Analytical Series-PID controller design with Smith Predictor approach for analyzing and mitigating the Time Delay Cyber Attack (TDCA)

Vivek Kumar
Department of Electrical Engineering
Indian Institute of Technology, Roorkee
Uttarakhand, India
vivek_k1@ee.iitr.ac.in

Yogesh V. Hote
Department of Electrical Engineering
Indian Institute of Technology, Roorkee
Uttarakhand, India
yogesh.hote@ee.iitr.ac.in

2022 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES) | 978-1-6654-5566-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/PEDES56012.2022.10080153

***Abstract*—For a cyber-physical system (CPS_m), communication and control channels are the most crucial part, which is used for enhancing efficiency and providing a better response to the physical systems. However, these channels are also responsible for the vulnerability of cyber attacks and can create severe problems for physical systems. Among the different kinds of cyber attacks, this paper focuses on a particular cyber attack, i.e., a time delay cyber attack (TDCA), which can destabilize or disrupt the system. To handle such a problem, this article proposed a joint method consisting of (i) a Series Proportional Integral Derivative (series-PID) controller and (ii) Smith Predictor approach. The proposed method provides better performance and stable response, verified by an illustrative example. A comparative analysis has been done through simulation work, and performance criteria are based on the integral square error (ISE_e), integral absolute error (IAE_e), and total variations (TV_q).**

***Index Terms*—Time delay cyber attack (TDCA), Cyber-physical system, Performance, Communication, Stability**

I. Introduction

The effect of a significant and generic class of attacks which we term the time delay cyber attack on a CPS_m, that uses a closed-loop control system [1], [2], [3], can be assessed and mitigated in this study which is motivated by the numerous security issues. The attacker intentionally delays control or communication information delivery without interfering with the information. CPS_m control frequently has strict timing requirements; because of that, the attack can drastically degrade the system's performance and potentially result in serious safety accidents. Unlike information interfering, which requires breaking non-trivial encryption technology, the TDCA may be carried out very easily by exploiting hacked gateways to increase connection delay. As a result, it is a severe hazard that must be addressed immediately. However, the attack may be easily identified by synchronizing the clocks of cooperating CPS_m devices and then verifying packet timestamps [4]. Analyzing and minimizing the attack's effect in real-time is difficult due to the complexity of real-world CPS_m. This article suggested a series-PID controller with a smith predictor for minimizing the influence of the time delay cyber-attack. The smith predictor approach is used to detect the time delay in the communication channel and nullifies this time delay effect before reaching it to the controller.

For decades, because of the simple behavior in controller design, resistance to external uncertainty, and ease of tuning the parameters, the Proportional Integral Derivative (PID) control technique has played a significant role in industrial and research work. As the present era grows, PID parameter estimation procedures are challenging with demanding technical aspects for the complex nature of controlled processes. In the existing literature, there are several tuning formulae for PID controllers. The tuning approach based on the process response curves have presented by Ziegler and Nichols [5], Astrom and Hagglund [6], and Cohen and Coon [7]. Intellectual PID control approach [8], fuzzy-based PID control methodology [9], and neural network-based PID control methodology [10] have been used to improve PID control efficiency by merging it with some other sophisticated control systems. The study on the PID control issue has received much interest from the network science and control technologies fields so far [11]. Because of their straightforward physical application, series-PID controllers are commonly utilized in hydraulic control strategies and analog electronic circuits. The generalized structure of the series-PID is given below:

$$Q(s) = K_q \left(1 + \frac{1}{T_{iq}s}\right)(1 + T_{dq}s); \quad K_q, T_{iq}, T_{dq} > 0 \quad (1)$$

Here, K_q, T_{iq}, and T_{dq} represent the controller's gain, integral's time constant, and derivative's time constant of the controller, respectively. Due to the derivative part, noises will add in the high-frequency region, so a low pass filter (LPF) is required to avoid those noises. So the modified structure of the series-PID controller is represented as [12]:

$$Q(s) = K_q \left(1 + \frac{1}{T_{iq}s}\right)\left(\frac{1 + T_{dq}s}{1 + \delta T_{dq}s}\right); \quad 0.01 \leq \delta \geq 0.2 \quad (2)$$

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

978-1-6654-5566-4/22/$31.00 ©2022 IEEE

A. Tuning of the controller parameters

This paper uses a model-based tuning rule for tuning the parameters of the series-PID controller. For the arrangement of the value of T_{iq}, and T_{dq} the pole placement-based method has been used [13]. To get the controller's gain on account of better performance, the D-decomposition method is used for a given stability range [14]. The Pole placement approach is based on the settings of the root locus so that the modified root locus version of the closed-loop process passes through the relevant pole locations. Assume the relevant poles of closed-loop process are: $s_r = -x \pm jy$; $(x, y > 0)$. If the location of the relevant poles are not present on the root locus, then an amount of phase needs to be added to the controller to get the desired phase angle criterion. So the required angle can be provided by: angle$(Q(s_r))$ + angle$(P_p(s_r)) = -180°$. Here angle$(P_p(s_r))$ is known as process's angle and angle$(Q(s_r))$ is known as controller's angle at relevant pole location (s_r). So total angle contributed by series-PID can be represented by [13]:

$$angle(Q(s_r)) = angle\left(1 + \frac{1}{T_{iq}s_r}\right) + angle\left(\frac{1 + T_{dq}s_r}{1 + \delta T_{dq}s_r}\right) \tag{3}$$

The series-PID controller's angle is affected by the variables T_{iq}, T_{dq}, and δ. The derivative section of the controller with an LPF is placed in the feedback loop so that the δ effect is negligible on the performance and the controller, so assume δ is persistent. The placement of δ in the feedback path influences the measurement disturbances. So, for the allowable value of measurement disturbances, select the δ value reasonably [15]. Furthermore, two more parameters need to be calculated. Therefore, we consider a second-order time-delay system (SOPTD) i.e.

$$P_p(s) = \frac{K_p e^{-\alpha s}}{(T_{p1}s + 1)(T_{p2}s + 1)}; \quad T_{p1} \geq T_{p2} \tag{4}$$

By assuming the less significant pole of the system, $T_{p2} = T_{dq}$, the numerator part (zeros of the controller) can be wiped out. So, with the help of first part of controller $\left[angle\left(1 + \frac{1}{T_{iq}s_r}\right)\right]$; Integral's time constant (T_{iq}) can be calculated. From Fig. 1 [13]:

$$phase\left(1 + \frac{1}{T_{iq}s_r}\right) = \theta_{zz} - \theta_{pp}; \tag{5}$$

$$\text{where, } \theta_{pp} = 180 - tan^{-1}\left(\frac{y}{x}\right) \tag{6}$$

So, the final value can be determined by:

$$T_{iq} = \frac{1}{x + \frac{y}{tan(\theta_{zz})}} \tag{7}$$

B. Time delay cyber attack (TDCA)

TDCA is a type of Denial-of-service (DoS) attack. Contrary to DoS attacks, the connection between the physical system and the control center is not entirely cut off. Instead, the intrusion will cause a delay in the signal that is sent over the infected communication route. The sensors collect data on the condition of the process and transmit the data to the controller, and the controller utilizes these data to make control choices. The controller provides the appropriate actions to the actuators, who carry them out and adjust the process's state correspondingly, which helps to establish the closed loop. Because of that, communication lines are much more prone to attack than controllers, perhaps more likely to be targeted. The introduction of time delay in communication lines that carry sensor information to the central controller or control information to the actuators is known as a TDCA. A time-delay cyber attack occurs when intruders introduce delays into a control system. Even if the number of infected channels is less, intentional delays might create an unstable system. Because the TDCA happens in a feedback loop system, it has the potential to create instability or otherwise distort the system's operational state, which is harmful to the system. Some existing work has been done in the past for detection and mitigation of the TDCA [16], [17].

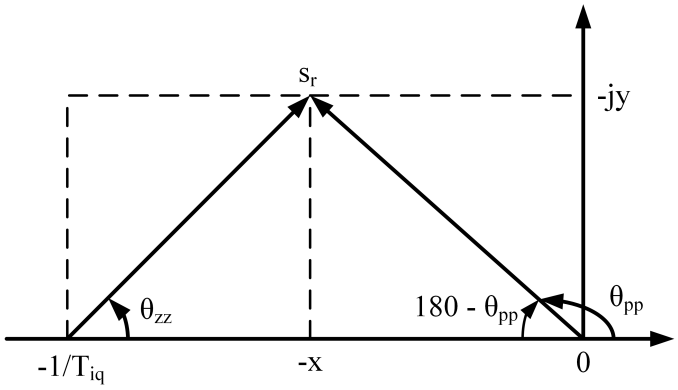

Fig. 1. Pole-zero figure of the first part of controller [13].

In this article, we proposed a smith predictor with the series-PID controller to mitigate the effect of the time delay, i.e., introduced by the attacker. Smith predictor nullifies the delay before reaching to the controller, whereas series-PID will provide better time domain specifications.

II. Mathematical design of proposed approach

To mitigate the impact of time delay cyber attack, the proposed controller structure is shown in Fig. 2. With the help of the smith predictor approach along with the series-PID controller, a time delay, which is introduced by the attacker in the form of a measurement attack or time delay cyber attack, in the communication path (sensor-controller channel), will be detected and minimized by the proposed methodology. According to Fig. 2, when the attacker has performed a time delay cyber attack, then the neutralization of the delay time attack has been done by the proposed methodology, so that $Y_5(s) = Y_1(s)$ must be satisfied.

From the proposed structure in Fig. 2:

$$Y(s) = P_p(s) * U(s) \tag{8}$$

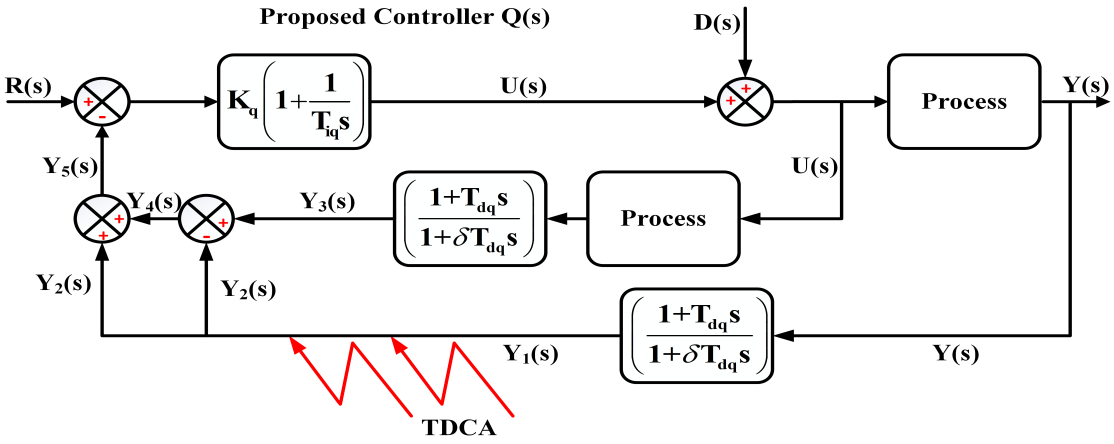

Fig. 2. Block diagram of proposed controller structure.

Where $P_p(s)$ is transfer function of process, and $U(s)$ is controller's outcome. Then the feedback output of the structure is:

$$Y_1(s) = P_p(s) * U(s) * \left(\frac{1+T_{dq}s}{1+\delta T_{dq}s}\right) \tag{9}$$

So, after the TDCA of τ_t sec.:

$$Y_2(s) = Y_1(s) * e^{-\tau_t s} \tag{10}$$

According to the TDCA, the smith predictor output is:

$$Y_3(s) = P_p(s) * U(s) * \left(\frac{1+T_{dq}s}{1+\delta T_{dq}s}\right) \tag{11}$$

$$Y_4(s) = P_p(s) * U(s) * \left(\frac{1+T_{dq}s}{1+\delta T_{dq}s}\right) * \left[1-e^{-\tau_t s}\right] \tag{12}$$

So, after nullifying the time delay cyber attack (TDCA), the final feedback signal is:

$$Y_5(s) = Y_2(s) + Y_4(s) = P_p(s) * U(s) * \left(\frac{1+T_{dq}s}{1+\delta T_{dq}s}\right) \tag{13}$$

Finally, it can be observable from the (13), that $Y_5(s) = Y_1(s)$ and time delay attack has mitigated.

III. Performance Evaluation of Closed-Loop System

The outcomes have been estimated for the step-change of unity in set point $R(s)$ and disturbance $D(s)$. The assessment of response is based on the two kinds of errors (ISE_e and IAE_e) and (TV_q) for a particular value of maximum sensitivity (M_s), i.e., (i) Integral square error (ISE_e), (ii) Integral absolute error (IAE_e), and Total variations (TV_q). They are represented as follows:

$$ISE_e = \int_0^\infty e^2(t)dt \tag{14}$$

$$IAE_e = \int_0^\infty |e(t)|dt; \tag{15}$$

$$TV_q = \sum_{i=0}^{\infty} |u_{i+1} - u_i| \tag{16}$$

$$M_s = \max_{0\le\omega\le\infty} \left|\frac{1}{1+P_p(j\omega)Q(j\omega)}\right| \tag{17}$$

IV. Robustness Analysis

In the modern era, every model has some imperfections. So the efficiency of the proposed controller must be analyzed in the presence of disturbances and noises in the model of the system. Due to these reasons, the proposed controller should be robust even if uncertain parameters exist. The condition of robust stability is given below [18]:

$$L_m(j\omega)\eta_{cs}(j\omega) < 1, for\ \ all\ \ \omega \in (-\infty, \infty) \tag{18}$$

where $\eta_{cs}(j\omega) = \frac{C(j\omega)P_p(j\omega)}{1+C(j\omega)P_p(j\omega)}$ - is the complementary sensitivity equation.
And $L_m(j\omega) = \left|\frac{P_p(j\omega)-P(j\omega)}{P(j\omega)}\right|$ - is model multiplicative uncertainty bound, $P_p(j\omega)$ is the nominal model of real process and $P(j\omega)$ is the actual model of the process.
For the robust analysis, the proposed design can be analyzed as per (19).

$$\|\eta_{cs}(j\omega)\|_\infty < \frac{1}{\left|\left(\frac{\delta K_p}{K_p}+1\right)-1\right|} \tag{19}$$

V. Simulation and Outcomes

This section presents the simulation work for the proposed methodology with an example by MATLAB-Simulink (R2022a).
Consider the process given as [13]:

$$P_p(s) = \frac{(0.17s+1)^2}{s(s+1)^2(0.028s+1)}$$

To get the improved performance and better-tuned parameters of the controller, the significant poles must be located at $s_r = -0.506 \pm j0.669$, according to the pole placement approach so that the root-locus of the process passes through the relevant pole (s_r). For assuring the phase criterion at pole

location (s_r), the PID controller should provide an additional phase of 41.07°. To neglect the insignificant pole with zeros of PID controller, consider $T_{dq} = 1.33$. So the angle of first part of the controller according to the eq. (3) is -28.21°, and second part is 69.28° at the constant value of $\delta = 0.01$. By using the proposed mechanism the remaining adjusted parameters of controller are $K_q = 1.84$ and $T_{iq} = 2.493$.

After taking the unit step set point and step disturbance of magnitude 1, at time $t = 20sec$, and observing the response as mentioned in Fig. 3. After considering the time delay cyber attack of $10sec$ as a measurement attack or communication attack, the S. Tavakoli method provides an unstable response, as shown in (a) part of Fig. 3. At the same time, the proposed controller completely neglects the TDCA and provides a stable response with better set-point tracking and disturbance rejection, as shown in (b) part of Fig. 3. Also, it can be verified by the performance evaluations, reported in Table I. After the TDCA, it can be observed that the proposed method provides less values of errors and control effort than the S. Tavakoli method after TDCA.

The magnitude response shown in Fig. 4 describes the robustness analysis for $+50\%$ uncertainty in the gain of the process model. By satisfying the stability condition as mentioned in (19), it can be observed from the response that the proposed controller is robustly stable.

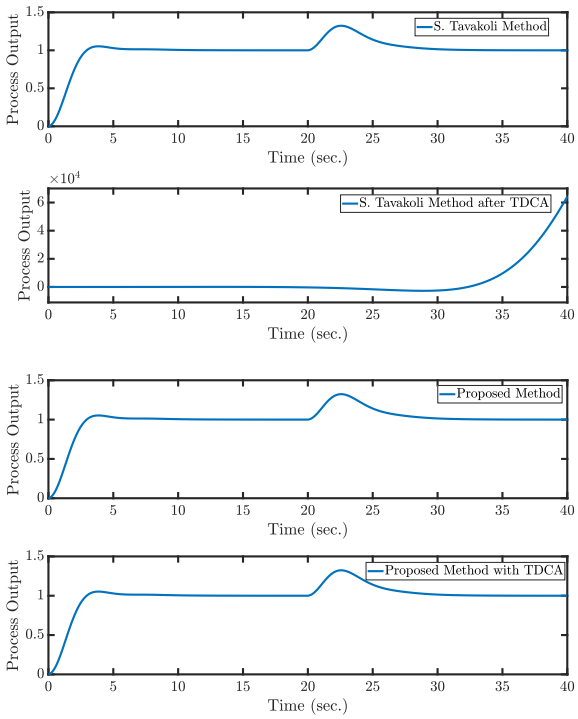

Fig. 3. (a) Output response of S. Tavakoli method (b) Output response of proposed method

VI. Conclusion

This paper has suggested a method to minimize the time delay cyber attack (TDCA) or measurement attack in the communication loop (sensor-controller channel). The proposed controller mainly consists of a series-PID controller with a smith predictor approach for a higher-order process model. The proposed controller method has neutralized the effect of TDCA, which can be verified by the response for a time delay attack of $10sec$. The simulation results of the output response of the proposed method are settling quickly with less amount of overshoot as shown in Fig. 3 (b). Also, the simulation results reveal the supremacy of the proposed method, which provides a stable response with less values of the errors (ISE_e, IAE_e) and control effort (TV_q). In the future, the proposed design will be tested through the real-time control prototyping system. Also, the proposed method will be implemented on micro-grid in the future.

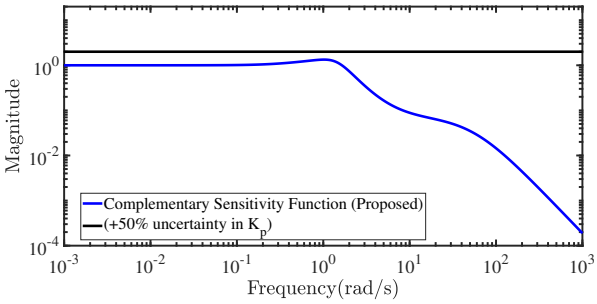

Fig. 4. Robustness Analysis for $+50\%$ uncertainty in K_p

Acknowledgment

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

References

[1] Chen, B., Mashayekh, S., Butler-Purry K. L., and Kundur, D., 2013. Impact of cyber attacks on transient stability of smart grids with voltage support devices. IEEE Power & Energy Society General Meeting, pp. 1-5, doi: 10.1109/PESMG.2013.6672740.

[2] Cao, X., Cheng, P., Chen, J., Ge, S. S., Cheng Y., and Sun, Y., 2014. Cognitive Radio Based State Estimation in Cyber-Physical Systems. IEEE Journal on Selected Areas in Communications, vol. 32, no. 3, pp. 489-502, doi: 10.1109/JSAC.2014.1403002.

[3] Farraj, A., Hammad, E. and Kundur, D., 2016. A cyber-physical control framework for transient stability in smart grids. IEEE Transactions on Smart Grid, 9(2), pp.1205-1215.

[4] Viswanathan, S., Tan, R. and Yau, D.K., 2018. Exploiting electrical grid for accurate and secure clock synchronization. ACM Transactions on Sensor Networks (TOSN), 14(2), pp.1-32.

[5] Ziegler, J.G. and Nichols, N.B., 1942. Optimum settings for automatic controllers. trans. ASME, 64(11).

[6] Åström, K.J. and Hägglund, T., 1995. PID controllers: theory, design, and tuning. ISA-The Instrumentation, Systems and Automation Society.

[7] Cohen, G., 1953. Theoretical consideration of retarded control. Trans. Asme, 75, pp.827-834.

[8] Kim, D.H. and Cho, J.H., 2006. A biologically inspired intelligent PID controller tuning for AVR systems. International Journal of Control, Automation, and Systems, 4(5), pp.624-636.

[9] Carvajal, J., Chen, G. and Ogmen, H., 2000. Fuzzy PID controller: Design, performance evaluation, and stability analysis. Information sciences, 123(3-4), pp.249-270.

TABLE I
CRITERIA FOR EVALUATING PERFORMANCE

Method	M_s	Set-Point$_q$			Disturbance$_q$		
		ISE$_e$	IAE$_e$	TV$_q$	ISE$_e$	IAE$_e$	TV$_q$
S.Tavakoli Method	1.25	0.46	1.095	2.47	0.41	1.35	1.58
S.Tavakoli Method with TDCA	1.25	4.3×10^7	2.1×10^4	1.9×10^4	297	46.4	51.9
Proposed Method with TDCA	1.25	0.46	1.095	2.47	0.41	1.35	1.58

[10] Cong, S., and Liang, Y., 2009. PID-Like Neural Network Nonlinear Adaptive Control for Uncertain Multivariable Motion Control Systems. IEEE Transactions on Industrial Electronics, vol. 56, no. 10, pp. 3872-3879, doi: 10.1109/TIE.2009.2018433.

[11] Kiam Heong Ang, Chong G., and Yun Li, 2005. PID control system analysis, design, and technology. IEEE Transactions on Control Systems Technology, vol. 13, no. 4, pp. 559-576, doi: 10.1109/TCST.2005.847331.

[12] Vilanova, R. and Visioli, A., 2012. PID control in the third millennium. London: Springer.

[13] Tavakoli, S. and Safaei, M., 2018. Analytical PID control design in time domain with performance-robustness trade-off. Electronics letters, 54(13), pp.815-817.

[14] Le, B.N., Wang, Q.G. and Lee, T.H., 2015. Development of D-decomposition method for computing stabilizing gain ranges for general delay systems. Journal of Process Control, 25, pp.94-104.

[15] O'dwyer, A., 2009. Handbook of PI and PID controller tuning rules. World Scientific.

[16] Saxena, S., Bhatia, S. and Gupta, R., 2021. Cybersecurity Analysis of Load Frequency Control in Power Systems: A Survey. Designs, 5(3), p.52.

[17] Mohan, A.M., Meskin, N. and Mehrjerdi, H., 2020. A comprehensive review of the cyber-attacks and cyber-security on load frequency control of power systems. Energies, 13(15), p.3860.

[18] Kumar, V., Ranganayakulu, R. and Uday Bhaskar Babu, G., 2022. 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, https://doi.org/10.1007/978-981-19-0193-5-39.