Advanced algorithm to detect stealthy cyber attacks on automatic generation control in smart grid

Fatemeh Akbarian1,2, Amin Ramezani1, Mohammad-Taghi Hamidi-Beheshti1, Vahid Haghighat3

1Department of Electrical and Computer Engineering, Tarbiat Modares University, Tehran, Iran
2Department of Electrical and Information Technology, Lund University, Lund, Sweden
3Department of Electrical and Computer Engineering, Shahid Beheshti University, Tehran, Iran
E-mail: ramezani@modares.ac.ir

Abstract: One of the basic requirements of today's sophisticated world is the availability of electrical energy, and neglect of this matter may have irreversible damages such as an extensive blackout. The problems which were introduced about the traditional power grid, and also, the growing advances in smart technologies make the traditional power grid go towards smart power grid. Although widespread utilisation of telecommunication networks in smart power grid enhances the efficiency of the system, it will create a critical platform for cyber attacks and penetration into the system. Automatic generation control (AGC) is a fundamental control system in the power grid, and it is responsible for controlling the frequency of the grid. An attack on the data transmitted through the telecommunications link from the sensors to the AGC will cause frequency deviation, resulting in disconnection of the load, generators and ultimately global blackout. In this study, by using a Kalman filter and a proposed detector, a solution has been presented to detect the attack before it can affect the system. Contrary to existing methods, this method is able to detect attacks that are stealthy from the area control error signal and χ2-detector. Simulations confirm the effectiveness of this method.

1 Introduction

Power grid is one of the vital infrastructures of each community, so occurrence of any problems for it can have catastrophic consequences. According to the advent of new technology and the expansion of telecommunication networks, smart power grid was introduced in response to encountered problems in traditional power grid. Smart grid transmits a lot of information through electric lines or wireless communication networks and controls the power system automatically by collecting these data and using decision-making software. The expansion of telecommunication networks in smart grid makes it a cyber-physical system. Although this increases the efficiency of the system, it will jeopardise the system's security at the same time because communication links can provide a critical platform for cyber attacks and infiltration of attackers into the system. In recent years, in some cyber-physical systems which, similar to smart power grid, have been created of cyber technology and physical processes, some kind of cyber attacks and problems have been occurred such as attack on the Ohio Nuclear Power Plant by Slammer worm [1], Stuxnet computer worm attacks on Iran's nuclear installation [2], numerous blackouts in recent years in Brazil [3] and so on. Such problems indicate that conducting research and providing appropriate solutions for preserving the cybersecurity of smart power grid is very important. One of the main parts of the power grid is automatic generation control (AGC) whose main task is controlling frequency of grid in its nominal value. In terms of cyber security, AGC can be very attractive to attackers because of two reasons. First, the data which are sent or received by AGC should be transmitted through telecommunication lines, so this can cause these data to be accessible by attackers. Second, occurring attack on data which are sent from sensors to AGC and manipulating them causes the frequency of grid to deviate from its nominal value. Since imbalance between power generation and consumption in power grid will lead to the deviation of the frequency from its nominal value. AGC maintains the frequency by adjusting the output power of the generators based on the measurements collected from the sensors distributed in the grid. This frequency deviation caused by attackers will trigger unplanned actions such as load shedding, disconnection of customers and interruptions of generators that finally will result in extensive blackout and damage to equipment. Hence, timely detection of attacks on AGC is crucial.
In the field of cybersecurity in various parts of the smart power grid, some studies have been done. For example, Ao et al. [4] have proposed adaptive sliding mode observer (ASMO) for detecting cyber attacks in power system and recovery of the system. In this paper, first, for investigating detectability of attacks some sufficient conditions are established. Then two ASMOs for detecting state and sensor attacks are designed. Ultimately, performance of this method has been validated on the IEEE 39-bus system [5], power grid is considered as a distributed system with wide area measurement system. Distributed model predictive control has been proposed to control this system in the presence of time-varying data injection attacks that describe delayed input states. Also, this paper has demonstrated the stability of closed-loop system with the designed controllers by using Lyapunov theorem and linear matrix inequality. In practice, cyber attacks also may appear in power systems where transducers are used in setting the reference. In this case, the system may inherently encounter derivative inputs that are resolved based on algebraic approach [6]. In [7], power system has been modelled as a linear time-invariant system by using the Swing equation. Authors have proposed a robust defence scheme to cope with cyber attacks whose goal is to destabilising the system. In this method, the protected dynamic of the system will be decoupled from the dynamics of the subsystem targeted by the attack. In [8], cyber attack detection and identification are not necessarily done using the typical state estimation and it is avoided by model-based fault detection and isolation. Li et al. [9] have investigated the feasibility and limitations of using the distributed flexible AC transmission system (D-FACTS) devices, termed as proactive false data detection (PFDD) approach to detect three types of false data injection (FDI) attacks namely single-bus, uncoordinated multiple-bus and coordinated multiple-bus FDI attacks on smart grids. Beibei et al. proved that PFDD can detect all these three types of FDI attacks if and only if the deployment of D-FACTS devices covers branches containing at least a spanning tree of the grid graph. In [10], an algorithm for detecting and mitigating cyber attacks has been proposed. In this algorithm, by sensing network delays, probability density function (PDF) of this array of delays in each time is obtained. If the difference between this PDF in each time and previous time becomes more than a threshold, a fault can be detected. Meanwhile, if there is no abnormal behaviour in observer in the system, it can corroborate that cyber network fault has happened, and it is not a physical fault. Afterwards, by predicting and evaluating performance of the system in the presence of this cyber fault, it can be determined that it is a hard or soft fault. If a hard fault is detected, a resilience controller will be triggered. Otherwise, adverse effects on the system performance can be handled by the existing controller in the system. Some papers specifically studied cybersecurity in AGC. For example, in [11], a method has been proposed for detecting malicious attacks on AGC by scanning the real-time area control error (ACE) data. This method by utilising load forecasted data tries to predict a range of ACE, mean of ACE and summation of ACE and then in three stages tries to detect attacks. Li et al. [12], by the combination of the deep learning algorithm and the extreme learning machine algorithm, propose a defence method against denial of service (DOS) attack on the load frequency control system. In this paper, DOS attack causes dropping measurement data which is sent to the control centre. In this situation, the control centre can quickly predict the loss data based on historical data in the real-time database and use them for generating control signals. In [13], an attack impact assessment approach including stability and safety assessment for AGC has been suggested. In the system, if the total delay in transmitting sensor measurements and control commands exceeds a threshold, the assessment of the power system will be launched. First, the stability of AGC, which depends on delay and total loads in the power system, is investigated. If the system is unstable, the mitigation part will be initiated; otherwise, the safety of the system, which depends on load distribution, will be checked, and if the system is classified unsafe, the mitigation process will be initiated. In [14], an attack detection algorithm is designed based on load prediction. AGC performance is predicted in each work cycle by using the predicted load, and associated ACE is generated. Then, the actual AGC performance obtains based on the measurements, and the ACE generated on the base of them are compared with the predicted one. If the difference is greater than a predetermined amount, the attack will be detected. Although the algorithm presented in this paper has high efficiency, the need to predict load for its implementation will increase computations and complexity. In [15], designing an optimal attack in such a way that can cause deviation of the frequency more than the acceptable range in the shortest possible time is investigated. Furthermore, the system's information that the attacker needs to launch such attacks, and how to get this information has been reviewed. Also, in this paper, a model-based method to detect this kind of attack has been proposed. However, one of the weak points of this paper is that the range that should be considered for the ACE signal is not considered and it is not discussed in this paper.

In our prior work [16], we employed an algorithm to detect and estimate cyber attacks on smart grid. We modelled the power system as a linear time-invariant system, and we considered attackers to manipulate voltage signals which are measured by sensors at each bus in the power system and sent to the control centre. Based on [16], we make the following novel contributions in this paper:

- We first illustrate the impact of some of the most common integrity attacks on AGC on the frequency of the power system.
- We demonstrate some kinds of attacks on AGC are stealthy and conventional methods are not able to detect them.
- We develop an algorithm for timely detection of attacks on AGC before attacks can affect the system and cause damages. Also, we demonstrate our scheme is able to detect the attacks on this system which are stealthy from conventional methods’ perspective.
- We propose a new detector.
- We evaluate the detection capability of the proposed anomaly detection algorithm through simulation studies.

In the following, first, we express the characteristics of AGC system and frequency control in the power system, and we try to obtain the model of this system. In the next section, the models of some types of cyber attacks, how they affect the system and stealthy attacks are investigated. Finally, our proposed algorithm and detector is explained, and its performance for detecting the attacks that are not detectable by conventional methods is evaluated. Nomenclature summarises the parameters and notations used in this paper.

2 Frequency control in power system

To the satisfactory function of a power system, it is necessary to maintain the frequency almost constant. The power system’s frequency depends on active power balance, and the Imbalance between consumption power and generating power leads to deviation of the frequency from its nominal value. Since frequency is a common factor throughout the system, any changes in the active power demand at a point will be reflected in the frequency variation throughout the system. Equation (1) shows the relation between frequency deviation and changing of power in the Laplace domain

\[
\Delta P_m(s) - \Delta P_f(s) = MSs\Delta\omega(s) + D\Delta\omega(s)
\]

where \(\Delta P_m\) is the mechanical power change, \(\Delta P_f\) is the change of load, \(\Delta\omega\) is the frequency deviation, \(M\) is the inertia constant and \(D\) is the load damping coefficient that is equal to percent change in load for a 1% change in frequency. To control the frequency of the power system, there are two primary and secondary control loops as shown briefly in Fig. 1.

In each generation unit, a governor is present as the primary controller. This governor usually consists of a PI controller, and by comparing the frequency measured by frequency sensors with the set-point, it produces the necessary control signal to adjust the valve of water or steam that enters the turbine. The secondary or complementary control system is AGC. In addition to frequency
control, it is also responsible for maintaining the power exchanges between the control areas in the power system at scheduled amounts [17].

Power exchanges between every two areas are accomplished through the transmission lines called tie-line. In fact, tie-line is a transmission line that connects two buses that belong to two different areas. These lines are indicated in Fig. 2 which shows a three-area power system. In this figure, \( \ell_{ij} \) demonstrates the tie-line between area \( i \) and \( j \).

On these lines, there are some sensors to measure power flow. By comparing this measured value with the scheduled value, deviation of exchanged power between area \( i \) and \( j \) is calculated as

\[
\Delta P_{ij} = P_{ij} - P_{ij, Sch}. 
\]

(2)

Furthermore, in each area the frequency is measured by sensors and frequency deviation is calculated as follows:

\[
\Delta \omega_i = \omega_i - \omega_{nom}. 
\]

(3)

Then both frequency deviation and deviation of the export power of each area are sent to the AGC that is located in the control centre. AGC by using these signals generates ACE signal as follows:

\[
ACE_i = \alpha_i \Delta P_{Ei} + \beta_i \Delta \omega_i 
\]

(4)

where \( \alpha \) and \( \beta \) are constant.

Fig. 3 shows an overview of the AGC function for the three-area power grid in Fig. 2. Since AGC is located at the control centre, data from sensors, including \( \Delta \omega \) and \( \Delta P_{E} \), are sent to AGC via telecommunication links. In this way, a critical opportunity will be provided for infiltration of an attacker into the system through these telecommunication lines. If the attacker can manipulate the data transmitted from the sensors to the control centre and change their value, this will result in wrong calculation of ACE signal by AGC. Consequently, the amount of generator's output power will be set up incorrectly and eventually lead to deviation of the grid's frequency.

As it was stated previously, frequency deviation indicates the degree of imbalance between load and generation power. The purpose of frequency control is to keep frequency constant at its nominal value, and it is desirable that the frequency deviation \( \Delta \omega \) is maintained at \( 0 \text{ Hz} \). However, in practice, the load is an instantaneous variable, and it is constantly changing. In fact, we can have an estimate of the load, and this estimate also is continuously changing. Therefore, it is very arduous to assess the exact load versus the exact total generation, particularly in the presence of losses from various sources. For these reasons, a permissible range is usually considered for frequency deviation. In this paper, the permissible range for frequency deviation, based on [15], is considered to be \([-0.5, 0.5]\text{ Hz}\).

Fig. 4 shows the frequency deviation of Area 1 in the normal operation mode of the system. The attacker's goal is to increase frequency deviation \( \Delta \omega \) as far as it exceeds the permissible range. After that, this frequency deviation which has been created by the attack will spread to the whole grid. The system which cannot distinguish this frequency deviation is not due to an imbalance between load and generation power, triggers corrective actions such as disconnecting generators or customer loads in order to eliminate this imbalance. As a result, these inappropriate actions lead to equipment damage and extensive blackout.

Since frequency is a global parameter in the power grid, any change in the frequency at any point of the grid will cause frequency deviation in the whole grid. Therefore, in this paper, just the frequency deviation of Area 1 has been investigated.
Cyber-physical systems, which are a combination of physical systems and telecommunication network, can be attacked by a variety of data which are sent through telecommunication links in the system. From security perspective, three essential features are defined for cyber-physical systems. These features include confidentiality, availability and integrity, which are briefly represented by ‘CIA’, and each of these features is invaded by a type of attacks. The confidentiality feature is related to hide sent data so that the message is only identifiable to authorized users. However, in disclosure attack, the attacker penetrates to the telecommunication network and eavesdrops on the sent message. Although this kind of attack does not have a devastating effect on the system, the enemy may use it to launch more complicated attacks. The availability feature means timely access of the unauthorised change between sent and received information, but in deception attack, the enemy manipulates the transmitted data and alters them [18].

According to the given explanations in the previous sections and as shown in Fig. 5, in the frequency control system in the power grid, some signals are sent through the telecommunication link, so there is the possibility of occurring cyber attacks on them. These signals are the ones that are sent from the sensors in different parts of the power grid to the AGC in the control centre such as ΔPE and Δω, or it can be the ACE signal generated by the AGC, which is sent from the control centre to generators.

In Fig. 5, y is the measurement signal which is sent from the sensors to the AGC and defined as follows:

\[
y = [\Delta PE \quad \Delta \omega]
\]

and \(u\) is the control signal sent from the control centre to the generators, and about the frequency control system, it is the ACE signal produced by the AGC. In this paper, it is assumed that a deception attack will occur on the ΔPE signal. To change the actual value of ΔPE, the attacker penetrates in the system through the telecommunication network as shown in Fig. 5 and adds the attack vector to the measurement signal in this manner

\[
y = y + \bar{a}, \quad \bar{a} = [a \quad 0]
\]

where \(\bar{y}\) is the manipulated measurement signal, \(\bar{a}\) is the attack vector and \(a\) is the factor which is added to ΔPE. As a result, the value of the ΔPE signal changes and then will be sent to the AGC.

### 3.1 Attack models

According to what \(a\) is and how it changes the ΔPE signal, various types of attacks can be designed. An attack will affect the power system if it causes frequency deviation to exceed the permissible range. In this paper, according to [14], three types of attacks including scaling attack, random attack and ramp attack are considered. In the following, \(z(t)\) and \(\tilde{z}(t)\), respectively, represent the actual signal before the attack and manipulated signal after the attack. In this paper, \(z(t)\) is equivalent to ΔPE signal. Furthermore, \(t\) and \(\tau\) indicate time and attack period, respectively.

#### 3.1.1 Scaling attack

In this type of attack, the measurement signal is manipulated and its value depending on the amount of scaling attack parameter \(\lambda_s\) is converted to a value greater or less than the actual value

\[
z'(t) = \begin{cases} 
z(t) & \text{for } t \notin \tau_a \\
(1 + \lambda_s) \cdot z(t) & \text{for } t \in \tau_a 
\end{cases}
\]

#### 3.1.2 Ramp attack

In this type of attack, since the beginning of the attack, \(\lambda_r \cdot t\) is added to the actual signal and depending on the amount of \(\lambda_r\), increases or decreases value of the signal

\[
z'(t) = \begin{cases} 
z(t) & \text{for } t \notin \tau_a \\
z(t) + \lambda_r \cdot t & \text{for } t \in \tau_a 
\end{cases}
\]

#### 3.1.3 Random attack

In this type of attack, since the beginning of the attack, random values are added to the signal periodically

\[
z'(t) = \begin{cases} 
z(t) & \text{for } t \notin \tau_a \\
z(t) + \text{rand}(a, b) & \text{for } t \in \tau_a 
\end{cases}
\]

and these random values are chosen between the values of \(a\) and \(b\).

The effects of these three types of attacks on the system’s frequency deviation are shown in the following. In Fig. 6, scaling attack with \(\lambda_s = 5\), ramp attack with \(\lambda_r = 0.01\) and random attack with \((a, b) = (1, 2)\) occur on the ΔPE signal at the 50th second.

### 3.2 Stealthy attack

In power systems, in addition to frequency deviation signal, a permissible range is also considered for ACE signal generated by the AGC, and overflowing this signal from this range will trigger an alarm in order to indicate the existence of a problem in the system [14]. Hence, an attack in order to be stealthy or undetected by the controller should be designed so that not only does it make frequency deviation to exceed allowed threshold, but also ACE signal remains in its permissible range during the attack. On the contrary, if an attack on the system causes excessive deviation of the frequency, but the ACE signal surpasses the allowed range during this attack, the alarm will be triggered, and the attack will be detected before it can affect the system. In this paper according
to [14], the permissible range for ACE is considered to be [−0.05, 0.05] pu.

Fig. 7 shows the attack signal, the frequency deviation signal and the ACE signal in the presence of a scaling attack with \( \lambda_s = 5 \) which is started at the 50th second. In this case, as soon as the attack begins, the attacker adds a coefficient of the \( \Delta PE \) signal to it. However, due to the fact that the value of the \( \Delta PE \) signal is close to zero, as shown in Fig. 7a, despite starting the attack at the 50th second, the attack remains in its permitted range and does not cross the thresholds. Therefore, no alarms will be triggered and this attack will remain hidden and will not be detected by the controller.

Fig. 8 shows the attack signal, the frequency deviation signal and the ACE signal in the presence of a random attack with \( (a, b) = (1, 2) \) begun at the 50th second. In this kind of attack, the attacker periodically adds a random value between 1 and 2 to the \( \Delta PE \) signal during the attack period. According to Fig. 8b, the attack immediately has led to the departure of the \( \Delta\omega \) from its allowed range. Also, according to Fig. 8c, which corresponds to the ACE signal, before the departure of the \( \Delta\omega \) from the allowed range, the ACE signal exceeds the thresholds defined for it. Although the time of attack occurrence, detection and the time in which attack can damage the system are close together, this attack cannot be stealthy and will be detected by the controller before it affects the system.

Fig. 9 shows the attack signal, the frequency deviation signal and the ACE signal in the presence of a ramp attack with \( \lambda_r = 0.01 \) which is begun at the 50th second. In this kind of attack, the attacker increases the \( \Delta PE \) signal by a gentle slope. According to Fig. 9b, the attack makes the \( \Delta\omega \) surpass its permissible range, and according to Fig. 9c, the ACE signal, in the presence of this attack, remains in its permitted range and does not cross the thresholds. Therefore, no alarms will be triggered and this attack will remain hidden and will not be detected by the controller.

According to these results, it can be seen that there are attacks that cannot be detected by using the ACE signal. Therefore, it is necessary to use an algorithm to detect these types of attacks on the AGC. In the next section, we will provide a solution to detect this kind of stealthy attack.

4 Attack detection

Regarding the presence of measurement noise and process noise in real systems, the AGC system can be considered as a stochastic system. Hence, in this paper, utilisation of Kalman filter is proposed for detecting stealthy attacks, because Kalman filter by optimal removal of the destructive effects of the attack and noises from the manipulated signal can estimate the actual signal, and then this estimated signal can be used to detect the occurrence of the attack. First, in order to implement this attack detection algorithm on the system, Fig. 3, which includes the three-area power grid and its related AGC system, is considered as the main system. Main purpose of AGC is controlling the frequency, and maintaining it at the nominal value. Also, frequency changes depend on the load variations in each area, so the frequency deviation \( \Delta\omega \) should be defined as the system's output: \( y \), and based on it, load changes \( \Delta p \) will be defined as the input of the system: \( u \).

In this system, in addition to the input signal represented by \( u(t) \), process noise, measurement noise and attack signal are entered into the system which are shown, respectively, with \( w(t) \), \( \nu(t) \) and \( \alpha(t) \). By designing the Kalman filter for this system, state variables are estimated, and then we can obtain an estimate of the system's output by using the model of the system. Afterwards, by comparing the estimated output with actual output, that is measured by sensors, a residual signal can be obtained. By entering this residual signal into a detector, the attack can be detected. To
implement this algorithm and design the Kalman filter, we need the state-space model of the system. For this purpose, by defining frequency deviation as output and load variations as inputs and based on the method presented in [19, 20], the system model is obtained as a system with three inputs and three outputs

$$\Delta W = \Phi^{-1} \Delta P$$  \hspace{1cm} (10)

where $\Delta W$ and $\Delta P$ are, respectively, the output and input vectors of the system with dimensions 3 x 1 which are defined as follows:

$$\Delta W = \begin{bmatrix} \Delta \omega_i \\ \Delta \omega_j \\ \Delta \omega_k \end{bmatrix} \quad \Delta P = \begin{bmatrix} \Delta P_i \\ \Delta P_j \\ \Delta P_k \end{bmatrix}$$  \hspace{1cm} (11)

$\Delta \omega_i$ and $\Delta P_i$ are, respectively, the frequency deviation and load change of the $i$th area of the power grid. Also, $\Phi^{-1}$ in (10) is transformation matrix of the system. Ultimately, by considering process noise and measurement noise as white noise with the covariances $\mathbf{Q}$ and $\mathbf{R}$, respectively, the observable state-space realisation of this model is obtained as the following form:

$$x(t) = Ax(t) + Bu(t) + Gw(t) \quad w(t) \rightarrow N(0, \mathbf{Q})$$
$$y(t) = Cx(t) + Fv(t) \quad v(t) \rightarrow N(0, \mathbf{R})$$  \hspace{1cm} (12)

Now by using this observable state-space model of the system, we can design a Kalman filter for it.

### 4.1 Kalman filter designing

Kalman filter designing consists of two parts: time update and measurement update [21]. Time update part consists of steps as follows:

1. \[ \hat{x}_{k-1} = A\hat{x}_{k-1} + B\mu_k \]  \hspace{1cm} (13)
2. \[ \mathbf{P}_{k-1} = G_{k-1} \mathbf{Q}_{k-1} G_{k-1}^T + A\hat{x}_{k-1} \Delta \mathbf{F}_{k-1} \]  \hspace{1cm} (14)

and measurement update part consists of steps as follows:

3. \[ \mathbf{K}_k = \mathbf{P}_{k-1} C^T (C_{k} \mathbf{P}_{k-1} C^T + I)^{-1} \]  \hspace{1cm} (15)
4. \[ \hat{x}_k = \hat{x}_{k-1} + K_k (y_k - C_{k} \hat{x}_{k-1}) \]  \hspace{1cm} (16)
5. \[ \mathbf{P}_k = (I - K_k C_{k}) \mathbf{P}_{k-1} \]  \hspace{1cm} (17)

where $\hat{x}$ is the estimated state variable, $\mathbf{P}_k$ is the estimating covariance matrix, $\mathbf{Q}_k$ is the covariance matrix of the process noise, $\mathbf{R}_k$ is the covariance matrix of the measurement noise and $\mathbf{K}_k$ is the Kalman gain. In this paper, we consider $\mathbf{Q}_k$ as a diagonal matrix with $5 \times 10^{-6}$ on the diagonals, and $\mathbf{R}_k$ as a diagonal matrix with the $1 \times 10^{-3}$ on the diagonals. Then, by considering the initial value $I$ for the $\mathbf{P}$, where $I$ is the identity matrix, we can obtain Kalman gain and design a Kalman filter for our system. Using this Kalman filter, state variables of the system are estimated. The system's output can also be estimated based on these state variables and using the system model as follows:

$$\hat{y}(t) = C\hat{x}(t)$$  \hspace{1cm} (18)

Now by comparing this estimated signal $\hat{y}(t)$ with the actual signal $y(t)$ which is transmitted from sensors to the central controller, the residual signal is generated

$$r(t) = y(t) - \hat{y}(t)$$  \hspace{1cm} (19)

In fact, we can say this residual signal is an estimation of anything that has been added to the actual signal that could be noises or attacks.

---

**Fig. 10** Detection of stealthy ramp attack by using $\chi^2$-detector in attack detection algorithm

(a) Attack signal, (b) Frequency deviation, (c) $g(t)$ generated by $\chi^2$-detector

### 4.2 Detector

In order to distinguish attacks from noises and detect the occurrence of an attack, it is necessary to use a detector. $\chi^2$-detector is the conventional detector which is usually used with Kalman filter to detect faults in the system. In this paper, the performance of this detector for detecting attacks on the AGC is evaluated, and then, given its results and the weaknesses of this detector for this purpose, another detector is proposed to be embedded in this attack detection algorithm.

#### 4.2.1 $\chi^2$-detector

As described in [22], this detector by using the residual signal and its covariance matrix generates the signal called $g(t)$ as follows:

$$g(t) = r(t)^T \mathbf{B}(t) r(t)$$  \hspace{1cm} (20)

where $\mathbf{B}(t)$ is the covariance matrix of the residual signal. This detector by comparing $g(t)$ with a predetermined threshold, try to detect attacks. If the hypothesis $H_0$ indicates the normal operation of the system and $H_1$ indicates the abnormal mode of the system, the basis of this detector is as follows:

$$H_0: \text{if} \ g(t) \leq \text{threshold}$$
$$H_1: \text{if} \ g(t) > \text{threshold}$$  \hspace{1cm} (21)

In fact, since the Kalman filter cannot distinguish the changes caused by the attack from the changes due to the presence of noise, a threshold for filtering the effects of noises and preventing false alarms should be considered. Based on 68-95-99.7 rule, in a Gaussian distribution, 68.27, 95.45 and 99.73% of the values lie within one, two and three standard deviations of the mean, respectively [23]. Since the noises in this paper are assumed Gaussian noise with zero mean, by considering a threshold equal to $3\sigma$ that $\sigma$ is the standard deviation of measurement noise, 99.73% false alarms that may occur due to these noises can be filtered. Fig. 10 shows the result of the implementation of the attack detection algorithm using the $\chi^2$-detector for the ramp attack shown in Fig. 9. As shown earlier, regarding the description of Section 3.2, this attack is stealthy and cannot be detected by the ACE signal.

According to Fig. 10, it is obvious that in the presence of ramp attack, $g(t)$ generated by the $\chi^2$-detector always remains below the threshold, and thus, this detector is not able to detect this kind of attack. If $g(t)$ is simulated in this condition in a longer period of time, Fig. 11 will be obtained.
According to Fig. 11, it is seen that \( g(t) \) has increased due to the attack, but its speed is very slow, and it takes a long time to rise above the threshold. Therefore, this detector cannot detect this kind of attack.

### 4.2.2 Proposed detector

According to the previous sections, it was found that the ramp attack could not be detected by the ACE signal and the \( x^2 \)-detector. Hence, in this paper, we propose a detector which uses residual signal and generates \( h(t) \) so as to detect attacks as follows:

\[
h(t) = \sup_{t - \tau < t < t + \tau} |r(t)| \cdot \begin{cases} H_2; & h(t) \leq \text{threshold} \\ H_1; & h(t) > \text{threshold} \end{cases}
\]

This detector in each time \( t \) calculates the infinity norm of the residual signal in the period \( \tau \) before that time. Considering the supremum of the difference between the actual output signal and the estimated output signal at each time interval \( \tau \) can cause the fact that the signal \( h(t) \) rises above the threshold timely and faster than the \( x^2 \)-detector. Also, it decreases false warnings due to noise. Fig. 12 shows the attack signal, the system's output and the output of the proposed detector in the presence of the stealthy ramp attack shown in Figs. 9 and 10.

As can be seen, our proposed detection algorithm by using this detector is able to detect the ramp attack before the frequency deviation can surpass the allowed range, and much earlier than the attack can cause damages to the system. Therefore, the efficiency of this algorithm using this detector for detecting this kind of attack on AGC system is confirmed.

In Table 1, to verify the efficiency of the proposed algorithm as well as the proposed detector, numerous experiments have been conducted on the system via applying various ramp attacks by taking into account different \( \lambda_r \). In this table, No. represents the test number, \( t_i \) represents the starting time of the attack, \( t_d \) represents the time of attack detection by using the presented method in this paper and \( t_s \) represents the time when the triggered attack causes frequency deviation more than the permissible range and damages to the system.

According to Table 1, in tests 1st, 2nd, 3rd, 4th and 6th, the amount of ACE signal did not exceed the threshold 0.05 pu, so these attacks cannot be detected through this signal and remain stealthy. However, by using the attack detection algorithm which is presented in this paper, these attacks were detected shortly after the start of the attack, and also, the important point is the attack has been detected before it can affect the system and cause damages to the system. For example, in Test 4, a ramp attack occurs with \( \lambda_r = 0.022 \) at 50’. In this test, the value of ACE signal after little increasing remains constant at 0.0418 pu which is \(<0.05\) pu. Thus, this attack is not detected by ACE signal method and finally causes the frequency deviation to cross the threshold at 66.745pu and the system to be damaged. However, by the presented approach in this paper, the attack was detected at 53.52’, before it can damage the system.

In tests 5th, 7th, 8th, 9th and 10th, in the presence of the attack, the amount of ACE signal has increased from 0.05 pu, so these attacks are not hidden and can be detected by ACE signal. But anyway, as shown in Table 1, these attacks also are recognised by the proposed method at an appropriate time.

We can also examine our proposed detector to detect the scaling and random attacks we previously had in Figs. 7 and 8. As can be seen in Figs. 13a and b, our proposed detector can detect not only ramp attack but also these other types of attacks.

### 5 Conclusion

Regarding the vulnerability of smart grid to cyber attacks, AGC is noteworthy from the attacker’s perspective due to a couple of reasons. First, it is responsible for controlling frequency in power system, so any interference in its function can cause catastrophic consequences such as widespread blackout. Second, since essential data for this system is measured by sensors and transmitted to AGC through a communication link, this system is exposed to cyber attacks. In this paper, first, we showed that some kinds of attacks

| No. | \( \lambda_r \) | max [ACE] | \( t_i \) | \( t_d \) | \( t_s \) |
|-----|--------------|-----------|---|---|---|
| 1   | 0.01         | 0.019     | 50 | 53.43 | 83.51 |
| 2   | 0.015        | 0.0285    | 50 | 53.46 | 73.236 |
| 3   | 0.02         | 0.038     | 50 | 53.518 | 68.53 |
| 4   | 0.022        | 0.0418    | 50 | 53.52 | 66.745 |
| 5   | 0.03         | 0.057     | 50 | 53.4 | 62.794 |
| 6   | -0.02        | 0.038     | 50 | 53.049 | 66.651 |
| 7   | -0.03        | 0.057     | 50 | 52.86 | 61.7 |
| 8   | 0.04         | 0.076     | 50 | 52.737 | 59.6 |
| 9   | 0.05         | 0.095     | 50 | 52.737 | 57.99 |
| 10  | 0.09         | 0.171     | 50 | 51.581 | 54.327 |
can be detected only by using ACE signal such as scaling attack and random attack. However, there are some kinds of attack which are stealthy and are not detected by ACE signal such as some kinds of ramp attack. Hence, an algorithm by designing Kalman filter and using $\chi^2$-detector was proposed to detect stealthy ramp attack. It was seen that utilising this conventional detector in our algorithm is not able to detect such attacks. Therefore, we proposed a detector for embedding in our detection algorithm and finally, simulations proved the efficiency of our proposed algorithm by using our detector.

6 References

[1] Kuvshinkova, S.: ‘SOL slammer worm lessons learned for consideration by the electricity sector’, North Am. Electr. Reliab. Council, 2003, 1 (2), pp. 1–5
[2] Farwell, J. P., Rohozinski, R.: ‘Stuxnet and the future of cyber war’, Survival, 2011, 53 (1), pp. 23–40
[3] Conti, J. P.: ‘The day the samba stopped’, Eng. Technol., 2010, 5 (4), pp. 46–47
[4] Ao, W., Song, Y., Wen, C.: ‘Adaptive cyber-physical system attack detection and reconstruction with application to power systems’, IET Control Theory Appl., 2016, 10 (12), pp. 1458–1468
[5] Liu, A., Bai, L.: ‘Distributed model predictive control for wide area measurement power systems under malicious attacks’, IET Cyber-Phys. Syst.: Theory Appl., 2018, 3 (3), pp. 111–118
[6] Shafai, B., Moradmand, A., Nazari, S.: ‘Observer-based controller design for systems with derivative inputs’, Proc. Conf. Communication, Control, and Computing (Allerton), Allerton Park and Retreat Center, Monticello, IL, USA, September 2019, pp. 1038–1044
[7] Di Giorgio, A., Pietrabissa, A., DelliPriscoli, F., et al.: ‘Robust protection scheme against cyber-physical attacks in power systems’, IET Control Theory Appl., 2018, 12 (13), pp. 1792–1801
[8] Nazari, S., Shafai, B., Moradmand, A.: ‘Robust intrusion detection in dynamic networks’, Proc. Conf. Control Technology and Applications, Kowloon, HONG KONG, August 2019, pp. 988–993
[9] Li, B., Xiao, G., Lu, R., et al.: ‘On feasibility and limitations of detecting false data injection attacks on power grid state estimation using D-FACTS devices’, IEEE Trans. Ind. Inf., 2019, 16, pp. 854–864
[10] Bi, S., Wang, T., Wang, L., et al.: ‘A novel cyber fault prognosis and resilience control for cyber-physical systems’, IET Cyber-Phys. Syst., Theory Appl., 2019, 4 (4), pp. 304–312
[11] Roy, S.D., Debbarma, S.: ‘Detection and mitigation of cyber-attacks on AGC systems of low inertia power grid’, IEEE Syst. J., 2019, 14, pp. 2023–2031
[12] Li, Y., Zhang, P., Ma, L.: ‘Denial of service attack and defense method on load frequency control system’, J. Franklin Inst., 2019, 356 (15), pp. 8625–8645
[13] Lou, X., Tran, C., Tan, R., et al.: ‘Assessing and mitigating impact of time delay attack: case studies for power grid controls’, IEEE J. Sel. Areas Commun., 2019, 38, pp. 141–155
[14] Sridhar, S., Govindaraju, M.: ‘Model-based attack detection and mitigation for automatic generation control’, IEEE Trans. Smart Grid, 2014, 5 (2), pp. 580–591
[15] Tan, R., Nguyen, H.H., Foo, E.Y., et al.: ‘Modeling and mitigating impact of false data injection attacks on automatic generation control’, IEEE Trans. Inf. Forensics Sec., 2017, 12 (7), pp. 1609–1624
[16] Akbarian, F., Ramezani, A., Hamidi-Beheshti, M. T., et al.: ‘Intrusion detection on critical smart grid infrastructure’, Smart Grid Conf. (SGC), Kurdistan, Iran, November 2018, pp. 1–6
[17] Bevrani, H.: ‘Robust power system frequency control’ (Power Electronics and Power Systems, Springer, Cham, 2014)
[18] Teixeira, A., Sou, K. C., Sandberg, H., et al.: ‘Secure control systems: a quantitative risk management approach’, IET Control Theory Mag., 2015, 35 (1), pp. 24–45
[19] Tan, R., Nguyen, H.H., Foo, E.Y., et al.: ‘Optimal false data injection attack against automatic generation control in power grids’, Proc. Int. Conf. Cyber-Physical Systems, Vienna, Austria, April 2016, pp. 1–10
[20] Kundur, P., Balu, N.J., Lauby, M.G.: ‘Power system stability and control’ (McGraw-hill, New York, 1994), pp. 581–610
[21] Simon, D.: ‘Optimal state estimation: kalman, H infinity, and nonlinear approaches’ (John Wiley & Sons, USA., 2006)
[22] Brunback, B., Srinath, M.: ‘A chi-square test for fault-detection in Kalman filters’, IEEE Trans. Auton. Control, 1987, 32 (6), pp. 552–554
[23] Dixon, W. J., Massey, F. J.: ‘Introduction to statistical analysis’ (McGraw-Hill, New York, USA, 1969), pp. 344–345