Detection of False Data Injection Attacks Based on Kalman Filter and Controller Design in Power System LFC

Rujun Zhu¹, Chongxin Huang¹, Song Deng² and Yichen Li¹

¹ College of Automation & College of Artificial Intelligence, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu, 210023, China
² Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu, 210023, China

*Corresponding author’s e-mail: hcx@njupt.edu.cn

Abstract. False data injection attacks pose a great threat to the safe and stable operation of power systems. Therefore, the detection and defense of false data injection attacks in LFC systems is becoming more and more important. First, based on the equivalent model of the LFC system and the Kalman filter algorithm, this paper proposes a false data injection attack detection method; secondly, a robust controller is used to reduce load disturbances according to the operating characteristics of the LFC system; then the idea of switching links is proposed to reduce the impact of cyberattack on the system; finally, MATLAB/Simulink software is used to carry out simulation tests. The test results verify the effectiveness of the false data injection attack detection method and switch link defense method proposed in this paper.

1. Introduction
The stable operation of the power system requires that the power generation and load maintain a balance, and the frequency of the power grid is stable. Load frequency control (LFC) is an important means to maintain the stability of the grid frequency [1]. By controlling the active power of the generator set to track load changes, the system frequency deviation is zero, so as to achieve stable operation of the power system. In recent years, with the continuous extension of the power system communication network and the further expansion of the coverage, the operation structure and operation mode of the power system have become more complicated. There have been a large number of studies showing that the power system is extremely vulnerable to cyberattack [2]. The signals that need to be transmitted over long distances in the LFC system are more vulnerable to false data injection attacks. If it is not possible to detect whether the system is under false data injection attacks in time, it not only affects system frequency, but also impacts the stability and economical operation of the power grid[3-5]. Therefore, network security in load frequency control has become one of the important requirements for ensuring the safe operation of power systems.

There have been a lot of researches on cyberattack in power systems at home and abroad at present. False data injection attack (FDIA) is a typical attack in malicious cyberattack. This attack involves hackers injecting designed false data into the system to bypass the data detection module, misleading the control center, and making the power system unable to operate safely and stably[6]. The authors in [7] summarize the research status of AGC system cyberattack from the angle of attack form, attack variables, attack detection and defense; The authors analyze the vulnerability of false data injection attacks from the perspective of the attacker, and improves the attack effect by increasing the sensitivity.
of attack parameters in [8]; From the perspective of the defender, through the method of load forecasting, the range of load changes is considered, and the range of change of regional control deviation is predicted to determine whether the system is under malicious cyberattack in [9,10]; The authors in [11,12] from the perspective of the defender use the original training samples in different scenarios to perform machine learning on the consistency information of different modes to detect attacks; In order to defend against cyberattack, the authors take false data as unknown input and proposes a random data estimator, which uses numerical comparison to detect false data in [13,14]. The authors use real-time load forecasting to predict the regional control deviation, compare the predicted value with the measured value to determine whether it is under attack, and use the predicted value instead of the measured value after the attack is detected in [15].

However, the detection of cyberattack in the above-mentioned literature mainly relies on the model prediction of the system and the original training samples of different scenarios. In practical applications, the accuracy of prediction and the diversity of training samples need to be considered. However, there are few studies on the detection and defense of cyberattack based on the equivalent model of the LFC system. Aiming at the problem of whether the collected signals in power system load frequency control are subject to cyberattack, this paper proposes a false data injection attack detection method suitable for power system load frequency control. This method uses the Kalman filter algorithm to effectively determine the reliability of the system frequency and tie line power. Based on this detection method, a robust controller in load frequency control is designed, and a defense method for link switching is proposed. The simulation verified that this method can effectively ensure the safe and stable operation of the power system.

2. Principle and analysis of false data injection attacks
False data injection attack is an attack that destroys the integrity of system data. The attacker invades the system through the network link, tampering with the measurement value of the system state, deceiving the control center, so as to change the operating state of the system, affecting the safe and stable operation of the system, and allowing the attacker to obtain economic benefits. As shown in Figure 1, the signals that need to be collected are the frequency deviation and the tie-line power in the LFC system. Since the signal needs to be transmitted over a long distance, it is possible to be attacked by false data injection during the signal acquisition and transmission process. By tampering with the frequency deviation and the tie-line power in the system, the system misestimates the area control error (ACE) or forces the load frequency control system to overshoot and cause frequency fluctuation. Then change the control effect of the controller, even cause the frequency to cross the boundary, induce the system to deviate from the normal operation state, and trigger the action of the safety and stability device.

According to the load frequency control system model diagram shown in Figure 1, the state-space LFC space model can be written as:

\[
\begin{align*}
\dot{x}_i(t) &= Ax_i(t) + Bu_i(t) + B_d d(t) \\
y_j(t) &= Cx_i(t) + v_j(t) \\
x_i(t) &= [\Delta f_i(t), \Delta P_j(t), \Delta P_{\text{g}}(t), \Delta P_{\text{e}}(t), \Delta A_{\text{c}}(t), I_{\text{acc}}]^T \\
y_j(t) &= \Delta f_j \\
y_{\text{g}}(t) &= ACE = \beta \Delta f_j + \Delta P_{\text{g}} \\
y_{\text{e}}(t) &= I_{\text{acc}} \\
y_j(t) &= [y_j(t), y_{\text{g}}(t), y_{\text{e}}(t)]^T \\
u(t) &= \Delta P_{\text{t}}(t) \\
d_j(t) &= [\Delta P_{\text{g}}(t), \eta(t)]^T
\end{align*}
\]  

(1)

(2)

Where \( x_i(t) \) denotes the system state variables; \( y_j(t) \) denotes the output variable; \( u_i(t) \) denotes the control variable; \( d_j(t) \) denotes the process noise vector; \( v_j(t) \) denotes the measurement noise and is assumed to have Gaussian distribution; \( f_j(t) \) denotes the system frequency; \( P_{\text{g}}(t) \) denotes the turbine power; \( P_{\text{e}}(t) \) denotes the governor value; \( P_{\text{t}}(t) \) denotes the net tie-line power; \( ACE(t) \) denotes the area.
control error; \( I_{\text{ace}}(t) \) denotes the integral of \( ACE(t) \); \( \Delta \) denotes the deviation from normal value; \( \beta \) denotes the frequency bias coefficient; \( R \) denotes the droop coefficient; \( T_g \) denotes the governor time constant; \( T_t \) denotes the turbine time constant; \( H \) denotes the area aggregate inertia constant; \( D \) denotes the area load damp constant; \( T_i \) denotes the tie-line synchronizing coefficient; and the continuous state-space matrices \( A \), \( B \), \( B_a \) and \( C \) are given as:

\[
A = \begin{bmatrix}
\frac{D}{H_s} & \frac{1}{H_s} & \frac{1}{H_s} & 0 & \frac{1}{H_s} & 0 \\
0 & \frac{1}{T_s} & \frac{1}{T_s} & 0 & 0 & 0 \\
0 & 0 & \frac{1}{T_s} & 0 & 0 & 0 \\
-\frac{1}{RT_s} & 0 & 0 & 0 & 0 & 0 \\
\gamma_t & 0 & 0 & 0 & 0 & 0 \\
\beta & 0 & 0 & 1 & 0 & 0
\end{bmatrix}
\]

\[
B = \begin{bmatrix}
0 \\
0 \\
0 \\
0 \\
0 \\
0
\end{bmatrix}
\]

\[
B_a = \begin{bmatrix}
\frac{1}{H_s} \\
0 \\
0 \\
0 \\
0 \\
0
\end{bmatrix}
\]

\[
C = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\]

The attacker uses certain technical means to inject false measurement data into the system's frequency deviation signal or tie line power signal. That is, the frequency deviation or the tie-line power measured by the sensor becomes: \( \Delta f(t) = \Delta f(t) + \alpha \), \( \Delta P_{tie}(t) = \Delta P_{tie}(t) + \alpha \), where \( \Delta f(t) \) denotes frequency deviation when not under attack; \( \Delta P_{tie}(t) \) denotes tie-line power when not under attack; and \( \alpha \) denotes false data designed by attackers.

Figure 1. LFC diagram of Area

3. Detection of FDI attacks using Kalman filter

3.1. System state estimation based on Kalman filter

The measurement data in LFC system is transmitted to the control center through sensors. Due to the measurement noise of the device, the measurement data of the sensor is not completely accurate, so the error generated by the measurement noise under normal circumstances is far smaller than the allowable error threshold in statistics. For the measured values of system frequency deviation and tie-line power deviation being attacked by false data injection, a Kalman filter is used to detect false data. The process of Kalman filtering can be divided into two steps: Predict the state variables of the system and correct each state variable, that is, detect whether the system is under false data injection attacks and send the obtained optimal estimation value of the system to the control center.

For the above-mentioned dynamic model of load frequency control, after discretization at time \( k \), the state space model of discretized load frequency control can be obtained:
\[
\begin{align*}
\mathbf{x}(k+1) &= \mathbf{\Phi}(k)\mathbf{x}(k) + \mathbf{w}(k) + \mathbf{F}(k)\mathbf{d}(k) \\
\mathbf{y}(k) &= \mathbf{H}(k)\mathbf{x}(k) + \mathbf{v}(k)
\end{align*}
\]

(3)

Where \( \mathbf{\Phi} = \text{e}^{\mathbf{A}T} \); \( \mathbf{w} = \int_0^T \text{e}^{\mathbf{A}t}\mathbf{B}_w \, dt \); \( \mathbf{F} = \int_0^T \text{e}^{\mathbf{A}t}\mathbf{F} \, dt \); \( \mathbf{H} = \mathbf{C} \); \( k \) denotes the sampling time, which is a positive integer; \( T \) denotes the sampling period; \( \mathbf{x}(k) \) denotes the state vector of the system at time \( k \); \( \mathbf{y}(k) \) denotes the observation signal of the corresponding state; \( \mathbf{d}(k) \) denotes the process noise vector; \( \mathbf{v}(k) \) denotes the measurement noise; \( \mathbf{\Phi} \) denotes the state transition matrix; \( \mathbf{F} \) denotes the noise driving matrix; \( \mathbf{H} \) denotes the observation matrix.

Perform Kalman filter estimation on the above discrete system:

Step 1: State estimation at time \( k \):
\[
\hat{\mathbf{x}}(k+1|k) = \mathbf{\Phi}(k)\hat{\mathbf{x}}(k) + \mathbf{w}(k)
\]

(4)

Step 2: Forecast covariance at time \( k \):
\[
\mathbf{P}(k|k-1) = \mathbf{P}(k-1)\mathbf{\Phi}^T + \mathbf{F}Q\mathbf{F}^T
\]

(5)

Step 3: Filter gain matrix:
\[
\mathbf{K}(k) = \mathbf{P}(k|k-1)\mathbf{H}^T[\mathbf{H}\mathbf{P}(k|k-1)\mathbf{H}^T + \mathbf{R}]^{-1}
\]

(6)

Step 4: Update the covariance matrix:
\[
\mathbf{P}(k|k) = \mathbf{P}(k|k-1) - \mathbf{K}(k)\mathbf{H}\mathbf{P}(k|k-1)
\]

(7)

Step 5: Update the status:
\[
\tilde{\mathbf{x}}(k) = \hat{\mathbf{x}}(k|k-1) + \mathbf{K}(k)[\mathbf{y}(k) - \mathbf{H}\hat{\mathbf{x}}(k|k-1)]
\]

(8)

The Kalman gain converges in few steps where the Kalman filter equation can be updated as:
\[
\tilde{\mathbf{x}}(k+1) = \mathbf{\Phi}(k)\hat{\mathbf{x}}(k) + \mathbf{w}(k) + \mathbf{K}(k)[\mathbf{y}(k + 1) - \mathbf{H}(\mathbf{\Phi}(k)\hat{\mathbf{x}}(k) + \mathbf{w}(k))]
\]

(9)

The error between the predicted value of the Kalman filter and the measured value is defined as:
\[
\epsilon(k+1) = \mathbf{y}(k + 1) - \mathbf{H}(\hat{\mathbf{x}}(k) + \mathbf{w}(k))
\]

(10)

Where \( \mathbf{x}(k) = [\Delta f(k), \Delta P_{\text{me}}(k), \Delta P_{\text{re}}(k), \Delta P_{\text{re}}(k), I_{\text{ac}}]^T \); \( \mathbf{R} \) is the variance of the measurement noise \( \mathbf{d}(k) \); and \( \mathbf{Q} \) is the variance of the process noise \( \mathbf{v}(k) \).

The optimal estimation value of the system state is obtained, and the optimal estimation value after Kalman filtering is transmitted to the controller.

3.2. Detection of FDI attacks

The measurement data in the LFC system of the power system is transmitted to the control center through the sensor. The measurement data of the sensor is not completely accurate, and the equipment itself has measurement noise. The error caused by the measurement noise of the system under normal conditions is very small, far less than the allowable error threshold of the power system, which is a sign that the system has not been attacked by false data injection. If the attacker injects designed false data into the vector measurement signal, the system error will exceed the error allowable threshold. At this time, the system state quantity predicted by the Kalman filter and the measured value of the system state are used for the prediction residual test.

\[
|\Delta f(k) - \hat{\Delta f}(k)| \leq \epsilon_f
\]

(11)

\[
|\Delta P_{\text{me}}(k) - \hat{\Delta P}_{\text{me}}(k)| \leq \epsilon_{\text{me}}
\]

(12)

Where \( \Delta f(k) \) and \( \Delta P_{\text{me}}(k) \) denote the measured value obtained by the sensor; \( \hat{\Delta f}(k) \) and \( \hat{\Delta P}_{\text{me}}(k) \) denote the predicted value of the Kalman filter; \( \epsilon \) denotes a predefined threshold which is chosen to be greater than the maximum absolute value of error in case of the healthy system. If formula (11) or (12) is satisfied, the system is considered to be operating normally; if the above formula is not satisfied, the system is considered to be under false data injection attacks.
4. Design of load frequency controller

Once the power system suffers a cyberattack, it is very likely to cause the paralysis of the entire power information physical system. Therefore, it is not only necessary to detect cyberattack in time, but also has high robust performance requirements for the power system. When the false data injection attack is detected, a $H_{\infty}$ robust controller is designed to suppress the frequency fluctuation of the system against the perturbation of internal parameters and the disturbance of external power. The design goal of the $H_{\infty}$ robust controller is to make the $H_{\infty}$ norm of $\mathbf{z}'(s)$ smaller than the predetermined value $\gamma$. That is, when $\|\mathbf{z}'(s)\| \leq \gamma$, in view of the uncertain factors caused by external disturbance, the closed-loop system can meet the corresponding robust performance requirements.

Usually, we focus on the frequency deviation, the ACE and the control energy cost when evaluating the LFC performances. Thus, the controlled variables $z$ for the $H_{\infty}$ control design are elected as follows:

$$\begin{align*}
z_1(t) &= \Delta f(t) \\
z_2(t) &= I_{acx} \\
z_3(t) &= \Delta P_i(t)
\end{align*}$$  \hspace{1cm} (13)

Then the state space of LFC system is can be rewritten as:

$$\begin{align*}
\dot{x}(t) &= A x(t) + B_1 u(t) + B_d d(t) \\
y(t) &= C_1 x(t) + C_{in} u(t) + D_d d(t) \\
\mathbf{z}(t) &= C_2 x(t) + C_{in} u(t) + D_{in} d(t)
\end{align*}$$  \hspace{1cm} (14)

Assuming that the system is controllable and observable, we can design an $H_{\infty}$ dynamic controller $K$ with the following form:

$$\begin{align*}
\dot{x}_e(t) &= A_k x_e(t) + B_k u(t) \\
\mathbf{y}_e(t) &= C_k x_e(t) + D_k d(t)
\end{align*}$$  \hspace{1cm} (15)

where $x_e$ denotes the state variables of the controller; $y_e$ denotes the output variable of the controller; $u$ denotes the input variables of the controller; and $A_k$, $B_k$, $C_k$, $D_k$ are the constant matrices with appropriate dimension.

The closed-loop system can be stable and meet the following goals:

$$\begin{align*}
\dot{x}_e(t) &= A_k x_e(t) + B_k u(t) \\
\mathbf{z}(t) &= C_k x_e(t) + D_k d(t)
\end{align*}$$  \hspace{1cm} (16)

That is, for the closed-loop transfer function from $\omega$ to $z$, if and only if there is a symmetric matrix $X$ that satisfies the following formula, the $H_{\infty}$ norm is less than the predetermined value $\gamma$:

$$\begin{bmatrix}
A_k X + X A_k^T & B_k & X C_k \\
B_k^T & -I & D_k \\
C_k X & D_k & -\gamma^2 I
\end{bmatrix} < 0 \hspace{1cm} X > 0$$  \hspace{1cm} (17)

This paper uses the linear matrix inequality (LMI) toolbox in MATLAB to solve the robust controller.

5. Simulation analysis

In order to verify the effectiveness of the false data injection attack detection method and the robust controller proposed in this paper, this section uses MATLAB/Simulink software to conduct simulation experiments on the LFC system interconnected between two areas. Table 1 shows the parameters of the two-area LFC system used.

| Area | D (pu) | H (sec) | Tt (sec) | Tg (sec) | R (pu) |
|------|--------|--------|--------|--------|--------|
| 1    | 0.008  | 0.016  | 0.3    | 0.08   | 2.4    |
| 2    | 0.01   | 0.2    | 0.5    | 0.09   | 0.09   |
5.1. Attack detection
As shown above, the absolute value of error is calculated to detect cyberattack, and the selected attack detection threshold is greater than the maximum value of the error when there is no cyberattack, which is set to $\epsilon_1 = 4 \times 10^{-4}$, $\epsilon_2 = 5 \times 10^{-4}$.

Figure 2 shows that a false data injection attack with a magnitude of $-3.1 \times 10^{-1}$ (pu) and a time of 1 sec is applied to the frequency deviation in area 1 at $t = 1$ sec. Through the Kalman filter algorithm in Section 3, it can be seen that when $t = 1$ sec and an attack occurs, the absolute value of error exceeds the set threshold, which can effectively detect that the frequency deviation has suffered a false data injection attack.

![Figure 2. The absolute value of frequency deviation error](image1)

Figure 3 shows a false data injection attack with a magnitude of $-4.1 \times 10^{-1}$ (pu) and a time of 1 sec applied to the tie-line power in area 1 at $t = 1$ sec. Through the Kalman filter algorithm in Section 3, it can be seen that when $t = 1$ sec and an attack occurs, the absolute value of error exceeds the set threshold, which can effectively detect that the tie-line power has suffered a false data injection attack.

![Figure 3. The absolute value of tie-line power error](image2)

5.2. Link switching
The Kalman filter algorithm can only detect false data injection attacks, and the robust controller designed in Section 4 can only suppress a part of the attack disturbance, but cannot remove the impact
of cyberattack. The power grid has a high degree of reliability and security for the communication system. Therefore, strong defensive measures are required for false data injection attacks. At this stage, there are two links between the frequency and the power of the tie line in the LFC system. The two are physically isolated and serve as backup links. The possibility of an attacker attacking the two links at the same time is very small. Cyberattacks can be detected in time, link switching can be performed, and backup measurement signals can be used to transmit to the control center to maintain the stability of the LFC system.

As shown in Figure 4 for the load frequency control of the single-area power system, if it is detected that link 1 suffers from a false data injection attack, the equipment on link 2 can still receive data, then the equipment on link 1 needs to disconnect the fault link from the corresponding port by itself, then the power system switches the backup link to realize the redundancy protection of the power system.

![Backup link of power system](image)

**Figure 4. Backup link of power system**

Fig. 5 shows the frequency deviation signal of area 1 attacked by false data injection. It can be seen that the robust controller can only suppress the disturbance of external input, and it cannot suppress the impact of false data injection attack. Simulation results show that the Kalman filter can effectively detect the false data attack, but it has little inhibition effect on the attack, and cannot keep the frequency at a stable value. When selecting the switching link, the frequency deviation of the system can be kept to zero and the stability of LFC system can be maintained.

![Frequency deviation in area 1](image)

**Figure 5. Frequency deviation in area 1**
Figure 6 shows the tie line power under false data injection attack. It can be seen that the robust controller can only suppress the disturbance of the external input, and it cannot suppress the influence of the false data injection attack on the tie line. Simulation results show that the Kalman filter can effectively detect whether the tie line power is attacked by false data, but it has little inhibition effect on the attack and cannot keep the tie line power at a stable value. After selecting the switching link, the tie line power of LFC system can be maintained at a stable value to maintain the stability of LFC system.

6. Conclusion
With the continuous extension of the power system communication network and the further expansion of the coverage, the network security of the power system has gradually become the focus of attention. In this context, this paper proposes a method for detecting LFC false data injection attacks based on Kalman filtering and a method for link switching. The results show that the Kalman filter algorithm can accurately detect whether the power system is under false data injection attacks, while robust controller can only suppress a part of the false data injection attacks. But the link switching method can effectively guarantee the power system operates safely and stably.

Acknowledgments
Thanks to all the authors who contributed to this article. The work is supported by National Nature Science Foundation under Grant 51977113.

References
[1] Wang, Y.L., Tan, W. (2014) Robust load frequency control for multi-area power systems. J. Computer Simulation, 31 (2): 179-182.
[2] Liang, J., Sankar, L., Kosut, O. (2016) Vulnerability analysis and consequences of false data injection attack on power system state estimation. J. IEEE Transactions on Power Systems, 31 (5): 3864-3872.
[3] Tang, Y., Chen, Q., Li M.Y., Ni, M., Liang, Y. (2016) Overview on Cyber-attacks Against Cyber Physical Power System. J. Automation of Electric Power Systems, 40 (17): 59-69.
[4] Liu, Y., Ning, P., Reiter, M.k. (2011) False data injection attacks against state estimation in electric power grids. J. ACM Transactions on Information and System Security, 14 (1): 1-33.
[5] Chen, W.H., Chen, W.G., Xue, A.C. (2019) Physical power system security risk assessment and defense resource allocation for cooperative information attacks. J. Power grid technology, 43(07): 2353-2360.

[6] Liang, G., Weller, S.R., Zhao, J. (2017) The 2015 ukaine blackout: Implications for false data injection attacks. J. IEEE Transactions on Power Systems, 32 (4): 3317-3318.

[7] Xu, F.Y., Xue, A.C., Chang, N.C. (2020) Research status and prospect of cyberattacks and defenses on automatic generation control in power system. J/OL. Automation of Electric Power Systems: 1-15.http://kns.cnki.net/kcms/detail/32.1180.TP.20200828.0746.010.html.

[8] Yuan, Y., Li, Z., Ren, K. (2011) Modeling load redistribution attacks in power systems. J. IEEE Transactions on Smart Grid, 2 (2): 382-390.

[9] Roy, S.D., Debbarma, S. (2020) Detection and mitigation of cyberattacks on AGC systems of low inertia power grid. J. IEEE Systems Journal, 14 (2): 2023-2031.

[10] Zhou, X.H., Zhou, G., Fan, Y. (2019) Resilient event triggered output feedback control for load frequency control systems subject to cyberattacks. J. IEEE Access, 7: 58951-58958.

[11] Zhang, Y.S., Li, X.W., Li, J.C. (2019) Spark-based power grid industrial control system flow anomaly detection platform. J.Computer system application, 28 (08): 46-52.

[12] Ameli, A., Hooshyar, A., Yazdavar, A.H. (2018) Attack detection for load frequency control systems using stochastic unknown input estimators. J. IEEE Transactions on Information Forensics and Security, 13 (10): 2575-2590.

[13] Ameli, A., Hooshyar, A., Elsaaadany, E.F. (2018) Attack detection and identification for automatic generation control systems. J. IEEE Transactions on Power Systems, 33 (5): 4760-4774.

[14] Ni, M., Yan, J., Bai, R., Tang, Y. (2016) Power system cyberattack and its defense. J. Automation of Electric Power Systems, 40 (5): 148-151.

[15] Sridhar, S., Govindarasu, M. (2014) Model-based attack detection and mitigation for automatic Generation control. J. IEEE Transactions on Smart Grid, 5 (2): 580-591.