Counteractive control against cyber-attack uncertainties on frequency regulation in the power system

Sheetla Prasad

Abstract: In this study, an observer based control strategy is proposed for load frequency control (LFC) scheme against cyber-attack uncertainties. Most of research work focused on detection scheme or delay estimation scheme in presence of cyber-attack vulnerabilities and paid less attention on design of counteractive robust control scheme for LFC problem. Thus, observer based control scheme is designed here and provides robust performance against unknown input attack uncertainty and communication time-delay attack uncertainty. The generalized extended state observer (GESO) is used not only for state and disturbance estimation but also for disturbance rejection of the system. The said observer ensures accurate estimation of the actual states leading to convergence of estimation error to zero. So, the observer based linear quadratic regulator (LQR) is used to regulate the closed-loop damping ratio against cyber-attack uncertainty. In addition to fast response in terms of settling time and reduced over/undershoots, the proposed control scheme satisfactorily compensates the cyber-attack uncertainties in power system cyber physical networks and also compared with existing traditional PI and PID controllers. The simulation results demonstrate the robustness in terms of stability and effectiveness in terms of system security with proposed controller when subjected to cyber-attack uncertainties and load disturbances.

1 Introduction

Load frequency control (LFC) is an auxiliary and necessary control scheme in interconnected power systems. The LFC minimises the frequency deviation through real power effective matching between generation units and connected loads, and contributes to achieving needs of the automatic generation control (AGC). The real power effective matching condition can be achieved with proper control between real power generation units and tie-line power exchange among control areas [1, 2]. However, the intelligent LFC strategy needs additional information from plant remote terminals. Thus, the control areas and its generator units both are interconnected to control centre through communication networks. The measured signals from remote terminal units (RTUs) in interconnected power system are transferred to control centre via communication channels [2]. In the interconnected power system, the time delays exist in sensors at RTUs, control process and especially in communication channels. Due to delay, the power system faces a stability problem and also degrades system performance or even leads to power system blackout. Several LFC schemes were developed in the literature to enhance power system performances with consideration of current state information and assumed all plant states information are free from communication delays [3, 4].

On increasing demand for the reliable smart energy system, the traditional power system modified through numerous technological infrastructure and motivated to implement wide-area monitoring system [5–12]. Therefore, the power system cause to participate in a typical delayed cyber-physical power system. In [5], a novel resilient control system for LFC is designed against open communication network vulnerabilities. Authors developed a second defence layer to detect and mitigate simultaneously communication vulnerabilities in power systems. The impact of transmission line failure is analysed experimentally and designed two mitigation structures to avoid transmission line failure using optimal power flow [12]. Dealing with communication delays in cyber-physical power system is also a formidable task. Several researchers considered the impact of communication delay in the design of LFC [13–15]. A delay-dependent stability based a novel adaptive control strategy is designed to coordinate multi-microgrid energy system in the presence of the communication failure and minimised effect of communication delay [13]. A non-linear sliding mode based LFC scheme is developed for constant time delay and time-varying delay for multi-area interconnected power system [14]. To reduce complexity in the computation of controller and observer gains, a decoupled observer-based control strategy developed using a recursive linear matrix inequality (LMI) in the presence of input and output time delays [15]. A delay margin estimation approach is applied and enhanced power system performance in [16]. Thus, several control strategies designed to minimise effect of delays on plant performance in plant state, input and output signals.

On the other hand, to achieve smart energy system objectives, the supervisory control and data acquisition and phasor measurement unit integrated into information technology networks, which develop cyber-physical security issues. Thus, the smart power system cyber-physical networks enhance the growing opportunity of numerous threats against the security and stability of the modern power system. The classification and origin of threats are investigated in [8–10] for the security of future smart power system. The performance of modern power system control areas is extensively dependent on associated cyber networks, which inevitably leads to increased cyber vulnerabilities. The cyber assessments, weakens and detection strategies of a smart power network on AGC are investigated in [17, 18]. Hence, smart cyber-physical power networks enhance the false attack vulnerability, which may lead to decrease in smart power system security and stability.

However, attackers have the main objective to deteriorate smart power system cyber-physical networks performance or destabilise through manipulation of cyber-physical network information either in terms of communication delays or false information. Thus, several research efforts applied on the smart power system cyber-physical networks to minimise the impacts of cyber attacks as reported in [19–28]. Hence, power system cyber-physical networks based AGC problems can be divided into four cyber-attack vulnerabilities such as (i) infrastructure-based design and analysis [5–12], (ii) dynamic characteristics based design and analysis [21, 22], (iii) unknown input attack uncertainty model-based detection and analysis [20, 22, 23, 28, 29] and (iv) communication delay...
attack uncertainty model-based detection and analysis [19, 24–26]. Thus, the security and stability of smart AGC against the cyber-attack vulnerabilities is a challenging task.

However, previous research is mainly centralised on the detection of LFC attacks and paid less attention to produce remedial control actions. In the most LFC attacks, the attacker falsifies only the area control error (ACE) via frequency and tie-line power measurement signals to interrupt the normal operation of the plant. Hence, the detection scheme of LFC attacks and corresponding remedial control actions needs to compromise simultaneously. Thus, a counteractive control scheme is designed in this study for infrastructure-based attack uncertainty and communication delay-based attack uncertainty. The infrastructure based attack uncertainty in LFC problem means that the attackers are altered control signals using full access or hijack of infrastructure. Thus, the controller will receive incorrect signals and system becomes open-loop means uncontrolled at control centre side. Meanwhile, the reformatted attackers can also execute communication time delay in the system states (through communication channel). The proposed control scheme is capable to mitigate the effect of both attack uncertainty on power system normal operation without the use of a separate advanced detection scheme. The LFC upgraded attacks are renamed as cyber-attack vulnerability and; considered here as unknown input attack uncertainty and time delay attacks vulnerability.

The linearised model of two-area power system [3] with communication time delay in the system states (through communication network) is shown in Fig. 1. The proposed controller uses estimated states instead of measured states directly and achieve minimum over/under shoots and reduced settling time simultaneously against unknown input attacks and time delay attacks vulnerability.

Remaining sections of study is organised as follows: Section 2 describes briefly the modelling of the two-area power system and design procedures of the observer, followed by a model of LFC attack uncertainty in Section 3. The formulation of observer-based control methodology is proposed in Section 4. LMI optimisation analysis is also included in this section. The proposed controller stability analysis is presented in Section 5, followed by results and discussions in Section 6. Lastly, the conclusions drawn from the presented work are given in Section 7.

2 Power system configuration

In the single area power system, the primary control loop is sufficient to minimise the mismatch between generation and demand. While in the interconnected power system, in addition to the primary control loop and secondary control loop, a supplementary control action in the secondary loop is implemented to minimise the mismatch between generation and demand. On this basis, a supplementary control loop is designed here without any change in the primary speed control loop and secondary control loop. As such, the power system network although being a complex nonlinear system can be considered first-order linearised transfer function for the study on LFC problem due to its slow convergence rate.

2.1 Two-area power system

The linearised model of two-area power system [3] with communication network is shown in Fig. 1a. The dynamics equations of the two-area system for $i=1, 2$ is given as:

\[
\Delta f_i(t) = \frac{1}{T_{ph}}\Delta f_i(t) + \frac{K_{fi}}{T_{ph}}\Delta P_{mi}(t) - \frac{K_{fi}}{T_{ph}}\Delta P_{pi}(t) - \frac{K_{fi}}{T_{ph}}\Delta P_{di}(t) - \frac{K_{fi}}{T_{ph}}\Delta P_{ei}(t)
\]

\[
\Delta P_{mi}(t) = - \frac{1}{T_{ch1}}\Delta f_i(t) + \frac{1}{T_{ch1}}\Delta P_{mi}(t) + \frac{1}{T_{ch1}}\Delta P_{pi}(t)
\]

\[
\Delta E_i(t) = K_{Ei}R_i\Delta f_i(t) + K_{Ei}\Delta P_{di}(t)
\]

\[
\Delta P_{di}(t) = 2\pi T_{pi}(\Delta f_i(t) - \Delta f_i(t))
\]

\[
\Delta P_{ei}(t) = \frac{1}{T_{ph}}\Delta f_i(t) - \frac{1}{T_{ph}}\Delta P_{pi}(t) - \frac{1}{T_{ph}}\Delta E_i(t) + \frac{1}{T_{ph}}\Delta \theta_i(t)
\]

\[
\Delta P_{ei}(t) = - \frac{1}{T_{ph}}\Delta f_i(t) - \Delta P_{pi}(t)_w, \quad \text{where } i, j = 1, 2 \text{ and } i \neq j.
\]

Now, two-area power system dynamic (1)-(5) are represented in the state-space as given below:

\[
x(t) = Ax(t) + Bu(t) + D\Delta P_{di}(t)
\]

\[
y(t) = Cx(t)
\]

The state variables; $\Delta f_i(t), \Delta P_{pi}(t), \Delta E_i(t), \Delta P_{di}(t), \Delta P_{ei}(t)$ and $\Delta P_{ei}(t)$ represent the small deviation in frequency (Hz), generator output (p.u. MW), integral control (p.u.), tie-line power flow (p.u. MW), load disturbance (p.u.) and governor valve position (p.u. MW), respectively; $K_{fi}, R_i, K_{ei}$ and $B_i$ are power system and machines gain, speed regulation coefficient (Hz/s), integral control gain and frequency bias factor, respectively; $T_{pi}, T_{ph}$ and $T_{ch1}$ are the time constants in (s) of the power system, governor and turbine-generator, respectively for the area $i$. $T_{ph}$ is the interconnection tie-line gain (p.u./(rad). Between areas $i$ and $j$. The dimension of system matrices (6) are considered as $A \in \mathbb{R}^{n \times n}, B_i \in \mathbb{R}^{n \times n}, D \in \mathbb{R}^{n, m}$ and $C \in \mathbb{R}^{n \times n}$ respectively, and $x \in \mathbb{R}^{n \times 1}, u \in \mathbb{R}^{k \times 1}, y \in \mathbb{R}^{m \times 1}$ and $\Delta P_i \in \mathbb{R}^{n 	imes 1}$ are considered as ‘$n$’ states, ‘$k$’ input, ‘$m$’ output, ‘$r$’ load disturbance vectors, respectively. The design of the observer and controller for the aforementioned general system matrices is considered in the following section.

2.2 Design of observer

The state observer is used to reconstruct the un-measurable state variables based on the measured system inputs and outputs. In practice, load disturbance is very difficult to directly measure in power system due to its unknown characteristics. Such as, deviations in governor valve position in power system are also not easy to measure. The modern power system states can be easily manipulated by attackers to deteriorate plant performance via cyber-physical networks. Therefore, power system states and load disturbances are estimated from the limited available measurements using GESO [3]. A GESO-based control method is designed here to solve the disturbance attenuation problem of a class of plant against cyber-attack uncertainties. In addition, the controller uses estimated states instead of measured states directly from the plant as shown in Fig. 1b and reduces the impact of cyber-attack uncertainties on plant performance. Hence, the observer is filtered un-modelled dynamics from actuators/sensors, states attack uncertainties and closed-loop system performance improves if an observer-based equivalent control was applied. To estimate the states and load disturbance simultaneously, the extended states are defined as $x_d(t)$ and $h(t)$ as given below:

\[
x_{d, i} = \begin{bmatrix} \Delta P_{di} \end{bmatrix} \quad \text{and} \quad h(t) = \begin{bmatrix} \Delta \Delta P_{di} \end{bmatrix} = \begin{bmatrix} \Delta \Delta P_{di} \end{bmatrix}
\]

\[
\dot{x} = \hat{A}x + \hat{B}u + \hat{E}h(t)
\]

\[
y = Cx
\]

Now, two-area plant state (6) is transformed into other state variables including plant states and extended states as:

\[
\dot{x} = \hat{A}x + \hat{B}u + \hat{E}h(t)
\]

\[
y = Cx
\]

The system (8) state variables and matrix dimensions are

\[
x = \begin{bmatrix} x_{d, i} \end{bmatrix}, \quad \hat{B} = \begin{bmatrix} B_i \end{bmatrix}, \quad E = \begin{bmatrix} 0_{n \times r} & 1_{r \times r} \end{bmatrix}, \quad \hat{A} = \begin{bmatrix} \tilde{A}_{d, i} & D_{d, i} \\ 0_{n \times r} & 1_{r \times r} \end{bmatrix}
\]

\[
\hat{A} = \begin{bmatrix} \tilde{A}_{d, i} & D_{d, i} \\ 0_{n \times r} & 1_{r \times r} \end{bmatrix}
\]

\[
C = \begin{bmatrix} C_{d, i} \end{bmatrix}, \quad \text{respectively.}
\]
The observer for the modified (8) can be designed when following Assumption 1 is satisfied.

**Assumption 1:** The system matrix $A$ and control input matrix $B_u$ of the state (6) is controllable implies system matrix $\bar{A}$ and output matrix $C_v$ of the reshaped state (8) is observable.

Then observer equation for the reshaped state (8) is given as:

\[
\begin{align*}
\dot{\hat{x}} &= \bar{A}\hat{x} + \bar{B}_\mu u + L(y - \hat{y}) \\
\hat{y} &= C_v\hat{x}
\end{align*}
\]  

where the state variable $\hat{x}$ is the estimated state and output of the system (8), respectively. Matrix $L \in \mathbb{R}^{(n+r)\times r}$ is the observer gain. The observer gain is designed here to make the observer dynamics fast and closed-loop system performance is robust against uncertainties and given in Section 4.

### 2.3 Objective of the study

The objective of the study is to mitigate the effect of infrastructure and communication-based attack uncertainty using remedial control scheme on modern LFC problem.

![Proposed control scheme structure](image)

Fig. 1 Proposed control scheme structure

(a) Two-area power system control structure, (b) Proposed control scheme with cyber-attack uncertainty region

The observer for the modified (8) can be designed when following Assumption 1 is satisfied.
proposed control scheme has the ability to maintain system dynamics within permissible limits according to present cyber-attack vulnerability and the system is still laid in closed-loop without the use of any detection scheme.

3 Attack uncertainty model

In the interconnected power system, signals are measured at remote using RTUs and send to control centre through cyber-physical networks for process them. The output control signals from control centre are applied to the modern power plant as shown in Fig. 1b. A smart attacker could trigger control efforts easily by manipulation of these measured or receive signals via cyber-physical networks. As results, the system may degrade performance and force the system to operate at uneconomical operating region due to non-optimal control actions or even leads to instability. On one hand, several arbitrary unknown measurements are injected by attackers to degrade system dynamics and plant stability in [21–23, 28, 29]. Therefore, some unknown measurement input attacks inputs [23] are described with a few standard signal pattern as:

(i) Scaling attack: A scaling attack involves modifying true measurement inputs to higher or lower values depending on the scaling attack variables. The modified output of the power system with the scaling parameter \( \alpha \) is described as

\[
y(t) = \begin{cases} 
Cx(t) & \forall t \not\in \text{ack} \\
(1 + \alpha)Cx(t) & \forall t \in \text{ack}
\end{cases}
\]  

(ii) Ramp attack: Ramp attacks involve gradual modification of true measurement inputs by the addition of ramp variables. In this attack, the modified output with ramp constant slope parameter \( \alpha \) is given as

\[
y(t) = \begin{cases} 
Cx(t) & \forall t \not\in \text{ack} \\
\alpha t + Cx(t) & \forall t \in \text{ack}
\end{cases}
\]  

(iii) Pulse attack: Pulse attack involves modifying measurement inputs through temporally spaced short pulses. The output is modified according to a pulse pattern with rate \( \alpha \) and given as

\[
y(t) = \begin{cases} 
Cx(t) & \forall t \not\in \text{ack} \\
(1 + \alpha)Cx(t) & \forall t \in \text{ack}
\end{cases}
\]  

(iv) Random attack: This attack is similar to ramp attack and increase or decrease true measurement inputs random manner. The modified output of the power system with the scaling parameter \( \alpha \) is described as

\[
y(t) = \begin{cases} 
Cx(t) & \forall t \not\in \text{ack} \\
(1 + \alpha)nC(t) & \forall t \in \text{ack}
\end{cases}
\]  

where \( \text{ack} \) is a time instant attack. The unknown input attack uncertainty may have different form/shapes and the above standard patterns of unknown attack uncertainty are considered for analysis in this study.

While on the other hand, an unknown time delay is injected by attackers in states of plant, with the purpose of destabilising the system [19, 24–26]. This is also known as the time-delay-switch attack as described in [24]. In this study, time delay attacks in LFC problem are assumed to provide intentionally delays in transmitted states by the attacker via cyber-physical communication channel. The time delay attack uncertainty is described as mentioned below.

(v) Time-delay attack: This attack prevents the transmitted signal from RTUs to the control centre through the communication channel and described as:

\[
y(t) = Cx(t - \tau(t))
\]  

where \( \tau(t) \) is a time delay in received plant states at control centre location. The time delay attack uncertainty may have a different pattern and in this study, the standard constant and time-varying delay patterns are considered for analysis.

In the literature, different types of attack uncertainty are analysed by several researchers. A large group of the researchers are considered unknown input attack uncertainty while rest researchers are considered time delay attack uncertainty on the LFC problem and designed a suitable detection scheme. Fewer contributions on the design of a counteractive robust control scheme are given by researchers. Here, based on time instant of attacks, unknown input attack uncertainty and time delay attack uncertainty are clubbed together for the LFC problem as

\[
y(t) = \begin{cases} 
y_{\text{ack}}(t)Cx(t) + (1 - \gamma)Cx(t - \tau(t)) & 1 \leq t - t_{\text{ack}}y(t) \\
0 > t - t_{\text{ack}}y(t) & 0 > t - t_{\text{ack}}y(t)
\end{cases}
\]  

where \( \gamma \) and \( \text{ack} \) are the attack type indicator constant and unknown input attack parameter. The term \( \tau(t) \) is the delay injected by the attacker to destabilise the power system. The performances of the proposed control scheme as described in the next section is illustrated against an unknown input attack uncertainty and time delay attack uncertainty in Section 6.

4 Control methodology

In this section, GESO is used here to estimate power system states and disturbances. The power system states are measured using sensors, etc. and communicated to control centre through cyber communication channels as shown in Fig. 1b. The attackers may attack the sensors or cyber communication channels. In the literature, several studies were considered known inputs based attack on the state and measurement. In this study, unknown inputs attack uncertainty and time delay attack uncertainty is considered. These unknown uncertainties are introduced by attackers to degrade the performance of the plant or even lead to power system instability. Thus, GESO is used to minimise cyber-attack uncertainties affects in estimated plant states. Then estimated plant states by the observer are applied as input to the LQR controller. The parameters of the LQR are optimised using LMIs. Finally, the effective control law is obtained using the estimated disturbance and minimised LQR controller. The detailed design and stability analysis is given in following subsections.

4.1 Linear quadratic regulator

The LQR design technique is well known and has widely implemented for the synthesis of controllers using state feedback and easily represented with the mathematical equation in terms of LMIs. The LQR control approach corresponds to a quadratic criterion, which is optimised linearly and defines an optimal control law associated with the energy function of the plant states and control effort variables. The quadratic criteria are seeking to balance the response speed and intensity of control effort, \( u(t) = -Kx(t) \) defines a quadratic cost function as

\[
J_{\text{min}} = \int_0^\infty (x(t)^TQx(t) + u(t)^TRu(t))dt
\]
where \( Q = Q^T \) is a semi-positive definite matrix that penalises the convergence speed of the plant states from any initial point, and \( R = R^T \) is the positive definite matrix that penalises the intensity of the control effort. The matrix \( K \) is state feedback gain. Thus, the selection of weighting matrices \( Q \) and \( R \) is a formidable task for the researchers. In the multi-variable power system, the selection of weight matrices \( Q \) and \( R \) remains difficult due to the involving actions of system states and control inputs. Therefore, in order to select optimal weights of matrices, the proposed systematic method in [30] is adopted here. The selection procedure of weight matrices \( Q \) and \( R \), is described in Fig. 2. To convert quadratic cost function into an LMI optimisation framework, (17) is represented by a function \( \chi \) and written as

\[
\chi = J^T_{mn}PJ_{mn} \tag{18}
\]

Equation (18) is a positive function \( \chi > 0 \), by differentiating it with respect to time we obtain:

\[
\dot{\chi} = J^T_{mn}P(\ddot{x}Q + x^T R x) \tag{19}
\]

After substituting from (17) into (19), we get

\[
\dot{\chi} = J^T_{mn}P(\ddot{x}Q + x^T R x) \tag{20}
\]

by substituting state feedback control law \( u(t) = -K\dot{x}(t) \) in (20), we get

\[
\dot{\chi} = J^T_{mn}P(\ddot{x}Q + x^T R x) \tag{21}
\]

Equation (21) is written [30, 31] by using the trace operator \( \text{Tr}(.) \) as follows:

\[
\dot{\chi} = \text{Tr}(Q) + \text{Tr}(R^{1/2}KPR^{1/2}) > 0 \tag{22}
\]

Suppose constraints equation \( X = R^{1/2}KPR^{1/2} \) is considered and written as

\[
\chi = \text{Tr}(Q) + \text{Tr}(R^{1/2}KPR^{1/2}) > 0 \tag{22}
\]
\[ X - R^{1/2} K P R^{1/2} \geq 0 \] (23)

The inequality (23) can be converted into LMI by using Schur complement [31] as follows:

\[
\begin{bmatrix}
X & R^2 Y \\
Y^T R^{-2} P & P
\end{bmatrix} > 0
\] (24)

The detailed overall system optimisation analysis is given below.

4.2 Design of state feedback gain K

After the selection of weighting matrices \( Q \) and \( R \), the state feedback gain \( K \) is computed using LQR-based LMI optimisation framework and written in a form of LMIs [31].

**Theorem 1:** The state feedback gain \( K \) and effective control law are designed in such a way that following cost function and LMIs hold simultaneously.

\[
\begin{align*}
\min_{P, X, Y} & \quad \text{Tr}(Q P) + \text{Tr}(X) \\
\text{subject to} & \quad P > 0 \\
& \quad A P + P A^T + B Y + Y^T B^T + I < 0 \\
& \quad X R^2 Y \\
& \quad Y^T R^{-2} P > 0
\end{align*}
\] (25)

where \( P \in \mathbb{R}^{n \times n}, Y \in \mathbb{R}^{n \times r}, X \in \mathbb{R}^{r \times r} \) and state feedback gain \( K \) can be obtained as

\[
K = -YP^{-1}
\] (26)

In order to achieve a smooth and fast response of the closed-loop system, an equivalent input disturbance (EID) compensator as discussed in [3] is applied here against bounded disturbances. Thus, an effective control law is designed as

\[
u(t) = u_d(t) - \Delta \dot{P}_d(t) \equiv - K \dot{x}(t) - \Delta \dot{P}_d(t)
\] (27)

where the variable \( \Delta \dot{P}_d(t) \) is \( \bar{x}_d \) is the estimated load disturbance of the two-area power system as given in Section 2.

**Proof:** The Lyapunov equation is written as

\[
\dot{v} = \dot{x}(t) P \dot{x}(t)
\] (28)

It is the first time derivative and by substituting from (8), it gives:

\[
\dot{v} = \dot{x}(t) [AP + A^T P] \dot{x}(t) + 2\dot{x}(t) P B \dot{e}_d(t) + 2\dot{x}(t) P D \Delta \dot{P}_d(t)
\] (29)

From control law (27) with EID compensator and after simplification, it is written as:

\[
\dot{v} = \dot{x}(t) [AP + A^T P - BPK - K^T PB^T] \dot{x}(t)
\] (30)

By defining a new term \( Y = K P \), (22), (24) and (30) can be written in a single LMI optimisation as given in (25). This completes the proof.

5 Closed-loop system stability

The closed-loop system stability with the proposed control scheme as shown in Fig. 1b is described in this section. The proposed control technique desires at the ultimate boundedness of all the signals of interest. The ultimate bounds can be defined by appropriate choice of observer and control parameters without any prior knowledge of the bounds of the uncertainties.

**Assumption 2:** The power system disturbance and rate of change of disturbances are bounded, i.e. \( \| \Delta P_d(t) \| \leq \rho \) and \( \| \dot{h}(t) \| \leq \lambda \). The state error and extended state error of the observer (9) is defined as

\[
\begin{align*}
e(t) &= \dot{x}(t) - x(t) \\
e_d(t) &= \dot{\Delta} \dot{P}_d(t) - \Delta \dot{P}_d(t)
\end{align*}
\] (31)

Then observe error dynamics is obtained using (8), (9) and (31) as follows:

\[
\dot{e}(t) = (\dot{A} - L C_v) e(t) - E \dot{h}(t)
\] (32)

The convergence of observer dynamics is determined by the stability of the state feedback gain. From (23), (27) and (33), it follows that

\[
\begin{align*}
u(t) &= \dot{x}(t) P x(t) + e^T(t) P e(t)
\end{align*}
\] (34)

The first time derivation of the Lyapunov function, \( \dot{v}(t) = x^T(t) P x(t) + \dot{x}(t) P \dot{x}(t) + e^T(t) P e(t) + e^T(t) \dot{P} e(t) 
\) (35)

Using (6) and (32), above (35) becomes

\[
\begin{align*}
v(t) &= \dot{x}(t) [AP + A^T P - BPK - K^T PB^T] x(t) \\
&= -2 \dot{x}(t) P E \dot{h}(t)
\end{align*}
\] (36)

Now equivalent control effort (27) applies and after simplification, gives

\[
\begin{align*}
u(t) &= \dot{x}(t) [AP + A^T P - BPK - K^T PB^T] x(t) \\
&= -2 \dot{x}(t) P E \dot{h}(t)
\end{align*}
\] (37)

From (25), (27) and (33), it follows that

\[
\begin{align*}
u(t) &= -\dot{x}(t) I x(t) - e^T(t) Q e(t) \\
&= -2 \dot{x}(t) P E \dot{h}(t)
\end{align*}
\] (38)

After further simplification, it gives

\[
\begin{align*}
u(t) &= -\dot{x}(t) I x(t) - e^T(t) Q e(t) \\
&= -2 \dot{x}(t) P E \dot{h}(t)
\end{align*}
\] (39)

Therefore, \( \nu(t) < 0 \), which proves the asymptotic stability of the closed-loop system. This completes the proof.
5.1 Summary of the proposed control design procedure

Detailed design procedure of the proposed control approach is summarised in the following steps:

Step 1: Design GESO with proper selection of the observer gain $L$, such that matrix $(A - LC)$ has negative real part of its eigenvalues.

Step 2: Obtain the state and control weighting matrices $Q$ and $R$ using described procedure in Fig. 2.

Step 3: The matrices $P$, $X$, and $Y$ are calculated by solving the LMI (25) using ‘feasp’ and ‘mincx’ solvers in MATLAB® Robust Toolbox [30] with proper selection of weight matrices.

Step 4: Obtain state feedback gain $K$ and finally design the equivalent control effort (27).

6 Results and discussions

To demonstrate the performance of proposed control technique through MATLAB® simulations are conducted on two-area power system as shown in Fig. 1a. Two-area power system is considered as linearised first order transfer function model for LFC problem because its time constant varies from seconds to minute. Thus, each area of the two-area power system is represented by two linear equivalent variables and its parameters are given in Table 1.

Based on two-area power system state-space dynamics, the weight matrices $Q$ and $R$ are calculated according to flow chart steps as shown in Fig. 2. The state feedback gain $K$ is obtained by solving the LMI (25) using ‘feasp’ and ‘mincx’ solvers in MATLAB® Robust Toolbox. The selection of observer gain $L$ is quite complex due to its generalised properties and applications [3]. To achieve quick observer response, the poles of observer is selected arbitrarily far way from closed-loop system poles. However, the observer gains are chosen such that $(A - LC)$ is a Hurwitz matrix. Finally, equivalent observer based LQR control scheme (25) is designed using obtained state feedback gain $K$ and observer gain $L$.

In this study, cyber-attack uncertainties on LFC scheme is considered as unknown input attack uncertainty and time delay attack uncertainty, and described in Section 3. The designed observer based controller is tested here in presence of cyber-attack uncertainties. Hence, following simulation scenarios are performed on two-area power system LFC scheme to illustrate the robustness of the proposed control scheme in presence of random load disturbance and cyber-attack uncertainties. The random load disturbance pattern for both control areas are shown in Fig. 3a.

- Validation of the observer-based LQR controller with proper choice of observer gain.
- Effectiveness of proposed controller with unknown bounded scaling pattern attack inputs.
- Performance of proposed controller with unknown bounded ramp pattern attack inputs.
- Validation of proposed controller with unknown bounded pulse pattern attack inputs.
- Performance of proposed controller with unknown bounded random pattern attack inputs.
- Effectiveness of proposed controller with unknown constant time delay attack inputs.
- Validation of proposed controller with unknown time-varying delay attack inputs.
- Performance indices based comparisons of all the above scenarios and comparison with proportional–integral (PI) controller [32].

6.1 Validation of the observer with proper choice of gain

The GESO is used here to estimate system states and load disturbances from measured input and system output. The designed
observer gains are given as $L = [-30 - 21 - 98 - 22 - 36 - 29 - 39 - 45 - 50 - 55]$. The observer error dynamic of the frequency deviation and deviation in real power generation state variable in area-1 at step load disturbance $\Delta P_d = [0.01 0.02]$ are shown in Fig. 3b. It is evident that observer is estimated the system states accurately.

6.2 Effectiveness of the proposed controller with unknown bounded scaling pattern attack inputs

In this subsection, the performance of the proposed control scheme is evaluated in the presence of random load disturbance and unknown bounded scaling attack uncertainty. The unknown bounded scaling attack input pattern in per unit basis is shown in Fig. 4a and described in (10). The scaled system output is applied to observer and estimated variables via observer are considered as input to LQR controller. The deviations in frequency in areas, tie-line real power exchange deviation and deviation in real power generation in area-1 responses are shown in Fig. 5 (solid line with blue colour) in presence of scaling attack uncertainty and random load disturbance. It is observed that the proposed control scheme is responded well and have ability to sustain the system response within permissible limits and within sight of unknown scaling attack uncertainty and random load disturbances. Hence, proposed control scheme is sustained closed-loop stability and robustness even in the presence of unknown input attack uncertainty.

6.3 Performance of proposed controller with unknown bounded ramp pattern attack inputs

In this subsection, the performance of the proposed control scheme is tested in the presence of unknown bounded ramp type attack uncertainty and random load disturbance. The unknown bounded ramp type attack input pattern in per unit basis is shown in Fig. 4b and described in (11). The attack based system equivalent output is applied to the proposed control scheme. The deviations in

---

**Fig. 4** Unknown input attack uncertainty patterns
(a) Unknown bounded scaling attack input pattern in per unit basis, (b) Unknown bounded ramp type attack input pattern in per unit basis, (c) Unknown bounded pulse attack uncertainty pattern, (d) Unknown bounded random attack uncertainty pattern in per unit basis

**Fig. 5** Proposed control scheme responses with different unknown input attack uncertainty and random load disturbances

---

This is an open access article published by the IET under the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/).
and have ability to sustain the system dynamics within permissible attack uncertainty and random load disturbance. The unknown area-1 dynamic responses are shown in Fig. 5 (dotted line with red colour) in presence of ramp type attack uncertainty and random load disturbance.

It is seen that the proposed controller is performed effectively and have ability to sustain the system dynamics within permissible limits even in the presence of unknown ramp attack uncertainty. Thus, the proposed control scheme is enhanced closed-loop stability and applicability even in the presence of unknown input attack uncertainty.

6.4 Validation of proposed controller with unknown bounded pulse pattern attack inputs

Similar to above subsections, the observer based controller performance is demonstrated in the presence of unknown pulse attack uncertainty and random load disturbance. The unknown bounded pulse attack uncertainty pattern is shown in Fig. 4c and it is described similar to unknown bounded scaling attack uncertainty as given in (12). However, the deviation in frequency in area-1 and area-2, tie-line real power exchange and real power generation in area-1 dynamic responses are shown in Fig. 5 (dotted line with pink colour) with pulse attack uncertainty and random load disturbance. It is evident that the observer based controller has ability to sustain the closed-loop system dynamics within permissible limits and minimised oscillations even in the presence of unknown input attack uncertainty. Thus, proposed controller is reduced the wear and tear problem in the governor valve mechanism.

6.5 Performance of proposed controller with unknown bounded random pattern attack inputs

Finally, to test robustness of the proposed controller, an unknown bounded random attack uncertainty is applied on the closed-loop system with random load disturbance. The unknown bounded random attack uncertainty pattern in per unit basis is shown in Fig. 4d and described as similar to unknown bounded scaling attack uncertainty as given in (13). The attack based system equivalent output is applied to the proposed control scheme. Hence, the deviations in frequency in area-1 and area-2, tie-line real power exchange and real power generation in area-1 dynamic responses are shown in Fig. 5 (dashed line with green colour) in presence of bounded random attack uncertainty. From said figure, the proposed observer based controller has ability to sustain the closed-loop system dynamics within permissible limits and enhanced closed-loop robustness. Hence, the proposed control scheme is allowed to provide satisfactorily over/under shoots as well as oscillations even in the presence of unknown input attack uncertainty.

6.6 Validation of the proposed controller with unknown constant time-delay attack inputs

Now, the robustness of proposed control scheme is illustrated under unknown constant time-delay attack uncertainty. The attacker have main objective is to significantly change measured data. Thus, four types of unknown constant time-delay attack uncertainty is arbitrarily considered here as (i) \( \tau = 0.0 \), (ii) \( \tau = 1.2 \), (iii) \( \tau = 2.0 \) and (iv) \( \tau = 5.0 \). The communicated plant states are manipulated by attacker via cyber-physical communication channels. The received manipulated data at observer location are shown in Fig. 6 and described in (14). This measured data is applied to observer and observer is used to estimate system dynamics accurately even in presence of different constant time delays. The tracking dynamics of observer is accurate without any delay estimation and tracking responses are given previous described in Fig. 3b. Estimated states by observer are applied to LQR controller. The deviations in frequency in area-1 and area-2, tie-line real power exchange and real power generation in area-1 closed-loop dynamic responses are shown in Fig. 7 in presence of different constant time-delays and step load disturbance \( \Delta P_d = [0.01 \ 0.02]^T \). It is observed from Fig. 7 that proposed controller have ability to maintain closed-loop dynamic response within limits. Thus, proposed observer based controller converges slowly and gives satisfactorily response.

This signifies that proposed control scheme is capable to sustain closed-loop dynamics even in presence of constant time-delay attack uncertainty.

6.7 Validation of the proposed controller with unknown inputs time-varying delay attack inputs

In this subsection, time-varying delay attack uncertainty is applied on proposed control scheme. To test effectiveness and robustness of the proposed controller, a three variant time-varying delay attack uncertainty is analysed on closed-loop system with random load disturbance. The three variant time-varying delays are shown in Fig. 8 and system output is described by (14). The received manipulated states at observer location are shown in Fig. 9 with three unknown time-varying delay attacks. As observed, the received states through cyber communication channels is completely changed by attackers as shown in Fig. 9 and now this
data is applied to proposed control scheme. The deviations in frequency in area-1 and area-2, tie-line real power exchange and real power generation in area-1 closed-loop system dynamic responses are shown in Fig. 10 in presence of three time-varying delay attacks and random load disturbance. It is observed from Fig. 10 that the proposed controller adaptively meets the robust performance against time-varying delay attack uncertainty in communication channels. The control effort in area-1 is given in Fig. 8 and found satisfactorily response with minimum chattering. It signifies that observer have good tracking ability even in presence of time-delay attack uncertainty. The influence of time-varying delay attack uncertainty on closed-loop system dynamics is marginal, which is tolerated and can be acceptable for practical frequency regulation.

6.8 Performance indices based comparisons all above scenarios

The integral square error (ISE), integral absolute error (IAE) and integral time absolute error (ITAE) is calculated for deviation in frequency in area-1 of the above simulations (Section 6.2 to Section 6.7) and given in Table 2.

It is observed that the closed-loop system dynamics exhibits better performance and provides robustness as evidenced by satisfactorily over/under shoots, settling time and transient frequency oscillations with proposed control scheme even in presence of unknown bounded input attack uncertainty and unknown time delay attack uncertainty.
Finally, proposed control scheme is tested and compared with PI-control structure scheme at resonance attack [32] on two-area power plant dynamic (6). To make plant states quickly unstable, an attacker manipulates any plant inputs according to rate of change of frequency (RoCoF) to provide false inputs through feedback on LFC problem as discussed in [32] and defined as resonance attacks. The frequency rate and PI controller gains are considered as given in Appendix and load input in area-1 is selected randomly as resonance attack input feedback signal with $\Delta P_{d_{\text{max}}} = 0.4 \text{ pu}$. The plant load in area-1 is considered as false input through feedback to the controller so as to drive RoCoF out of the admissible boundary. The resonance attack [32] load pattern in area-1 is applied to proposed controller and PI controller as shown in Fig. 11 (solid line with blue colour in first subfigure). The proposed controller (dotted black lines) and PI controller (solid red lines) responses for area-1 in terms of deviations in RoCoF and frequency are shown in Fig. 11. It is evident that proposed control scheme and PI controller responses are still stable with oscillations against resonance attacks in load input.

The over/undershoots and settling time in RoCoF and frequency responses with proposed controller is minimum compared to PI-controller in presence of resonance attack [32]. Hence, proposed control scheme provides robustness performance in the presence resonance attack and enhanced its application.

6.10 Comparison of proposed control scheme with GESO-based state-proportional–integral–derivative (PID) controller

In addition, the proposed control scheme is compared with GESO-based state-PID controller. The state-PID controller design steps are considered here as similar in [33] and LQR controller is replaced only with state-PID controller in the proposed control scheme structure. The state-PID controller gains for two area
power system are given in Appendix. The power system states are estimated via GESO and used by the state-PID controller. The measurement unknown bounded input attack uncertainties, communication constant delay (1.2 s) and time delay pattern τ, are taken as similar as given in Figs. 4, 7 and 8, respectively. The deviations in frequency in both areas dynamics with proposed control scheme and GESO-based state-PID controller are shown in Figs. 12 and 13, respectively in presence of measurement attack uncertainties.

It is evident that proposed control scheme responses are improved comparatively with GESO-based state-PID controller in terms of over/undershoots and settling time. The proposed control scheme dynamics are more robust compare to GESO-based controller given in Fig. 14. From said figure, it is seen that the proposed control scheme have ability to sustain closed-loop system dynamics within permissible limits even in unknown bounded input attack uncertainty and time delay attack uncertainty. Thus, very small deviations in frequency with the proposed observer based controller have less impact on the plant reserve capacity and power market.

6.11 Interpretations on the simulation studies

The effectiveness and robustness of the proposed control scheme is verified through MATLAB simulations against unknown bounded input attack uncertainty and time delay attack uncertainty. In this study, false data injection attacks and time delay switch attacks as reposted in the literature are studied and analysed simultaneously on proposed control scheme. The convergence of the proposed controller demonstrates the asymptotic stability of the closed-loop system. The performance of the proposed controller in terms of under/overshoots and settling time are simultaneously significantly reduced. The designed control signal provides very less chattering effect signifying reduced wear-out of actuators (valve) in steam turbine. In addition, proposed control scheme is compared with existing PI-controller in presence of resonance attacks [32], GESO-based PID controller [33] and it improved plant time response with minimum oscillations against resonance attack. It is evident that proposed control scheme have ability to sustain closed-loop system dynamics with optimised feedback gain to achieve the improved performance. The convergence of the proposed control scheme was studied simultaneously with proposed controller. The observer and LQR controller gains were selected using gramian approach as described in flow chart. The LMI technique applied in the design of the equivalent control law

| Scenario | ISE | IAE | ITAE |
|----------|-----|-----|------|
| scaling attack uncertainty | $2.4526 \times 10^{-6}$ | $0.0050$ | $0.1051$ |
| ramp attack uncertainty | $8.3821 \times 10^{-6}$ | $0.0121$ | $0.3188$ |
| pulse attack uncertainty | $2.9782 \times 10^{-6}$ | $0.0051$ | $0.1056$ |
| random attack uncertainty | $2.9700 \times 10^{-6}$ | $0.0050$ | $0.1040$ |
| constant time delay attack uncertainty | — | — | — |
| $\tau = 0.0 \text{s}$ | $9.2473 \times 10^{-7}$ | $0.0004$ | $0.0008$ |
| $\tau = 1.2 \text{s}$ | $4.1654 \times 10^{-7}$ | $0.0011$ | $0.0020$ |
| $\tau = 2.0 \text{s}$ | $5.5779 \times 10^{-7}$ | $0.0015$ | $0.0035$ |
| $\tau = 5.0 \text{s}$ | $7.1187 \times 10^{-7}$ | $0.0022$ | $0.0080$ |
| time-varying delay attack uncertainty | — | — | — |
| $\tau_1(t)$ | $1.5051 \times 10^{-5}$ | $0.0131$ | $0.2938$ |
| $\tau_2(t)$ | $1.4373 \times 10^{-5}$ | $0.0137$ | $0.3036$ |
| $\tau_3(t)$ | $1.3820 \times 10^{-5}$ | $0.0168$ | $0.4091$ |

Fig. 11 Comparative plant response analysis in presence of resonance attack [32] in area-1
reduced settling time and on other hand, security and stability of power system was also increased. The simulated results demonstrate feasibility, effectiveness and robustness of the proposed control scheme even in the presence of different unknown bounded input attack uncertainty and different time delay attack uncertainty. Based on the study presented in this paper,

Fig. 12 Comparative frequency deviations against unknown bounded scaling and ramp attack input
(a) Comparative responses in presence of unknown bounded scaling pattern attack input, (b) Comparative responses in presence of unknown bounded ramp pattern attack input

Fig. 13 Comparative frequency deviations against unknown bounded pulse and random attack input
(a) Comparative responses in presence of unknown bounded pulse pattern attack input, (b) Comparative responses in presence of unknown bounded random pattern attack input
future work will focus on the detection of resonance cyber attacks uncertainty in power system.

8 References

[1] Kundur, P.: ‘Power system stability and control’ (McGraw Hill, New York, 1994)
[2] Bevrani, H.: ‘Robust power system frequency control’ (Springer, New York, NY, USA, 2014), ch. 2
[3] Prasad, S., Parwar, S., Kishor, N.: ‘Load frequency regulation using observer based non-linear sliding mode control’, Int. J. Electr. Power Energy Syst., 2019, 104, pp. 78–93.
[4] Prasad, S., Parwar, S., Kishor, N.: ‘Non-linear sliding mode for frequency regulation with variable-speed wind energy systems’, Int. J. Electr. Power Energy Syst., 2019, 107, pp. 19–34.
[5] Abbaspour, A., Sargolzaei, A., Foruzanbehzad, P., et al.: ‘Resilient control design for load frequency control system under false data injection attacks’, IEEE Trans. Ind. Electron., 2019, 67 (9), pp. 7951–7962.
[6] Xiang, Y., Wang, L., Zhang, Y.: ‘Adequacy evaluation of electric power grids considering substation cyber vulnerabilities’, Int. J. Electr. Power Energy Syst., 2018, 96, pp. 368–379.
[7] Bompad, E., Huang, T., Wu, Y., et al.: ‘Classification and trend analysis of threats origins to the security of power systems’, Int. J. Electr. Power Energy Syst., 2013, 50, pp. 50–56.
[8] Sun, C.-C., Hahn, A., Liu, C.-C.: ‘Cyber security of a power grid: state-of-the-art’, Int. J. Electr. Power Energy Syst., 2018, 99, pp. 45–56.
[9] He, H., Yan, J.: ‘Cyber-physical attacks and defences in the smart grid: a survey’, IET Cyber-Phys. Syst. Theory Appl., 2016, 1 (1), pp. 13–27.
[10] Hua, C., Wang, Y., Wu, S.: ‘Stability analysis of micro-grid frequency control system with two additive time-varying delay’, J. Franklin Inst., 2020, 357 (8), pp. 4949–4963.
[11] Ashok, A., Hahn, A., Govindarasu, M.: ‘Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment’, J. Adv. Res., 2014, 5 (4), pp. 481–490.
[12] Poulal, S., Ni, Z., Manini, N.: ‘Real-time cyber physical system testbed for power system security and control’, Int. J. Electr. Power Energy Syst., 2017, 90, pp. 124–133.
[13] Hao, R., Ai, Q., Jiang, Z., et al.: ‘A novel adaptive control strategy of interconnected microgrids for delay-dependent stability enhancement’, Int. J. Electr. Power Energy Syst., 2018, 99, pp. 566–576.

Fig. 14 Comparative frequency deviations against unknown bounded constant and time-varying delay uncertainty
(a) Comparative responses in presence of constant time delay (1.2 s) attack uncertainty, (b) Comparative responses in presence of time-varying delay pattern (s) attack uncertainty

constant and time-varying delays’, IET Gener. Transm. Distrib., 2016, 10 (1), pp. 2771–2784.
[15] Majeed, R., Ahmad, S., Rehan, M.: ‘Delay-range-dependent observer-based control of nonlinear systems under input and output time-delays’, Appl. Math. Comput., 2015, 262, pp. 145–159.
[16] Xiong, L., Li, H., Wang, J.: ‘LMI based robust load frequency control for time delayed power system via delay margin estimation’, Int. J. Electr. Power Energy Syst., 2018, 109, pp. 91–103.
[17] Reddy, K.S., Kumar, M., Mallick, T.K., et al.: ‘A review of integration, control, communication and metering (ICCM) of renewable energy based smart grid’, Renew. Sust. Energy Rev., 2014, 38, pp. 180–192.
[18] Hammad, E., Farra, M.E.A.: ‘Implementation and development of an offline co-simulation testbed for studies of power systems cyber security and control verification’, Int. J. Electr. Power Energy Syst., 2019, 104, pp. 817–826.
[19] Mou, Q., Ye, H., Liu, Y., et al.: ‘Applications of matrix perturbation theory to delayed cyber-physical power system’, Int. J. Electr. Power Energy Syst., 2019, 107, pp. 507–515.
[20] Srithar, S., Govindarasu, M.: ‘Model-based attack detection and mitigation for automatic generation control’, IEEE Trans. Smart Grid, 2014, 5 (2), pp. 580–591.
[21] Taha, A.F., Qi, J., Wang, J., et al.: ‘Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs’, IEEE Trans. Smart Grid, 2018, 9 (2), pp. 886–899.
[22] Liang, J., Sankar, L., Kosut, O.: ‘Vulnerability analysis and consequences of false data injection attack on power system state estimation’, IEEE Trans. Power Syst., 2016, 31 (5), pp. 3864–3872.
[23] Pasqualetti, F., Dörfler, F., Bullo, F.: ‘Attack detection and identification in cyber-physical systems’, IEEE Trans. Auton. Control, 2013, 58 (11), pp. 2715–2729.
[24] Sargolzaei, A., Yen, K.K., Abdelghani, M.N.: ‘Preventing time-delay switch attack on load frequency control in distributed power systems’, IEEE Trans. Smart Grid, 2016, 7 (2), pp. 1176–1185.
[25] Li, J., Liu, X., Su, X.: ‘Sliding mode observer-based load frequency control of multi-area power system under delayed inputs attack’, 2018 Chinese Control And Decision Conf. (CCDC), Shenyang, China, 2018, pp. 3716–3720.
[26] Aminni, S., Pasqualetti, F., Mohsenian-Rad, H.: ‘Dynamic load altering attacks against power system stability: attack models and protection scheme’, IEEE Trans. Smart Grid, 2016, 9 (4), pp. 2862–2872.
[27] Peng, C., Li, J., Fei, M.: ‘Resilient event-triggering H∞ load frequency control for multi-area power systems with energy-limited DoS attacks’, IEEE Trans. Power Syst., 2017, 33 (5), pp. 4110–4118.
[28] Ding, D., Wang, Z., Ho, D.W.C., et al.: ‘Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks’, IEEE Trans. Cybern., 2017, 47 (8), pp. 1936–1947.

IET Cyber-Phys. Syst., Theory Appl., 2020, Vol. 5 Iss. 4, pp. 394–408
This is an open access article published by the IET under the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/)
9 Appendix

(a) The two-area power system state-space matrices are described as: (see equation below)

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

(b) Proposed control scheme controller gains see Table 3.

(c) PI-controller and state-PID controller gains see Table 4.

**Table 3** Proposed control scheme controller gains

| Area | Proposed LQR controller gains |
|------|-------------------------------|
| 1    | -0.2392 2.1818 0.2236 0.1208 -0.0014 0.1049 0.0033 0.1845 0.0012 |
| 2    | 0.2413 0.1253 0.0026 0.0010 0.1135 2.6606 0.2331 0.0007 0.1968 |

**Table 4** PI-controller and state-PID controller gains

| Area | PI controller gains | State-PID controller gains [33] |
|------|---------------------|---------------------------------|
| 1    | \( K_i = 0.532, K_p = 0.0496 \) | \( K_i = 61.3064, K_p = 1.3265, K_d = 5.0 \) |
| 2    | \( K_i = 0.510, K_p = 0.0498 \) | \( K_i = 24.5226, K_p = 0.5304, K_d = 2.0 \) |