2022 IEEE 61st Conference on Decision and Control (CDC)
December 6-9, 2022. Cancún, Mexico

Analyzing and Mitigating of Time Delay Attack (TDA) by using Fractional Filter based IMC-PID with Smith Predictor

Vivek Kumar and Yogesh V. Hote

2022 IEEE 61st Conference on Decision and Control (CDC) | 978-1-6654-6761-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/CDC51059.2022.9992756

***Abstract*— In this era, with a great extent of automation and connection, modern production processes are highly prone to cyber-attacks. The sensor-controller chain becomes an obvious target for attacks because sensors are commonly used to regulate production facilities. In this research, we introduce a new control configuration for the system, which is sensitive to time delay attacks (TDA), in which data transfer from the sensor to the controller is intentionally delayed. The attackers want to disrupt and damage the system by forcing controllers to use obsolete data about the system status. In order to improve the accuracy of delay identification and prediction, as well as erroneous limit and estimation for control, a new control structure is developed by an Internal Model Control (IMC) based Proportional-Integral-Derivative (PID) scheme with a fractional filter. An additional concept is included to mitigate the effect of time delay attack, i.e., the smith predictor. Simulation studies of the established control framework have been implemented with two numerical examples. The performance assessment of the proposed method has been done based on integral square error (ISE), integral absolute error (IAE) and total variation (TV).**

I. INTRODUCTION

Time delay is common throughout the nature. It can be found in a wide range of natural and artificial systems. Due to the time delay, a system can be destabilized, diminishing its performance properties. A considerable amount of research has been done to understand the challenge of controlling systems with time delay completely [1], [2], [3]. With the tremendous improvement in the Internet of Things and cyber-physical system (CPS) advancements, everything will be linked to the web anytime and from any location in the coming years. CPS are those systems that combine processing, transmission and control to satisfy the required standards from physical systems [4]. They are being used in a variety of applications, including intelligent transportation engineering, smart grid, process control industries and process automation systems [5]. Despite the many benefits, CPSs are subjected to malicious attacks, including denial-of-service (DoS) attacks [6], time delay attacks due to their structural properties. These attacks have the potential to interrupt operations as well as ruin the systems. So, enhancing CPS resiliency and reliability is crucial to get full advantages of cyber technology [7], [8]. Many industrial applications such as automation-based networking systems and power systems have also been subjected to time-delay attacks [3], [9], [10]. Time delay cyber-attacks can momentarily jam information lines to create a delay in the transmission of signal flows without affecting the data contained in the package [11]. In comparison with other attacks, the time-delay attack is a simpler attack since it does not necessitate previous control system understanding. The most prone area for time delay attack is the sensor-controller loop. Now, the concern is how to develop control mechanisms that allow the system to sustain the disturbance and also mitigating the time delay effect. As shown in Fig. 1, there are numerous attacks types on the sensor-controller loop in CPS. From the sensor module, the controller gets data about the status of the process and delivers control directives back to the real process. It can be seen in Fig. 1, where information flow from the sensor to the controller is vulnerable to TDA or DoS attack as shown by P. The controller is vulnerable to an integrity attack as shown by Q. The controller-process connectivity as represented by R is vulnerable to TDA or DoS attacks. Whereas, the plant is directly assaulted physically by the cyber-intruder as represented by S. In the TDA attack, the intruder makes the controller worthless by influencing it to collect delayed information regarding the condition of the system [11]. It is critical to develop new control procedures to maintain the system stability and enable control objectives to meet desired performance during TDA attacks. Many research studies are concerned with delay and system stability based on Lyapunov's stability criteria. Also the research exists related to TDA attack and its mitigation [12].

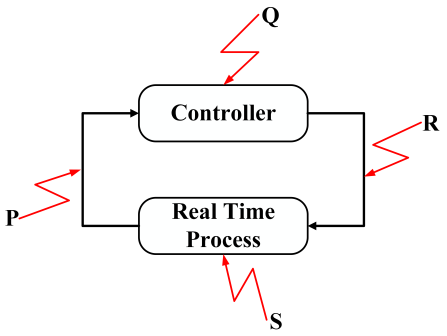

Fig. 1. Various kinds of cyber-attacks in the controller and sensor cycle.

The following points are the proposed contributions:

- Fractional Filter based Proportional Integral Derivative (FFPID) controller tuning utilizes the IMC scheme

This work is supported by IHUB NTIHAC Foundation, IIT Kanpur, India under the Project No: INF-1748-EED, IIT Roorkee.

V. Kumar is with the Department of Electrical Engineering, Indian Institute of Technology Roorkee, Uttarakhand, India, (247667) tripathivivek021@gmail.com

Yogesh V. Hote is with the Department of Electrical Engineering, Indian Institute of Technology Roorkee, Uttarakhand, India, (247667) yogesh.hote@ee.iitr.ac.in

corresponding to the maximum sensitivity.
- IMC-FFPID with Smith predictor control method for mitigating the time delay attack in the process.
- The suggested method's effectiveness is evaluated in the presence of system's delay time, load disturbances and time delay attack.

The proposed article investigates the evaluation and prevention of the effect of delay attacks, due to the security issues as mentioned above. The proposed research concentrates on delays injected into a sensor-controller loop by the hacker to disrupt the process. A simple way to implement the proposed approach is to design in the controller with the help of a fractional filter, based on the IMC scheme. Further, to nullify the delay attack, Smith predictor is used with the FFPID controller.

The following is a description of the paper's structure. The fractional filter-based IMC method is discussed in section 2. In section 3, the time delay attack is explained. The proposed idea to mitigate TDA is addressed in section 4. In section 5, the performance outcome of the closed loop is discussed. Robustness analysis has been done in section 6. Simulation study is carried out in section 7. Finally, in section 8 conclusion is discussed.

II. Internal Model Control (IMC) with Fractional Filter

The schematic representation of the IMC model with fractional filter is depicted in Fig. 2. Where $R(s)$, $D(s)$ and $Y(s)$ are set-point, disturbance input and closed loop output, respectively. This arrangement also involves model of the system $P_s(s)$, which is utilized in the controller design with the system $P(s)$ [18].

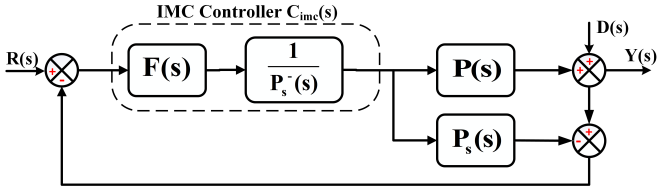

Fig. 2. Fundamental IMC structure [18].

For designing the IMC controller, the following steps are suggested.
Step 1: The system is separated into two parts. (1). Minimum phase part, (2). Non-minimum phase part.

$$P_s(s) = P_s^+(s)P_s^-(s) \tag{1}$$

where $P_s^+(s)$ contains non-minimum phase parts like time delay and right-half plane zeros. $P_s^-(s)$ contains minimum phase part.
Step 2: To construct the design of the IMC controller, adjoin a low-pass filter with minimum phase parts so that the IMC controller is appropriate.

$$C_{imc}(s) = \frac{1}{P_s^-(s)}F(s) \tag{2}$$

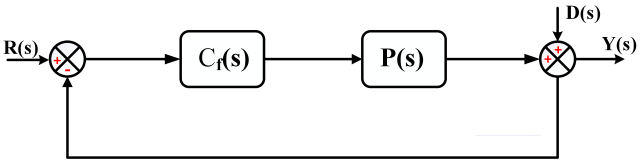

Fig. 3. Structure of basic feedback control system.

where $F(s)$ is a fractional filter formed as:

$$F(s) = \frac{1}{(\sigma s^{\gamma}+1)^p} \tag{3}$$

where the order of filter (p) should be decided in order to practical implementation of the IMC controller. Furthermore, σ is the adjustable filter time constant and γ is the fractional order of the filter, i.e., an adjustable variable.
Step 3: Finally, the feedback controller configuration is shown in Fig. 3. That can be formulated as:

$$C_f(s) = \frac{C_{imc}(s)}{1 - C_{imc}(s)P_s(s)} \tag{4}$$

III. Time Delay Attack (TDA)

The TDA intruder frequently flushes the sensor-controller transmission, which causes communication delay, in which the controller obtains the prior time's status data rather than the present information and after a while, the outcome becomes fairly unreliable because of the slower signal. When the TDA begins, the controller does not obtain any fresh information updates for a period of moments, as mentioned in (5). Delays are caused throughout TDA attacks, whether by compromising gateways or blocking distribution lines using an IoT cloud [14].

$$Out = Out(t - \tau) \tag{5}$$

Generally, in CPS, delay in time is inevitable. Therefore, purposeful delay infiltration can result in system failure. In [3], a time delay predictor is developed to predict possible delay time in order to minimize delay-based attacks, and disruption exclusion is handled using a standard PID controller. The research in [13], [15], [16] has a couple of extra detection and mitigation measures for cyber attacks with time delay approach. After estimating the delay in the sensor to controller loop using a clock counter, the proposed idea uses a smith predictor with a fractional filter-based PID controller to mitigate the time delay attack and disruption of the system.

IV. Proposed Controller for Mitigating the Time Delay Attack using FFPID with Smith Predictor

Fig. 4, shows a classic illustration of the proposed approach. In the present work, the controller is designed using a fractional filter (3) with $p = 2$, as per the approach outlined earlier. The final controller structure comprised a fractional filter with the PID controller part in cascaded form plus smith predictor, which uses to nullify the delay introduced by the attackers. In the proposed controller, the adjustable parameter of the filter is tuned such that it is enough

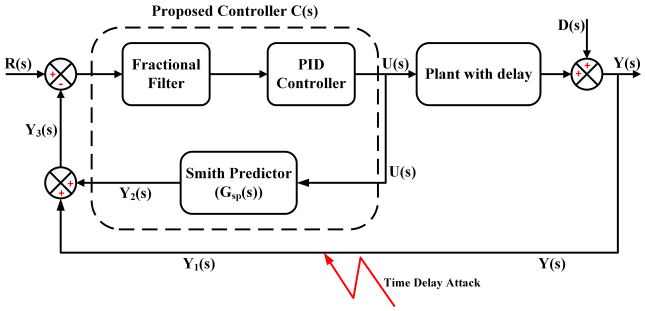

Fig. 4. Block diagram representation of the proposed method.

to optimize the controller response. Due to the fractional filter part, the number of tuning parameters is increased so that controller becomes more resilient toward set-point tracking and disturbance rejections. Furthermore, to mitigate the effect of time delay attack, Smith predictor is used along with FFPID in the inner feedback loop, which is expressed through the eq. (7).
The following is the FFPID controller configuration:

$$C_f(s) = (Fractional\ Filter\ Term\ f(s)) \times K\left(1 + \frac{1}{\tau_i s} + \tau_d s\right) \tag{6}$$

where K - is the proportional gain of the PID controller, τ_i and τ_d - are the integral time and derivative time of the PID controller, respectively. So, the Smith predictor function is:

$$G_{sp}(s) = P(s)e^{-st_d}(1 - e^{-s\tau}) \tag{7}$$

where t_d - is the delay in the process, and τ - is the amount of time introduced by the attacker.
Finally, the proposed controller structure is:

$$C(s) = \frac{C_f(s)}{1 + C_f(s)G_{sp}(s)} \tag{8}$$

A. Procedure for Mitigation of system's delay and Time delay attack through the proposed method

According to Fig. 4, when the attacker has performed a time delay attack then it's mitigation has been done by the proposed method, so that $Y_3(s) = Y(s)$ needs to be satisfied. Here,

$$Y(s) = P(s)e^{-st_d}U(s) \tag{9}$$

In Fig. 4, after the time delay attack with τ seconds:

$$Y_1(s) = P(s)e^{-s(t_d+\tau)}U(s) \tag{10}$$

Smith predictor output, according to the proposed methodology:

$$Y_2(s) = P(s)(1 - e^{-s(t_d+\tau)})U(s) \tag{11}$$

So, the final feedback signal after nullifying the system delay and time delay attack is:

$$Y_3(s) = Y_1(s) + Y_2(s) = P(s)e^{-st_d}U(s) = Y(s) \tag{12}$$

From this analysis, it can be observed that the effect of time delay attack and system's delay has been mitigated.

Consider a first order plus time delay (FOPTD) process:

$$P_s(s) = \frac{K_p e^{-st_d}}{(s\tau_p + 1)} \tag{13}$$

where K_p - is process gain, t_d - is delay time and τ_p - is time constant of process.
So, the minimum phase part of the process is determined as:

$$P_s^-(s) = \frac{K_p}{(s\tau_p + 1)} \tag{14}$$

The desired fractional filter configuration is given as:

$$F(s) = \frac{1}{(\sigma s^\gamma + 1)^2} \tag{15}$$

Now, the controller based on the IMC scheme is:

$$C_{imc}(s) = \frac{(s\tau_p + 1)}{K_p(\sigma s^\gamma + 1)^2} \tag{16}$$

The FFPID controller configuration obtained as a cascaded form of the fractional filter with PID term is:

$$C_f(s) = \frac{\left[\frac{(s\tau_p+1)}{K_p(\sigma s^\gamma+1)^2}\right]}{1 - \left[\frac{(s\tau_p+1)}{K_p(\sigma s^\gamma+1)^2}\right]\left[\frac{K_p e^{-st_d}}{(s\tau_p+1)}\right]} \tag{17}$$

$$C_f(s) = \frac{(s\tau_p + 1)}{K_p(\sigma s^\gamma + 1)^2 - K_p e^{-st_d}} \tag{18}$$

Finally,

$$C_f(s) = \left(\frac{1}{(\sigma s^\gamma + 1)^2 - e^{-st_d}}\right) \times \frac{1}{K_p}(1 + s\tau_p) \tag{19}$$

After comparison with (6), the parameters of PID controllers are:

$$K = \frac{1}{K_p}, \quad \tau_i = 0, \quad \tau_d = \tau_p \tag{20}$$

The parameters of the fractional filter are tuned by the trial and error method based on maximum sensitivity.
So, the Smith predictor part in designing the controller is shown in (21).

$$G_{sp}(s) = \frac{K_p e^{-st_d}(1 - e^{-s\tau})}{(s\tau_p + 1)} \tag{21}$$

By using (8), the final control structure is:

$$C(s) = \frac{s(\tau_p + 1)}{K_p\left[(\sigma s^\gamma + 1)^2 - e^{(-st_d+\tau)}\right]} \tag{22}$$

With the help of the time delay estimation method and the clock counter in the sensor-controller loop, it is possible to compute the delay in the information coming through the sensor. The estimated delay is then inserted into the Smith predictor to adjust for the delay attack and protect the process from the effects of the time delay attack. Also, the time delay in the process is added to the Smith predictor to avoid delay in the control action.

Consider a second order plus time delay (SOPTD) process:

$$P_s(s) = \frac{K_p e^{-st_d}}{(s\tau_1+1)(s\tau_2+1)} \tag{23}$$

where K_p - process gain, t_d - delay time, τ_1 and τ_2 - are the time constants of process.

The required fractional filter configuration is shown in (3), where $p = 2$.

So, the minimum phase part of the process is:

$$P_s^-(s) = \frac{K_p}{(s\tau_1+1)(s\tau_1+1)} \tag{24}$$

Now, the controller based on the IMC scheme is:

$$C_{imc}(s) = \frac{(s\tau_1+1)(s\tau_2+1)}{K_p(\sigma s^\gamma+1)^2} \tag{25}$$

The FFPID controller configuration obtained as a cascaded form of the fractional filter with PID term is:

$$C_f(s) = \frac{\left[\frac{(s\tau_1+1)(s\tau_2+1)}{K_p(\sigma s^\gamma+1)^2}\right]}{1-\left[\frac{(s\tau_1+1)(s\tau_2+1)}{K_p(\sigma s^\gamma+1)^2}\right]\left[\frac{K_p e^{-st_d}}{(s\tau_1+1)(s\tau_2+1)}\right]} \tag{26}$$

$$C_f(s) = \frac{(s\tau_1+1)(s\tau_2+1)}{K_p(\sigma s^\gamma+1)^2 - K_p e^{-st_d}} \tag{27}$$

Finally,

$$C_f(s) = \left[\frac{s}{(\sigma s^\gamma+1)^2 - e^{-st_d}}\right] \times \left[\frac{(\tau_1+\tau_2)}{K_p}\left(1+\frac{1}{(\tau_1+\tau_2)s}+\left(\frac{\tau_1\tau_2}{\tau_1+\tau_2}\right)s\right)\right] \tag{28}$$

After comparison with (6), parameters of PID controllers are:

$$K = \frac{(\tau_1+\tau_2)}{K_p}, \quad \tau_i = (\tau_1+\tau_2), \quad \tau_d = \left(\frac{\tau_1\tau_2}{\tau_1+\tau_2}\right) \tag{29}$$

Moreover, the Smith predictor part is presented in (30).

$$G_{sp}(s) = \frac{K_p e^{-st_d}(1-e^{-s\tau})}{(s\tau_1+1)(s\tau_2+1)} \tag{30}$$

By using (8), the final control structure is:

$$C(s) = \frac{\left[\tau_1\tau_2 s^2 + (\tau_1+\tau_2)s+1\right]}{K_p\left[(\sigma s^\gamma+1)^2 - e^{-s(t_d+\tau)}\right]} \tag{31}$$

V. Assessment of the Closed Loop Performance

The assessment of response of the closed-loop system has accomplished for a unit step alteration in reference input ($R(s)$) and a step alteration in disturbance ($D(s)$) of magnitude ($+0.5$). The performance of the proposed controller design is tested by using ISE, IAE, TV and M_s (maximum sensitivity), which is given below:

$$ISE = \int_0^\infty e_{rr}^2(t)dt \tag{32}$$

$$IAE = \int_0^\infty |e_{rr}(t)|dt \tag{33}$$

$$TV = \sum_{j=0}^{\infty} |u_{j+1} - u_j| \tag{34}$$

$$M_s = \max_{0\le\omega\le\infty}\left|\frac{1}{1+P_s(i\omega)C_f(i\omega)}\right| \tag{35}$$

VI. Robustness Assessment

In a real-world setting, there is no such thing as a flawless model. As a result, the efficiency of the designed controller should be tested in the presence of disturbances in the system model. So, the designed controller must be robust whenever there is a parametric uncertainty. The robust stability condition is given below [17].

$$P_m(j\omega)T(j\omega) < 1, for\ \ all\ \ \omega \in (-\infty,\infty) \tag{36}$$

where $T(j\omega) = \frac{C(j\omega)P(j\omega)}{1+C(j\omega)P(j\omega)}$ - is complementary sensitivity function.

And $P_m(j\omega) = \left|\frac{P(j\omega)-P_s(j\omega)}{P_s(j\omega)}\right|$ - is plant multiplicative unreliability bound.

For the robust analysis, the proposed design can be tested as per (37).

$$\|T(j\omega)\|_\infty < \frac{1}{\left|\left(\frac{\delta K_p}{K_p}+1\right)e^{-\delta t_d}-1\right|} \tag{37}$$

VII. Simulation Analysis

In this segment, the following two examples are presented for testing the effectiveness of the proposed controller in the presence of TDA.

Example 1: Consider the system represented in [18]:

$$P_s(s) = \frac{K_p e^{-st_d}}{s(s\tau_p+1)} \tag{38}$$

where gain of the servo motor is, $K_p = 21.721$, time constant is, $\tau_p = 0.147$ and the delay time is considered as $0.5s$.

After using the proposed mechanism, the tuned parameters of the controller are $K = 0.046$, $\tau_i = 0$, and $\tau_d = 0.147$. Also, the associated fractional filter term, which is mentioned in the (39), the parameters are $\sigma = 5.24$ and $\gamma = 1.01$, for the maximum sensitivity value $M_s = 1.2$. According to (6):

$$f(s) = \left(\frac{s}{(\sigma s^\gamma+1)^2 - e^{-0.5s}}\right) \tag{39}$$

Using the proposed method, the Smith predictor term is given as:

$$G_{sp}(s) = \frac{21.721e^{-0.5s}(1-e^{-10s})}{s(0.147s+1)} \tag{40}$$

For performance analysis, a step function with magnitude 1 for set-point observation and a step function of magnitude ($+0.5$) for disturbance rejection at time $100s$ are used. The closed loop outcome study is performed using the ISE, IAE and TV values listed in Table I, and the results have been observed for a fixed value of maximum sensitivity ($M_s = 1.2$). The servo and regulatory responses for the process mentioned above are shown in Fig. 5. Further, the control effort for the process is shown in Fig. 6, for a time delay attack of $10s$.

TABLE I

CRITERIA FOR EVALUATING PERFORMANCE AND ROBUSTNESS.

Method	Ms	Set-point			Disturbance		
		ISE	IAE	TV	ISE	IAE	TV
FFPID	1.2	30.86	57.14	0.0277	6.978	21.19	0.0104
Proposed	1.2	6.425	10.26	0.0066	1.606	5.092	0.0033

The magnitude response in Fig. 7, depicts the robust stability study for $+15\%$ uncertainty in delay time and gain of the system. By fulfilling the stability criterion in (37), it can be seen that the suggested model is robustly stable.

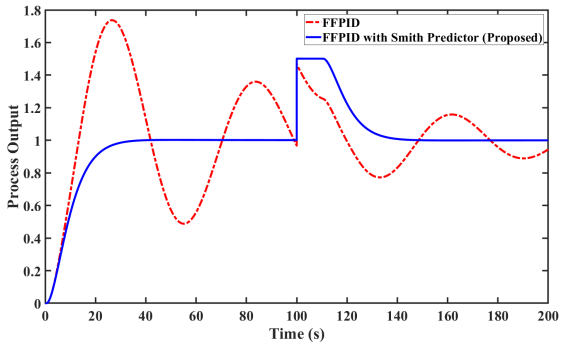

Fig. 5. Closed loop process output response of Example 1.

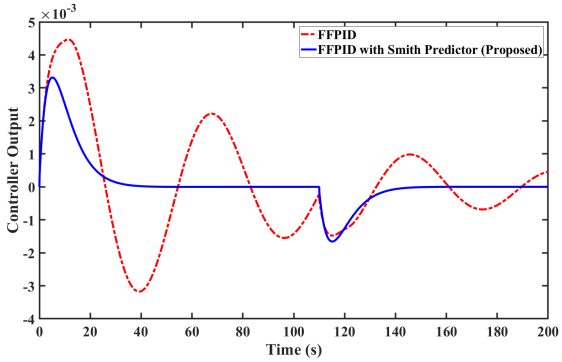

Fig. 6. Closed loop control effort response of Example 1.

From Table I, it is observable that all the outcome measurements of the proposed method are less than the normal FFPID. From the response, it is observed that the time delay which is inserted by the attacker is nullified through the suggested controller and provide a stable and quickly settled response with no oscillation.

Example 2: Suppose the higher-order process in [19] is represented as:

$$P_s(s) = \frac{1}{(s+1)(0.2s+1)(0.04s+1)(0.0008s+1)} \tag{41}$$

Using Skogestad's technique, SOPTD model is given in (42).

$$P_M(s) = \frac{1}{(s+1)(0.22s+1)} e^{-0.028s} \tag{42}$$

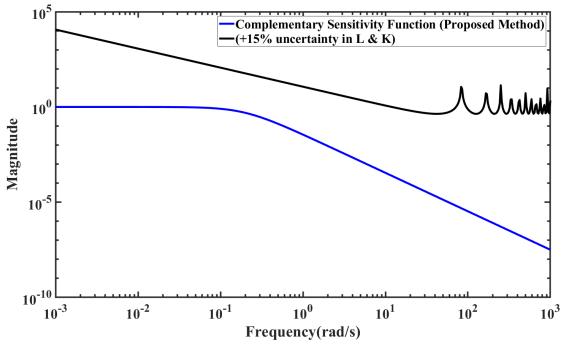

Fig. 7. Magnitude response for $+15\%$ unpredictability in t_d and K.

The controller parameters of the proposed technique are $K = 1.22$, $\tau_i = 1.22$ and $\tau_d = 0.1803$. Also the parameters of the fractional filter term (43) are $\sigma = 0.286$ and $\gamma = 1.01$ for $M_s = 1.2$. According to (6):

$$f(s) = \left(\frac{s}{(\sigma s^{\gamma}+1)^2 - e^{-0.028s}} \right) \tag{43}$$

The Smith predictor term, using the proposed method is:

$$G_{sp}(s) = \frac{e^{-0.028s}(1-e^{-2s})}{(s+1)(0.22s+1)} \tag{44}$$

The response of the closed loop is observed for set point tracking and disturbance rejection, i.e., applied after $50s$, for step input of magnitudes 1 and 0.5, respectively. Fig. 8, depicts the servo and regulatory responses for the aforementioned procedure and the control effort is shown by Fig. 9, for a time delay attack of $2s$ and $10s$. The responses show that the proposed technique provides a stable result even for $10s$ attack time, while a simple FFPID controller provides an unstable response at $2s$. The robust stability for $+15\%$ alteration in gain and delay time of the process is shown in Fig. 10, which proves the system's stability. From Table II, the supremacy of the proposed method is verified based on ISE, IAE and TV values which is less in comparison to the FFPID-based controller.

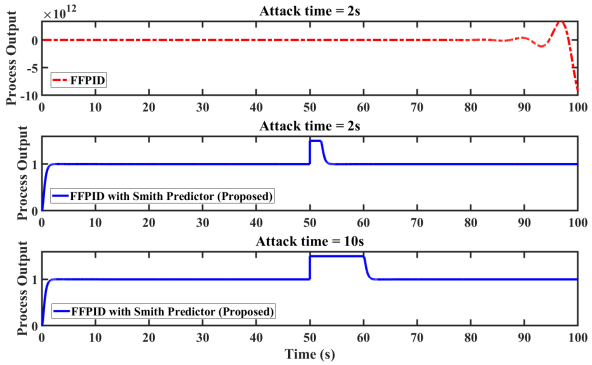

Fig. 8. Closed loop process output response of Example 2.

VIII. CONCLUSION

To overcome the effects of time delay attacks in the sensor-controller loop, a method has been developed for

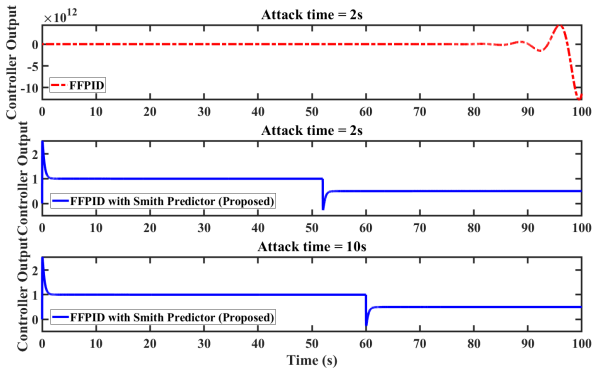

Fig. 9. Closed loop control effort response of Example 2.

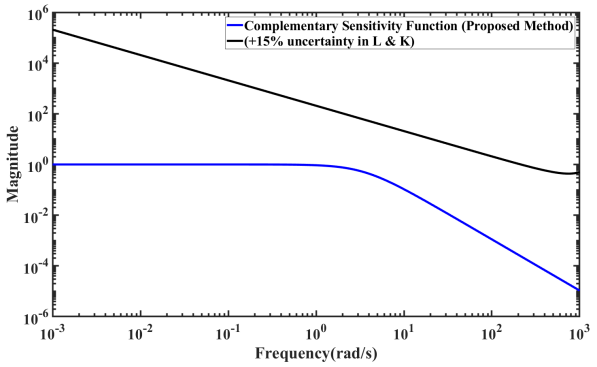

Fig. 10. Magnitude response for $+15\%$ unpredictability in t_d and K.

TABLE II

CRITERIA FOR EVALUATING PERFORMANCE AND ROBUSTNESS.

Method	Ms	Set-point			Disturbance		
		ISE	IAE	TV	ISE	IAE	TV
FFPID	1.2	9.2×10^4	691.9	1.7×10^3	14.99	8.291	26.61
Proposed	1.2	0.3624	0.58	4.0643	0.0906	0.287	2.03

designing the controller in this research work. The controller comprises a fractional filter PID controller with a Smith predictor for first-order integrating process with delay time and higher-order process. The designed controller can nullify the influence of time delay attack, which can be seen in the given examples mentioned above with delay attack time $10s$ for example 1 and $2s$ for example 2. The simulation results of the output responses of the proposed controller are settling fast with zero oscillations compared to the FFPID, which confirms the proposed method's supremacy. Error estimations also reveal the superiority of the proposed method with the minimal values of ISE, IAE and TV. Also, the proposed method required less control effort for performing the action. In the future, the proposed design will be tested for interconnected power system problems such as single-area and multi-area. Furthermore, the comparative study will be carried out with other control approaches such as Active Disturbance Rejection Control (ADRC) and H_∞.

REFERENCES

[1] C. -K. Zhang, L. Jiang, Q. H. Wu, Y. He and M. Wu, "Delay-Dependent Robust Load Frequency Control for Time Delay Power Systems," in IEEE Transactions on Power Systems, vol. 28, no. 3, pp. 2192-2201, Aug. 2013, doi: 10.1109/TPWRS.2012.2228281.

[2] M. S. Mahmoud, *Robust Control and Filtering for Time-Delay Systems.* New York, NY, USA: Marcel Dekker, 2000, pp. 75–101.

[3] A. Sargolzaei, K. K. Yen and M. N. Abdelghani, "Preventing Time-Delay Switch Attack on Load Frequency Control in Distributed Power Systems," in IEEE Transactions on Smart Grid, vol. 7, no. 2, pp. 1176-1185, March 2016, doi: 10.1109/TSG.2015.2503429.

[4] M. S. Mahmoud, M. M. Hamdan, and U. A. Baroudi, "Modeling and control of Cyber-Physical Systems subject to cyber attacks: A survey of recent advances and challenges," Neurocomputing, vol. 338, pp.101-115, Apr. 2019, https://doi.org/10.1016/j.neucom.2019.01.099.

[5] G. Wu, J. Sun, and J. Chen, "A survey on the security of cyber-physical systems," Control Theory and Technology, vol. 14, no. 1, pp. 2-10, Feb. 2016, doi: https://doi.org/10.1007/s11768-016-5123-9

[6] B. Chen, D. W. C. Ho, W. Zhang and L. Yu, "Distributed Dimensionality Reduction Fusion Estimation for Cyber-Physical Systems Under DoS Attacks," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 2, pp. 455-468, Feb. 2019, doi: 10.1109/TSMC.2017.2697450.

[7] Y. Yuan, H. Yuan, L. Guo, H. Yang and S. Sun, "Resilient Control of Networked Control System Under DoS Attacks: A Unified Game Approach," in IEEE Transactions on Industrial Informatics, vol. 12, no. 5, pp. 1786-1794, Oct. 2016, doi: 10.1109/TII.2016.2542208.

[8] Y. Wang, "Trust Quantification for Networked Cyber-Physical Systems," in IEEE Internet of Things Journal, vol. 5, no. 3, pp. 2055-2070, June 2018, doi: 10.1109/JIOT.2018.2822677.

[9] K. Rahimi, A. Parchure, V. Centeno and R. Broadwater, "Effect of communication Time-Delay attacks on the performance of Automatic Generation Control," 2015 North American Power Symposium (NAPS), 2015, pp. 1-6, doi: 10.1109/NAPS.2015.7335168.

[10] M. Wankhade and S. V. Kottur, "Security Facets of Cyber Physical System," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), 2020, pp. 359-363, doi: 10.1109/ICSSIT48917.2020.9214079.

[11] X. Lou et al., "Assessing and Mitigating Impact of Time Delay Attack: Case Studies for Power Grid Controls," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 1, pp. 141-155, Jan. 2020, doi: 10.1109/JSAC.2019.2951982.

[12] A. Sargolzaei, K. Yen and M. Abdelghani, "Delayed inputs attack on load frequency control in smart grid," ISGT 2014, 2014, pp. 1-5, doi: 10.1109/ISGT.2014.6816508.

[13] A. Sargolzaei, K. K. Yen, M. N. Abdelghani, S. Sargolzaei and B. Carbunar, "Resilient Design of Networked Control Systems Under Time Delay Switch Attacks, Application in Smart Grid," in IEEE Access, vol. 5, pp. 15901-15912, 2017, doi: 10.1109/ACCESS.2017.2731780.

[14] Lou, Xin, et al., "Assessing and mitigating impact of time delay attack: a case study for power grid frequency control." Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems. 2019, pp. 207-216, https://doi.org/10.1145/3302509.3311042.

[15] Saxena, S., Bhatia, S. and Gupta, R., "Cybersecurity Analysis of Load Frequency Control in Power Systems: A Survey". Designs, 5(3), p.52. 2021, https://doi.org/10.3390/designs5030052.

[16] Mohan, A.M., Meskin, N. and Mehrjerdi, H., "A comprehensive review of the cyber-attacks and cyber-security on load frequency control of power systems". Energies, 13(15), p.3860. 2020, https://doi.org/10.3390/en13153860.

[17] Kumar, V., Ranganayakulu, R., Uday Bhaskar Babu, G., "Analytical design of imc-based pid controller for non-minimum phase process with time delay". In: Control Applications in Modern Power Systems, pp. 499–511. Springer (2022), https://doi.org/10.1007/978-981-19-0193-5-39.

[18] Saxena, S. and Hote, Y.V., "Design and validation of fractional-order control scheme for DC servomotor via internal model control approach". IETE Technical Review, 36(1), pp.49-60, 2019, https://doi.org/10.1080/02564602.2017.1396935.

[19] Saxena, S. and Hote, Y.V., "Simple approach to design PID controller via internal model control". Arabian journal for science and engineering, 41(9), pp.3473-3489, Feb. 2016, doi: 10.1007/s13369-016-2027-4.