $i \neq k$, then $p(C_k|x) \simeq 1$, and $p(C_i|x) \simeq 0$.

For simplicity, we consider a case of two Gaussian distributed classes with the same covariance matrix. Thus, the density of C_k can be denoted as

$$p(x|C_k)=\frac{1}{(2\pi)^{D/2}}\frac{1}{|\Sigma|^{1/2}}\exp\left\{-\frac{1}{2}(x-\mu_k)^T\Sigma^{-1}(x-\mu_k)\right\} \tag{23}$$

The posterior probabilities of class 1 can be obtained,

$$p(C_1|x) = \sigma(w^T x + \omega_o) \tag{24}$$

where $w = \sum^{-1}(\mu_1 - \mu_2)$,

$$\omega_o = -\frac{1}{2}\mu_1^T \sum^{-1} \mu_1 + \frac{1}{2}\mu_2^T \sum^{-1} \mu_2 + \ln\frac{p(C_1)}{p(C_2)}.$$

Due to the common covariance matrix assumption, the quadratic terms in x from the exponents of the Gaussian densities have been eliminated. Therefore, the function becomes linear and logistic sigmoid.

For the general case of K classes with Gaussian distribution, we have $a_k(x) = w_k^T x + \omega_{k0}$, where $w_k = \sum^{-1}\mu_k$ and $\omega_{k0} = -\frac{1}{2}\mu_k^T \sum^{-1}\mu_k + \ln p(C_k)$.

The attacked ACE pattern recognition is essentially a supervised classification, for all the training samples are labeled with "normal ACE" or "attacked ACE," and what we need to do is to differentiate the two categories. This supervised pattern recognition is viable because the ACE data is available online, and we can add arbitrary coordinated attacks to the normal data to form the training data set.

It is worth noting that this probability approach for pattern recognition is empowered by the identifiability of the original data set. According to the actual needs of recognition, the combination of some parameters is selected as a feature vector. Therefore, the training process could be time-consuming. A better way to ensure real-time detection is "offline training, online detection," which means the detection model is obtained by offline training and updated every few hours. Other classification methods are also viable, such as deep learning-based data forgery detection [21], and RNN (Recurrent Neural Networks) [29].

It is straightforward to extract the features of single attacked ACEs. Fig. 8 and Fig. 9 shows scale attacked ACE pattern, and scale attacked plus ramp attacked ACE pattern, respectively. The real ACE dataset is download from the PJM company. We use two-years data set (which is about 1 million data records) for training and 1-month data set for testing for each ACE pattern. The attacked patterns are artificially made with different attack factors. From Fig. 9, we can see the attacked ACE follows a certain pattern, and the only difference is the translational displacement due to the attacking factor.

B. SIMULATION RESULTS

In this section, we use the IEEE 39-bus system to verify the pattern recognition method for coordinated attack identification proposed in Section V.A. The single-line diagram is shown in Fig. 10, and its specification can be found in [30]. This 39-bus system is a specific real 3-area system that we used in the previous sections. In Fig. 10, there are 3,

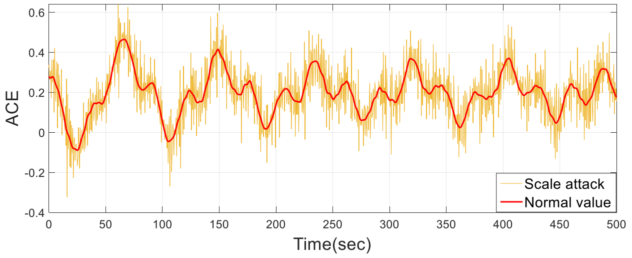


FIGURE 8. The ACE pattern of scale attack.

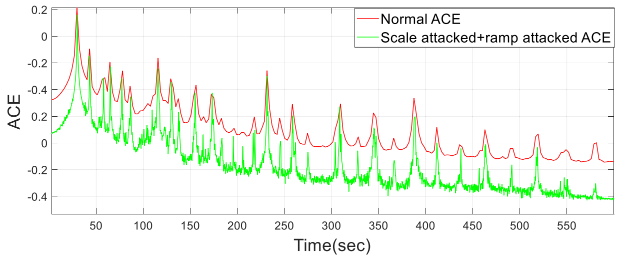


FIGURE 9. The ACE pattern of scale attack and ramp attack.

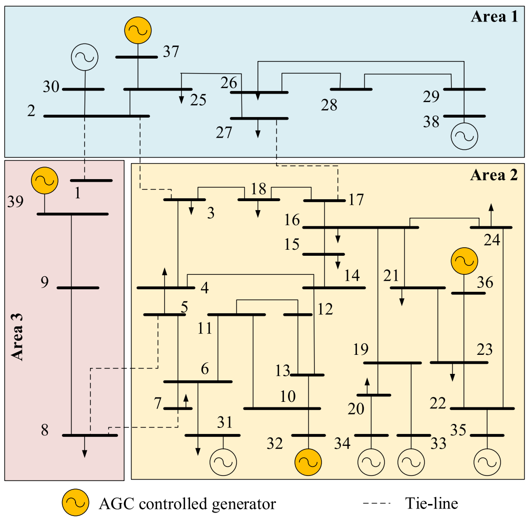


FIGURE 10. Single-line diagram of the IEEE 39-bus test system.

6, and 1 generator in Area 1, Area2, and Area3, respectively, and the generator controlled by AGC is marked by orange.

In the previous part of this section, we used real ACE data from PJM to form the attacked ACE and then find out its unique pattern. Here, although there is no real ACE data for the IEEE 39-bus system, we can fabricate the normal ACE data set resembled the real one. Without loss of generality, we add some fluctuation, which is Gaussian distributed, to the loads. Here, we consider the following scenarios to prove the effectiveness of the proposed method.

Scenario 1: A coordinated attack comprised of scale attack on tie-line 2-3, ramp attack on 5-8, and pulse attack on the frequency of Area 3.

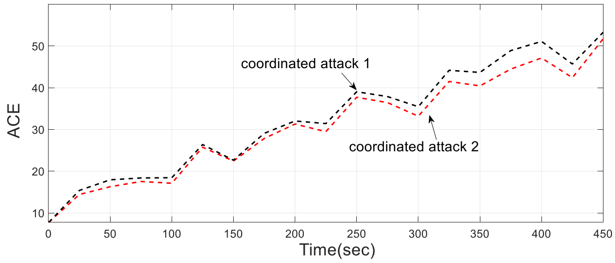


FIGURE 11. The attacked ACE pattern of Scenario 1.

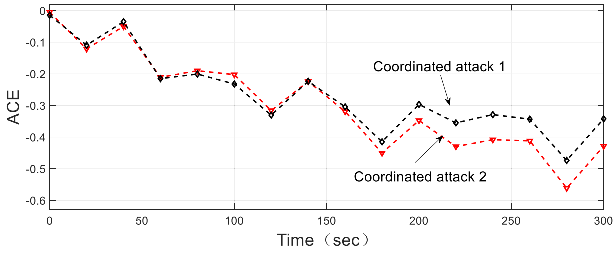


FIGURE 12. The attacked ACE pattern of Scenario 2.

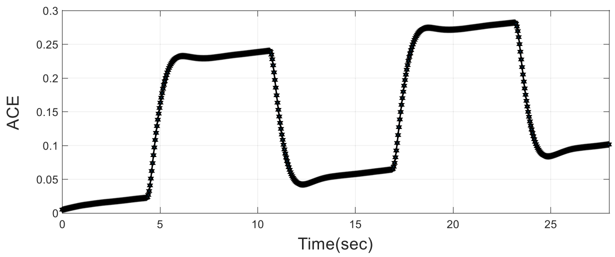


FIGURE 13. The attacked ACE pattern of Scenario 3.

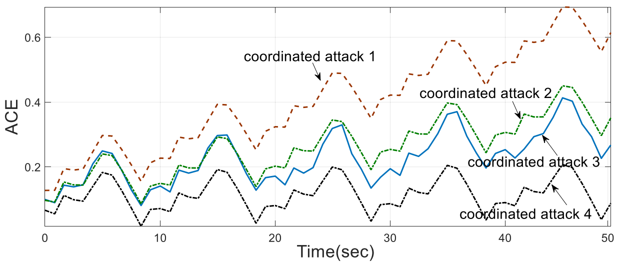


FIGURE 14. The attacked ACE pattern of Scenario 4.

Scenario 2: A coordinated attack comprised of scale attack on tie-line 17-27, ramp attack on 7-8, and pulse attack on the frequency of Area 3.

Scenario 3: A coordinated attack comprised of scale attack on tie-lines 1-2, 17-27, ramp attack on 7-8, 5-6, and pulse attack on the frequency of Area 2 and Area 3.

Scenario 4: A coordinated attack comprised of scale attack on all the tie-lines connecting Area1 and Area2, ramp attack on all the tie-lines connecting Area 2 and Area 3, and pulse attack on the frequency of all three areas.

For the first attack scenario, we illustrate the tendency of two coordinated attacks in *Scenario 1* by tilting the scale and ramp factor. In Fig. 11, it shows that the tendency is not a periodic one. However, it can be used to forecast future ACEs rather than a cycling pattern that can be used as a decisive approach to determine whether there is a coordinated attack or not. This forecast can be achieved by long-short memory networks (LSMN) or other commonly used forecast methods. Like *Scenario 1*, the tendency in *Scenario 2* is not an obvious repetitive one, though it may be found some pattern in the long-time window (however, that would be meaningless). Nevertheless, we can also use the LSMN to forecast the near future ACE value. From Fig. 11-12, we have proved that the ACE tendency of different coordinated attacks (due to parameter tilting) is consistent, and different ACE trajectory forms an ACE band.

The attacked ACE patterns for *Scenario 3* and *Scenario 4* are shown in Fig. 13 and Fig. 14, respectively. It shows that the ACE patterns are periodic, and the cyclic period in *Scenario 3* and *Scenario 4* is about 12s and 10s, respectively. Because the TTE value of a coordinated attack is quite small (3 AGC cycles), this cyclic period is ideal for identifying the malicious yet stealthy attack. In Fig. 14, we depict four different coordinated attacks by adjusting the attack parameters. All four attacks follow the same pattern. For practical usage, the operator can use the historic ACE data for training to form the pattern recognition function. Although this process is time-consuming, it can be done offline. Then the 2 or 3 cycles of newly input ACEs are used for the test. If the pattern of the newly input ACEs fits the pattern, it can be regarded as compromised. In this sense, this approach is quite fast and efficient because it only needs 10-15 seconds to identify the attack, and it has relatively high accuracy. The accuracy indexes are shown in Table 4.

However, the mechanism behind the cyclic or acyclic ACE pattern is unclear. From the four scenarios we have simulated, it can only be speculating that it has something to do with the scale of the coordinated attack itself, i.e., the more single attacks involved in a coordinated attack, the more likely the pattern would be cyclic (we can see the ACE pattern are cyclic in *Scenario 3* and *Scenario 4*). The correlation and rigorous poof will be investigated in our future work.

TABLE 4. Accuracy indexes from the last two scenarios.

	TP	FP	TN	FN
Scenario 3	97.6%	1.3%	98.7%	2.4%
Scenario 4	97.1%	1.6%	98.4%	2.9%

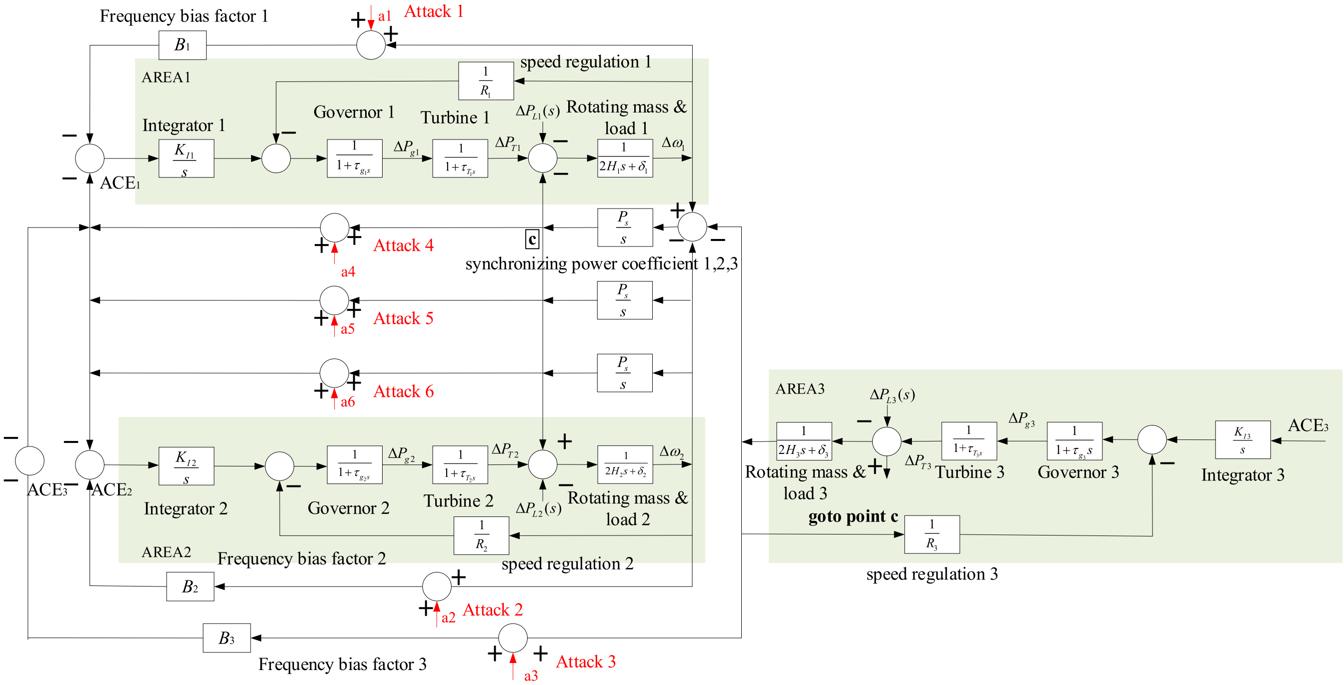
VI. CONCLUSION

This paper studied the coordinated FDI attack in the AGC system and proposed an artificial intelligence-based countermeasure. Through a 3-area AGC system study, we proved that the coordinated attack comprised of multiple single attacks could be more harmful and stealthier than the original one. The coordinated attack not only have much smaller TTE value (nearly ten times smaller), its attack parameters have much larger ranges. According to the characteristic of the coordinated attack, we proposed a detection method based on pattern recognition. Different from other detection methods that mostly rely on the load forecast or state estimation, the proposed approach is suitable to tackle this complicated attack. Through the IEEE 39-bus system test system, we proved that this method is effective and efficient.

.

APPENDIX A

The control block diagram of the 3-area system



APPENDIX B

Itineration of the scale attack process

Itineration	Injected data	ΔF	ACE
1	$(1+\lambda_s) * z(t)$	$\frac{-(1+\lambda_s)z(t)}{\sum_{i=1}^{n}(\frac{1}{R_i}+D_i)}$	$\sum_{j\in\delta}\left[(1+\lambda_s)z(t)\right]+\beta_i\cdot 2\pi\frac{-(1+\lambda_s)z(t)}{\sum_{i=1}^{n}(\frac{1}{R_i}+D_i)}$
2	$(1+\lambda_s)^2 * z(t)$	$\frac{-(1+\lambda_s)^2 z(t)}{\sum_{i=1}^{n}(\frac{1}{R_i}+D_i)}$	$\sum_{j\in\delta}\left[(1+\lambda_s)^2 z(t)\right]+\beta_i\cdot 2\pi\frac{-(1+\lambda_s)^2 z(t)}{\sum_{i=1}^{n}(\frac{1}{R_i}+D_i)}$
⋮	⋮	⋮	⋮
k	$(1+\lambda_s)^k * z(t)$	$\frac{-(1+\lambda_s)^k z(t)}{\sum_{i=1}^{n}(\frac{1}{R_i}+D_i)}$	$\sum_{j\in\delta}\left[(1+\lambda_s)^k z(t)\right]+\beta_i\cdot 2\pi\frac{-(1+\lambda_s)^k z(t)}{\sum_{i=1}^{n}(\frac{1}{R_i}+D_i)}$

REFERENCES

[1] Y. Arya and N. Kumar, "AGC of a multi-area multi-source hydrothermal power system interconnected via AC/DC parallel links under deregulated environment," *Int. J. Electr. Power Energy Syst.*, vol. 75, pp. 127–138, Feb. 2016.

[2] X. Zhao, Z. Lin, B. Fu, L. He, and C. Li, "Research on the predictive optimal PID plus second order derivative method for AGC of power system with high penetration of photovoltaic and wind power," *J. Electr. Eng. Technol.*, vol. 14, no. 3, pp. 1075–1086, May 2019.

[3] C. Tu, X. He, Z. Shuai, and F. Jiang, "Big data issues in smart grid—A review," *Renew. Sustain. Energy Rev.*, vol. 79, pp. 1099–1107, Nov. 2017.

[4] S. Aziz, H. Wang, Y. Liu, J. Peng, and H. Jiang, "Variable universe fuzzy logic-based hybrid LFC control with real-time implementation," *IEEE Access*, vol. 7, pp. 25535–25546, 2019.

[5] H. Wang, Z. Lei, X. Zhang, J. Peng, and H. Jiang, "Multiobjective reinforcement learning-based intelligent approach for optimization of activation rules in automatic generation control," *IEEE Access*, vol. 7, pp. 17480–17492, 2019.

[6] Y. Arya, "Effect of energy storage systems on automatic generation control of interconnected traditional and restructured energy systems," *Int. J. Energy Res.*, vol. 43, no. 12, pp. 6475–6493, Oct. 2019.

[7] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1–33, May 2011.

[8] G. Clarke, D. Reynders, and E. Wright, *Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems*. Oxford, U.K.: Newnes, 2004.

[9] H. Yoo and T. Shon, "Challenges and research directions for heterogeneous cyber–physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture," *Future Gener. Comput. Syst.*, vol. 61, pp. 128–136, Aug. 2016.

[10] M. J. Rice, "Secure ICCP final report," Pacific Northwest National Lab., Richland, WA, USA, Tech. Rep. PNNL-26729, 2017.

[11] K. Pan, E. Rakhshani, and P. Palensky, "False data injection attacks on hybrid AC/HVDC interconnected systems with virtual inertia–vulnerability, impact and detection," *IEEE Access*, vol. 8, pp. 141932–141945, 2020.

[12] C. Tu, X. He, X. Liu, Z. Shuai, and L. Yu, "Resilient and fast state estimation for energy Internet: A data-based approach," *IEEE Trans. Ind. Informat.*, vol. 15, no. 5, pp. 2969–2979, May 2019.

[13] W. Bi, C. Chen, and K. Zhang, "Optimal strategy of attack-defense interaction over load frequency control considering incomplete information," *IEEE Access*, vol. 7, pp. 75342–75349, 2019.

[14] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[15] 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, Mar. 2014.

[16] R. Tan, H. H. Nguyen, E. Y. S. Foo, X. Dong, D. K. Y. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "Optimal false data injection attack against automatic generation control in power grids," in *Proc. ACM/IEEE 7th Int. Conf. Cyber-Phys. Syst. (ICCPS)*, Apr. 2016, pp. 1–10.

[17] R. Tan, H. H. Nguyen, E. Y. S. Foo, D. K. Y. 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 Security*, vol. 12, no. 7, pp. 1609–1624, Jul. 2017.

[18] G. Wu, J. Sun, and J. Chen, "Optimal data injection attacks in cyber-physical systems," *IEEE Trans. Cybern.*, vol. 48, no. 12, pp. 3302–3312, Dec. 2018.

[19] A. Anwar and A. N. Mahmood, "Stealthy and blind false injection attacks on SCADA EMS in the presence of gross errors," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2016, pp. 1–5.

[20] 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, Sep. 2018.

[21] F. Zhang and Q. Li, "Deep learning-based data forgery detection in automatic generation control," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2017, pp. 400–404.

[22] S. Ahmed, Y. Lee, S.-H. Hyun, and I. Koo, "Feature selection–based detection of covert cyber deception assaults in smart grid communications networks using machine learning," *IEEE Access*, vol. 6, pp. 27518–27529, 2018.

[23] I. Saboya, E. Lobato, I. Egido, and L. Sigrist, "Machine learning based algorithms to dispatch multiple rapid-start units in AGC of power systems," *Int. J. Electr. Power Energy Syst.*, vol. 115, Feb. 2020, Art. no. 105412.

[24] S. D. Roy and S. Debbarma, "Detection and mitigation of cyber-attacks on AGC systems of low inertia power grid," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2023–2031, Jun. 2020.

[25] A. Ashok, S. Sridhar, A. D. McKinnon, P. Wang, and M. Govindarasu, "Testbed-based performance evaluation of attack resilient control for AGC," in *Proc. Resilience Week (RWS)*, Aug. 2016, pp. 125–129.

[26] I. A. Oyewumi, A. A. Jillepalli, P. Richardson, M. Ashrafuzzaman, B. K. Johnson, Y. Chakhchoukh, M. A. Haney, F. T. Sheldon, and D. C. de Leon, "ISAAC: The idaho CPS smart grid cybersecurity testbed," in *Proc. IEEE Texas Power Energy Conf. (TPEC)*, Feb. 2019, pp. 1–6.

[27] M. McDonald, GCT Service, and R. Cassidy, "Cyber effects analysis using VCSE, promoting control system reliability," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2008-5954, 2008.

[28] D. C. Bergman, "The virtual power system testbed and inter-testbed integration," in *Proc. CSET*, Montreal, QC, Canada, 2009.

[29] A. Ayad, M. Khalaf, and E. El-Saadany, "Detection of false data injection attacks in automatic generation control systems considering system nonlinearities," in *Proc. IEEE Electr. Power Energy Conf. (EPEC)*, Oct. 2018, pp. 1–6.

[30] M. Cupelli, C. Doig Cardet, and A. Monti, "Voltage stability indices comparison on the IEEE-39 bus system using RTDS," in *Proc. IEEE Int. Conf. Power Syst. Technol. (POWERCON)*, Oct. 2012, pp. 1–6.

XI HE (Member, IEEE) received the B.S. degree in electrical engineering and automation from Beijing Jiaotong University, Beijing, China, in 2009, the M.S. degree in software engineering from Zhejiang University, in 2011, and the Ph.D. degree in electric engineering from Hunan University, in 2019. He was with Hangzhou Hikvision Digital Technology Company Ltd., and Schneider Electric. He is currently a Lecturer with the Hunan Institute of Technology, Hengyang, Hunan. His research interests include cyber security in power grid, synchrophasor measurement, and distribution grid automation.

XUAN LIU (Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Sichuan University, China, in 2008 and 2011, respectively, and the Ph.D. degree in electrical engineering from the Illinois Institute of Technology (IIT), Chicago, in 2015. He is currently a Professor with the College of Electrical and Information Engineering, Hunan University, China. His research interests include smart grid security and operation and economics of power systems.

PENG LI received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from the South China University of Technology, Guangzhou, China, in 1993, 1995, and 2002, respectively, and the Ph.D. degree in electrical engineering from the Technical University of Braunschweig, Braunschweig, Germany, in 2004. He is currently a Professor of engineering with the Digital Grid Research Institute, China Southern Power Grid, Guangzhou, China. His research interests include microgrids, renewable energy, and data security.