2023 IEEE 64th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS) | 979-8-3503-7029-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ITMS59786.2023.10317694

Resilient Control for Cyber-Physical Systems Against Denial-of-Service Cyber Attacks Using Kharitonov's Theorem

HamidReza Chavoshi
K. N. Toosi University of Technology
Tehran, Iran
hr.chavoshi@email.kntu.ac.ir

Ali Khoshlahjeh Sedgh
K. N. Toosi University of Technology
Tehran, Iran
khoshlahjehali@email.kntu.ac.ir

Hamid Khaloozadeh
Industrial Control Center of Excellence, Systems and Control Engineering
K. N. Toosi University of Technology
Tehran, Iran
h_khaloozadeh@kntu.ac.ir

***Abstract*— Cyber-physical systems (CPS) and networked control systems (NCS) integrate control systems with modern information technologies. Alongside the benefits of these control systems, there has been a growing concern regarding the security of critical infrastructures that use these technologies. Communication channels in a CPS are susceptible to various cyber-attacks, such as Denial-of-Service (DoS) attacks, which lead to severe time delays, missed data, control performance degradation, and instability. In this article, a conservative model has been considered for the system when a DoS attack occurs, which makes it possible to design a robust PI controller based on Kharitonov's theorem for mitigating the effects of DoS attacks. Then, to illustrate the effectiveness of the proposed robust PI controller for reducing DoS attack effects, another PI controller tuned by the Ziegler-Nichols method has been designed, and the performance of these two PI controllers compared by practical implementation on a CPS (liquid-level networked control system). The results show that the robust PI controller based on Kharitonov's theorem performs better than the PI controller tuned by the Ziegler-Nichols method to mitigate the influences of DoS attacks on the behavior of the CPS.**

Keywords*— *Cyber-physical systems, Denial-of-Service attack, Kharitonov's theorem, PI controller, Resilient control.

I. INTRODUCTION

Modern society has increasingly depended on computers, digital systems, and automation. Meanwhile, some individuals and groups have exploited these technologies in criminal ways, such as cyber-attacks. In order to achieve different objectives, these attacks aim to compromise the security of these systems. Therefore, it is essential to ensure cybersecurity. A potential crisis can affect any government that operates its infrastructures with Cyber-Physical Systems (CPS) and Network Control Systems (NCS). In order to safeguard sensitive information, critical industries, and vital infrastructure, cybersecurity measures must be implemented across various sectors of society.[1]

Physical processes and objects are integrated with sensing, computation, control, and networking in a CPS. It enables data collected in the physical world to be analyzed in the virtual world to affect the course of the physical world. In addition to real-time monitoring and global optimization of systems, a CPS provides integration, sharing, and collaboration of information. So, CPSs help the efficiency of operations, reduce costs, and optimize the performance of the system.[2] There are some security risks associated with CPS despite their many advantages. CPS is vulnerable to cyber-attacks due to its reliance on communication networks. CPS communication networks suffer from multiple security weaknesses, including Denial-of-Service (DoS) attacks, False Data Injection (FDI), and Man-in-the-Middle (MITM) attacks.[1-3]

This article explores the effects of DoS attacks on a CPS and their mitigation. By disrupting the CPS communication network, DoS attacks prevent control and measurement data packets from being delivered. Performance issues can arise when CPSs are subjected to DoS attacks.[4] A DoS attack can be launched by jamming communication channels, compromising devices to prevent them from sending data, and flooding the network.[5] DoS attacks can be classified into weak or strong, depending on their severity level. In weak attacks, the controller and plant network links are slowed down slightly by DoS attacks. The result is additional packet loss and time delay. A strong attack occurs when DoS attacks shut down the communication network.[6]

Robust control is used to mitigate weak DoS attacks in this paper by considering the effects of DoS attacks as a parametric uncertainty. Robust control minimizes the effects of uncertainty in system behavior. Robust stability and robust performance conditions require modeling uncertainty and knowing its boundaries. There are several robust control methods. Kharitonov's theorem, μ synthesis, and H_∞ control are the most commonly known.[7]

This article uses a robust PI controller based on Kharitonov's theorem to mitigate DoS attack effects on system behavior, similar to [8,9]. DoS attacks interrupt the communication network of CPS. This interruption leads to the late usage of the control signal and missed sensor data. In this paper, these effects of weak DoS attacks have been considered as time delay (like a parametric uncertainty). With this assumption, a robust PI controller is proposed

using Kharitonov's theorem that is resilient to the DoS attacks and will reduce the effects of DoS attacks on system behavior. Then, to verify the effectiveness of the proposed robust PI controller, another PI controller is tuned by the Ziegler-Nichols method, and the performance of these two designed controllers is compared by experimental implementation on a CPS.

II. System Introduction

A. System Specifications

It is possible to consider the employed system as a CPS. The physical part of the system consists of a liquid-level control plant constructed of a cylindrical tank measuring 40 cm in height and 4.5 cm in radius. The process also includes a pump that transfers the liquid to the tank at a variable rate based on the input voltage of 0.2 V to 3 V. An adjustable valve allows the liquid to be drained from the tank at an appropriate rate. In order to communicate between the liquid-level control system and its data logger, a physical interface panel is provided. Communication between the data logger and the computer is achieved through a Wi-Fi module. Four analog-to-digital converters (ADC), two digital-to-analog converters (DAC), eight digital inputs, and eight digital outputs are provided with the data logger. These parts of the system are shown in Fig. 1.

Fig. 1. The system cylindrical tank, interface panel and data logger.

The liquid level inside the tank is measured by a 5 kg load cell. This sensor generates a voltage signal by converting the force exerted by the liquid due to its weight. The sensor voltage output also increases in response to an increase in liquid level. A range between 0 and 10 volts is available at the output of the sensor.

In the control loop, analog outputs from the load cell are converted into digital values using an analog-to-digital converter (ADC). Then, with the help of a Wi-Fi network, these digital values are transmitted to a computer. Once the desired target value has been applied to the system, the computed control signal is transmitted back to the data logger through the same Wi-Fi network. Pump activation is achieved by converting the digital control signal into analog values using a digital-to-analog converter (DAC). A real-time synchronization block facilitates real-time execution of the intended control algorithms in MATLAB/Simulink. Fig. 2 illustrates the system overview and the DoS attack point.

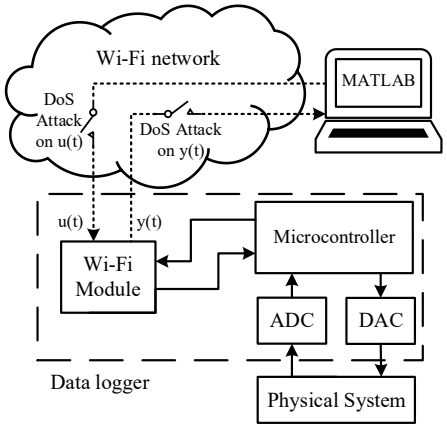

Fig. 2. System overview and the part where the DoS attack occurs.

B. System Model

The system model is needed to design the desired controllers. This system has been identified in [10] with a Second-Order Plus Time-Delay (SOPTD) model with sample time Ts=0.2 seconds.

$$G_d(z^{-1}) = \frac{0.03217 z^{-5}}{1 - 0.9 z^{-1} - 0.09 z^{-2}} \tag{1}$$

A single-tank liquid-level control system generally exhibits the characteristics of a first-order control system. Nevertheless, the limited output flow rate of the system caused it to behave more like an integrator. Therefore, an additional pole is incorporated into the system model to improve its alignment with actual system dynamics. The model also considers delays caused by the inherent characteristics of the system, such as the delay caused by pipes connecting the pump to the tank and the delay caused by the wireless connection between the computer and the data logger. [10]

III. PI Controllers Design

A. Kharitonov's Theorem

This paper used Kharitonov's theorem to design a robust controller for mitigating DoS attacks. Defining an interval polynomial is the first step in applying Kharitonov's theorem. An interval polynomial can be described as[11]

$$\begin{aligned} P(s,u) &= u_0 + u_1 s + u_2 s^2 + \cdots + u_n s^n \\ u_i &\in \left[\underline{u_i}, \overline{u_i}\right] \quad \forall i \\ 0 &\notin \left[\underline{u_n}, \overline{u_n}\right] \end{aligned} \tag{2}$$

If four Kharitonov's polynomials of an invariant degree family of an interval polynomial *P(s,u)* are stable, then that family of polynomials is robustly stable. It is important to note that the four Kharitonov's polynomials related to the interval polynomial *P(s,u)* are as follows[11]

$$\begin{aligned} K_1(s) &= \underline{u_0} + \underline{u_1} s + \overline{u_2} s^2 + \overline{u_3} s^3 + \underline{u_4} s^4 + \underline{u_5} s^5 + \overline{u_6} s^6 + \cdots \\ K_2(s) &= \overline{u_0} + \overline{u_1} s + \underline{u_2} s^2 + \underline{u_3} s^3 + \overline{u_4} s^4 + \overline{u_5} s^5 + \underline{u_6} s^6 + \cdots \\ K_3(s) &= \overline{u_0} + \underline{u_1} s + \underline{u_2} s^2 + \overline{u_3} s^3 + \overline{u_4} s^4 + \underline{u_5} s^5 + \underline{u_6} s^6 + \cdots \\ K_4(s) &= \underline{u_0} + \overline{u_1} s + \overline{u_2} s^2 + \underline{u_3} s^3 + \underline{u_4} s^4 + \overline{u_5} s^5 + \overline{u_6} s^6 + \cdots \end{aligned} \tag{3}$$

B. *Robust PI Controller Design Using Kharitonov's Theorem*

PI controllers have been chosen for simplicity. For applying Kharitonov's theorem, first, the continuous transfer function of the system is needed. So, by considering (1) the continuous model of the system using Tustin's method and the first-order Pade approximation is as follows.

$$G_c(s)=\frac{-0.01777s^3-0.3199s^2-1.066s+3.555}{s^3+14.04s^2+24.64s+1.105} \tag{4}$$

Considering weak DoS attack interruptions as time delay with a maximum length of 7 seconds, the total delay of the model will be 8 seconds and lead (1) to

$$G_{d-Max-DoS}(z^{-1})=\frac{0.03217z^{-40}}{1-0.9z^{-1}-0.09z^{-2}} \tag{5}$$

Therefore, the continuous transfer function (5) using the Tustin's method and the first-order Pade approximation can be calculated as

$$G_{Max\_DoS}(s)=\frac{-0.01777s^3-0.351s^2-1.688s+0.4443}{s^3+12.29s^2+3.564s+0.1381} \tag{6}$$

Now consider a system interval transfer function as

$$G(s)=\frac{b_3s^3+b_2s^2+b_1s+b_0}{a_3s^3+a_2s^2+a_1s+a_0} \tag{7}$$

Equations (4) and (6) transfer functions specify the ranges of open-loop system parameters for (7) interval transfer function, as shown in Table I.

TABLE I. UPPER AND LOWER LIMITS OF OPEN-LOOP SYSTEM TRANSFER FUNCTION PARAMETERS

Open-loop Transfer Function Parameters		**Parameter Limits**	
		Minimum	***Maximum***
Numerator	b_3	-0.01777	-0.01777
	b_2	-0.351	-0.3199
	b_1	-1.688	-1.066
	b_0	0.4443	3.555
Denominator	a_3	1	1
	a_2	12.29	14.04
	a_1	3.564	24.64
	a_0	0.1381	1.105

The closed-loop transfer function is obtained from

$$G_{cl}(s)=\frac{G(s)C(s)}{1+G(s)C(s)}=\frac{\frac{b_3s^3+b_2s^2+b_1s+b_0}{a_3s^3+a_2s^2+a_1s+a_0}\times\left(k_p+\frac{k_i}{s}\right)}{1+\frac{b_3s^3+b_2s^2+b_1s+b_0}{a_3s^3+a_2s^2+a_1s+a_0}\times\left(k_p+\frac{k_i}{s}\right)}$$
$$=\frac{b_3k_ps^4+(b_2k_p+b_3k_i)s^3+(b_1k_p+b_2k_i)s^2+(b_0k_p+b_1k_i)s+b_0k_i}{(b_3k_p+a_3)s^4+(b_2k_p+b_3k_i+a_2)s^3+(b_1k_p+b_2k_i+a_1)s^2+(b_0k_p+b_1k_i+a_0)s+b_0k_i} \tag{8}$$

where the denominator is our interval polynomial. k_p and k_i are design parameters and Based on Table I, the minimum and maximum values of interval polynomial coefficients are shown in Table II.

TABLE II. INTERVAL POLYNOMIAL COEFFICIENTS

Closed-loop Denominator Parameters		**Parameter Limits**	
		Minimum	***Maximum***
(Coeff)s^i	s^4	-0.01777k_p+1	-0.01777k_p+1
	s^3	-0.351k_p-0.01777k_i+12.29	-0.3199k_p-0.01777k_i+14.04
	s^2	-1.688k_p-0.351k_i+3.564	-1.066k_p-0.3199k_i+24.64
	s^1	0.4443k_p-1.688k_i+0.1381	3.555k_p-1.066k_i+1.105
	s^0	0.4443k_i	3.555k_i

So, four Kharitonov's polynomials are formed as follows.

$$\begin{aligned}
K_1(s)&=0.4443k_i+(0.4443k_p-1.688k_i+0.1381)s+(-1.066k_p-0.3199k_i+24.64)s^2\\
&+(-0.3199k_p-0.01777k_i+14.04)s^3+(-0.01777k_p+1)s^4\\
K_2(s)&=3.555k_i+(3.555k_p-1.066k_i+1.105)s+(-1.688k_p-0.351k_i+3.564)s^2\\
&+(-0.351k_p-0.01777k_i+12.29)s^3+(-0.01777k_p+1)s^4\\
K_3(s)&=3.555k_i+(0.4443k_p-1.688k_i+0.1381)s+(-1.688k_p-0.351k_i+3.564)s^2\\
&+(-0.3199k_p-0.01777k_i+14.04)s^3+(-0.01777k_p+1)s^4\\
K_4(s)&=0.4443k_i+(3.555k_p-1.066k_i+1.105)s+(-1.066k_p-0.3199k_i+24.64)s^2\\
&+(-0.351k_p-0.01777k_i+12.29)s^3+(-0.01777k_p+1)s^4
\end{aligned} \tag{9}$$

For obtaining the acceptable values of k_p and k_i, four Kharitonov's polynomials must be stable. A nested loop is used to determine the acceptable region of k_p and k_i. The design procedure pseudo-code is as follows.

1: **Input:** K_1, K_2, K_3, and K_4
2: **for** $k_{i,min}$: $k_{i,max}$ **do**
3: **for** $k_{p,min}$: $k_{p,max}$ **do**
4: **if** K_1, K_2, K_3, and K_4 are Hurwitz. **then**
5: put the k_p and k_i in the acceptable set.
6: **end if**
7: **end for**
8: **end for**
9: **Output:** acceptable region of k_p and k_i

So, the calculated acceptable region of k_p and k_i of the PI controller to robustly stabilize the interval polynomial and mitigate DoS attacks is shown in Fig. 3.

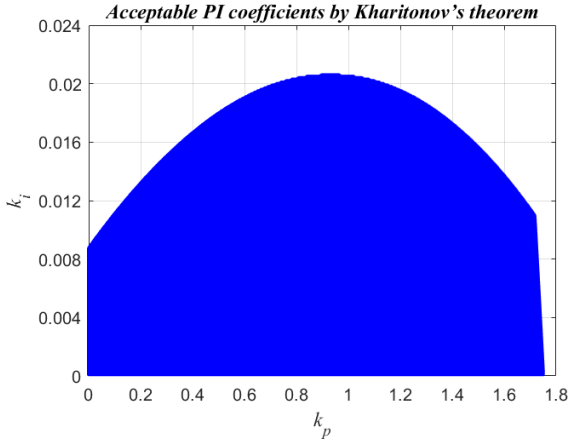

Fig. 3. Acceptable region of k_p and k_i to robustly stabilize the interval polynomial.

By fine-tuning of the robust PI controller coefficients among the acceptable values, k_p = 1 and k_i = 0.01 were selected, so

$$C_{KT}(z) = k_p + k_i \frac{Ts}{z-1} = 1 + 0.01\frac{0.2}{z-1} = \frac{z-0.998}{z-1} \quad (10)$$

C. Ziegler-Nichols Method PI Controller Coefficients

In the next section, the proposed robust PI controller will be evaluated by implementing it on the CPS, so Another PI controller is needed to compare results and verify the effectiveness of the proposed robust PI controller. Therefore, k_p = 6.5 and k_i = 0.3 were chosen by fine-tuning the Ziegler-Nichols PI controller design method, so

$$C_{ZN}(z) = k_p + k_i \frac{Ts}{z-1} = 6.5 + 0.3\frac{0.2}{z-1} = \frac{6.5z-6.44}{z-1} \quad (11)$$

IV. EXPERIMENT DESIGN AND RESULTS

A. Experiment Design and Assumptions

This section examines the performance of the proposed PI controllers on the CPS. This evaluation considered four scenarios: normal operation, DoS attack on the control signal, DoS attack on the sensor signal, and DoS attack on both. The performance of the controllers is extracted and compared in each scenario with practical implementation on the CPS.

All runs use consecutive ascending steps as the reference input. Steps are 5 cm in amplitude and 120 seconds in duration. Nine DoS attacks are applied to the system in scenarios containing DoS attacks. In each step, three DoS attacks are applied for seven seconds (The maximum limit that is considered in the robust PI controller design) respectively, in the transient state (5 seconds after each reference input step begins) and the steady state (50 and 90 seconds after each reference input step begins). During the DoS attacks, the communication network of the CPS is interrupted, and the last value of the signal under attack remains and is used in the computer or data logger.

In all subsequent figures, the output and control signals refer to the actual physical system sensor output and pump voltage rather the signal that the control unit uses and produces (especially during DOS attacks). Also, the maximum pump voltage can be 3 V, so the control signal is limited to this value for protecting the pump.

B. Normal Operation

Fig. 4 illustrates the system response and control signal of the Ziegler-Nichols PI controller (ZN-PI) in normal operation. Also, the system response and control signal of the Kharitonov's theorem-based PI controller (KT-PI) in normal operation is illustrated in Fig. 5. The lower values of KT-PI transient response characteristics, such as overshoot and settling time, indicate better performance of the KT-PI over the ZN-PI. However, the ZN-PI is faster and more aggressive. It is also a confirmation of the KT-PI superiority that the control signal is smaller than the ZN-PI and has low fluctuations that do not easily reach the danger range of the pump.

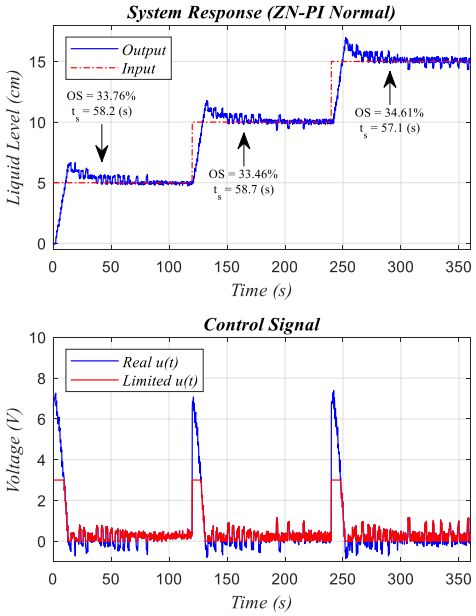

Fig. 4. System response and control signal of ZN-PI in normal operation.

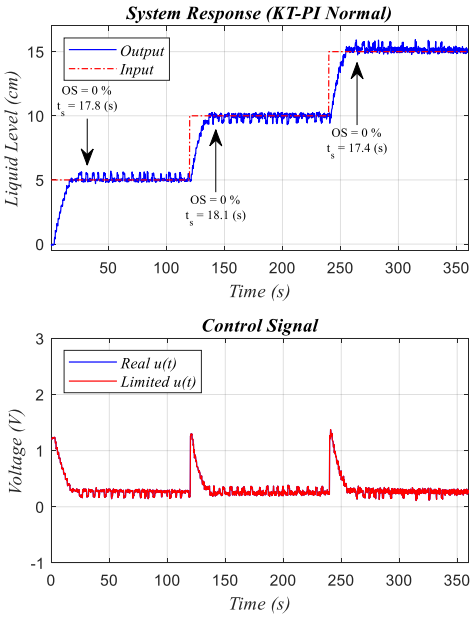

Fig. 5. System response and control signal of KT-PI in normal operation.

C. DoS Attack on Control Signal

The ZN-PI system response and its control signal when DoS attacks occur on the control signal are shown in Fig. 6. Also, Fig. 7 shows the KT-PI performance under the same conditions. When a DoS attack occurs on the control signal, the last value of the control signal at the start time of the attack remains on the DAC of the data logger. Whenever the attack ends, the data logger will continue to operate normally and apply the actual control signal to the pump. Therefore, by not applying the correct values of the control signal to the under DoS attack CPS, the absolute error of setpoint tracking will increase because of the uncontrolled changes in the liquid level. As the ZN-PI controller is more aggressive than the KT-PI, the effects of

the DoS attacks with ZN-PI are severe. However, the proposed KT-PI performs better and almost rejects the attacks.

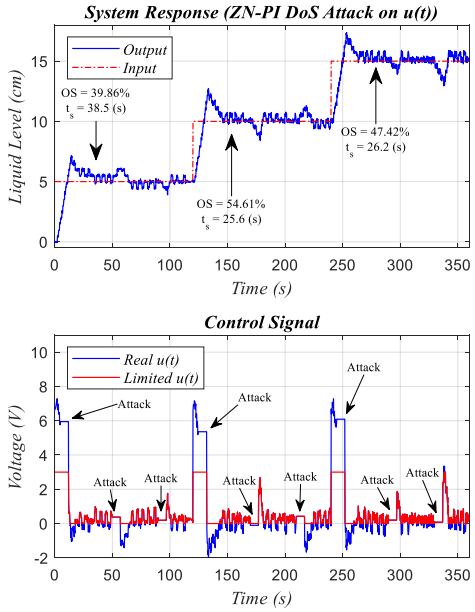

Fig. 6. System response and control signal of ZN-PI under DoS attack on the control signal.

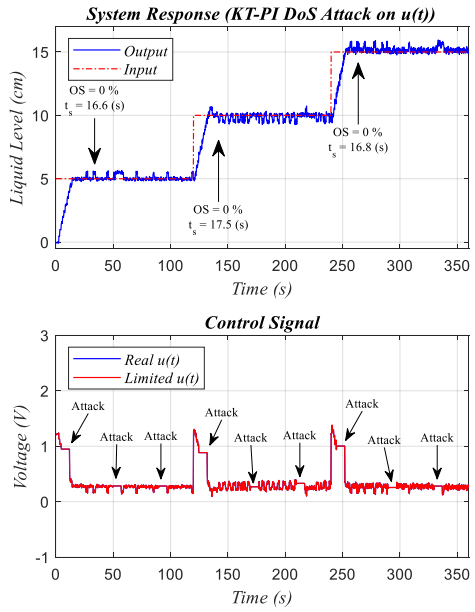

Fig. 7. System response and control signal of KT-PI under DoS attack on the control signal.

D. DoS Attack on Sensor Signal

The ZN-PI system response and its control signal when DoS attacks occur on the sensor signal are illustrated in Fig. 8. Moreover, Fig. 9 illustrates the KT-PI performance under the same conditions. When a DoS attack occurs on the sensor signal, the last value of the sensor signal at the beginning of the attack remains on the computer. So, this value will be used for control signal calculation. This wrong feedback increases the absolute setpoint tracking error. Consequently, the integrator part of both PI controllers enlarges the control signal to reduce this error. As the ZN-PI controller is more aggressive than the KT-PI, it produces larger values, and the effects of DoS attacks with ZN-PI are more severe. In contrast, the proposed KT-PI performs better and almost rejects most attacks.

On the other hand, by comparing the effects of DoS attacks on the control signal (Fig. 7) and sensor signal (Fig. 9), it can be seen that the KT-PI performs better in mitigating attack influences on the control signal than the sensor signal is under attack. This difference can be explained by the fact that DoS attacks on control signals are more like time delays than those on sensor signals, which are more like missed data.

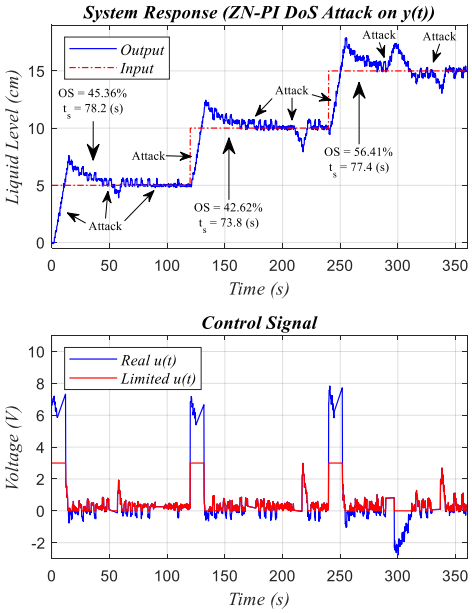

Fig. 8. System response and control signal of ZN-PI under DoS attack on sensor signal.

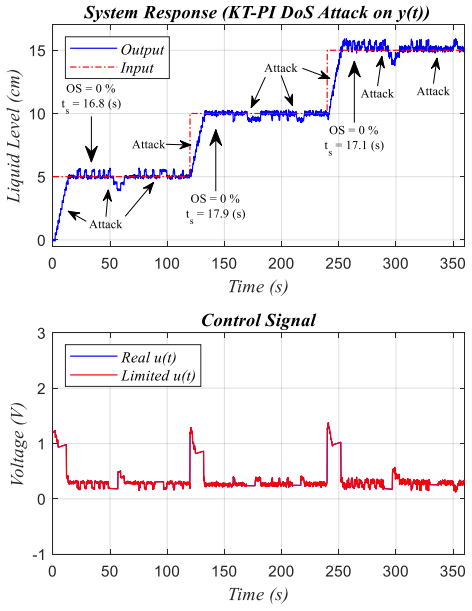

Fig. 9. System response and control signal of KT-PI under DoS attack on sensor signal.

E. DoS Attack on Control and Sensor Signal

Fig. 10 and Fig. 11 show the performance of ZN-PI and KT-PI under DoS attacks on both control and sensor signals simultaneously. The results are similar when we only have the DoS attack on the sensor signal. So, DoS attacks on the sensor signal are more dominant than those on the control signal. Furthermore, it is possible to see the superiority of the KT-PI over the ZN-PI for the CPS again.

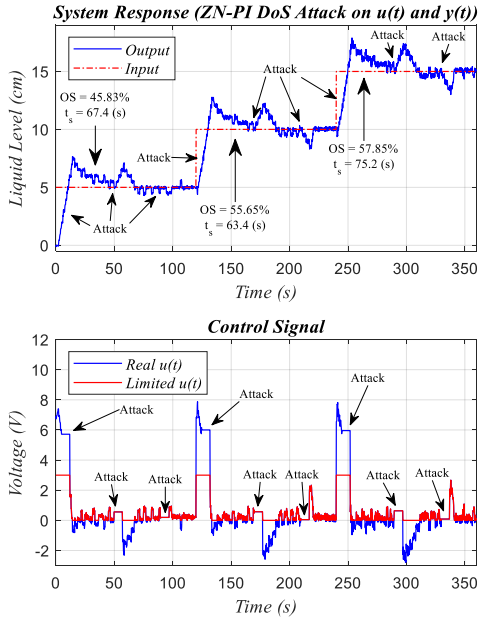

Fig. 10. System response and control signal of ZN-PI under DoS attack on control and sensor signal at the same time.

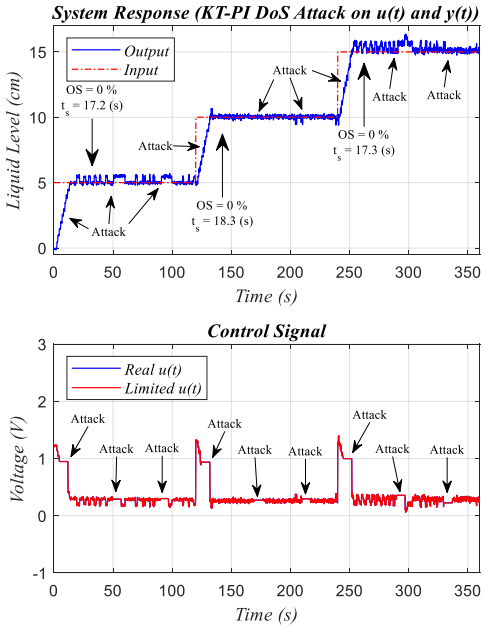

Fig. 11. System response and control signal of KT-PI under DoS attack on control and sensor signal at the same time.

V. CONCLUSION

This article considers a conservative assumption to design a resilient controller against DoS attacks for CPSs by applying Kharitonov's theorem. Due to DoS attack effects, this assumption added more delay to the system model. Based on this assumption, a robust PI controller is proposed using Kharitonov's theorem to minimize the effects of DoS attacks on system behavior. Next, the Ziegler-Nichols method was used to tune another PI controller in order to verify the effectiveness of the proposed robust PI controller. Experiments on a CPS (liquid-level networked control system) were conducted to compare the performance of these two designed controllers. According to the results, the robust PI controller based on Kharitonov's theorem is more effective and reliable than the Ziegler-Nichols method tuned PI controller in mitigating DoS attacks. Kharitonov's theorem based robust PI controller requires additional calculations, while this disadvantage is less significant than its advantages.

REFERENCES

[1] I. H. Sarker, A. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *Journal of Big data,* vol. 7, pp. 1-29, 2020.

[2] W. Duo, M. Zhou, and A. Abusorrah, "A survey of cyber attacks on cyber physical systems: Recent advances and challenges," *IEEE/CAA Journal of Automatica Sinica,* vol. 9, no. 5, pp. 784-800, 2022.

[3] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports,* vol. 7, pp. 8176-8186, 2021.

[4] A. Cetinkaya, H. Ishii, and T. Hayakawa, "An overview on denial-of-service attacks in control systems: Attack models and security analyses," *Entropy,* vol. 21, no. 2, p. 210, 2019.

[5] Y.-L. Huang, A. A. Cárdenas, S. Amin, Z.-S. Lin, H.-Y. Tsai, and S. Sastry, "Understanding the physical and economic consequences of attacks on control systems," International Journal of Critical Infrastructure Protection, vol. 2, no. 3, pp. 73-83, 2009.

[6] Z.-H. Pang, G. Liu, and Z. Dong, "Secure networked control systems under denial of service attacks," *IFAC Proceedings Volumes,* vol. 44, no. 1, pp. 8908-8913, 2011.

[7] F. Asadi and N. Abut, "Kharitonov's theorem: A good starting point for robust control," *The International Journal of Electrical Engineering & Education,* vol. 58, no. 1, pp. 57-82, 2021.

[8] K. Sharma, A. K. Yadav, and B. B. Sharma, "Kharitonov theorem-based robust control approach for sustainable microgrid against DoS cyber-attack," Digital Chemical Engineering, vol. 7, p. 100099, 2023.

[9] B. Raouf and S. Mousavian, "A Robust Controller Design based on Kharitonov's Theorem for Frequency Control in an Interconnected Power System," *European Journal of Electrical Engineering and Computer Science,* vol. 7, no. 1, pp. 1-9, 2023.

[10] H. Chavoshi, A. Salasi, O. Payam, and H. Khaloozadeh, "Experimental Comparison of STR and PI Controllers on a Nonlinear Liquid-Level Networked Control System," in 2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2023: IEEE, pp. 1-8.

[11] S. P. Bhattacharyya, H. Chapellat, and L. H. Keel, Robust control: the parametric approach. Prentice Hall PTR, 1995.