2023 9th International Conference on Control, Instrumentation and Automation (ICCIA)

Enhancing Cybersecurity in Nonlinear Networked Control Systems through Robust PI Controller Design and Implementation against Denial-of-Service Attacks

Amir Hossein Salasi
K. N. Toosi University of Technology
Tehran, Iran
salasi77@email.kntu.ac.ir

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

Omid Payam
K. N. Toosi University of Technology
Tehran, Iran
omid_payam@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*— Networked control systems (NCS) offer the fusion of control technology and modern information systems, delivering numerous advantages. However, this integration also presents security concerns, especially for critical infrastructure. NCS communication channels face vulnerability to cyber threats like Denial-of-Service (DoS) attacks, leading to issues such as delays, data loss, reduced control performance, and potential system instability. Introducing the liquid-level control system, which exhibits nonlinearity, this article explores the practical design and implementation of PI controllers within NCS. In this article, robust PI controllers are designed by Kharitonov's theorem. DoS attacks are applied practically to the NCS, utilizing Kali Linux in order to assess how the system behaves in response to different PI controller coefficients. This approach allows us to investigate the system performance under DoS attacks. The experimental results demonstrate that when PI controller coefficients are appropriately chosen, the impact of DoS attacks on system behavior and performance can be mitigated.**

***Index Terms*—cyber-attacks, denial-of-service attack, Kharitonov's theorem, networked control system**

I. INTRODUCTION

In today's technology-driven society, there is a growing risk of cyber-attacks exploiting computer-dependent systems. These attacks target system security with diverse objectives, underscoring the critical importance of prioritizing cybersecurity. Robust measures are essential across all sectors, safeguarding sensitive data, critical industries, and vital infrastructure. Governments worldwide face the constant risk of crises affecting Network Control Systems, including power plants and transportation networks.[1]

An NCS is made up of a physical system, which is governed by a digital controller. The digital controller functions as a link between the physical processes and the digital domain, allowing for communication between the two via a network. The purpose of integrating digital controllers and physical processes through communication networks is to improve the operational and managerial capabilities of these systems.

The advent of Networked Control Systems (NCS) has brought about a significant revolution in managing and controlling diverse industrial processes. Central to NCS is its network infrastructure, which serves as the fundamental framework enabling seamless communication among actuators, sensors, and the controller. TCP/IP, comprising a suite of communication protocols, plays a pivotal role in governing the transmission, routing, and reception of data across networks. Operating on a layered architecture, TCP/IP functions with distinct layers: the network interface layer handles data at the physical level, addressing, routing, and path determination are managed by the Internet layer, while reliable data transmission is ensured by the transport layer, and the application layer facilitates user interaction for efficient information exchange. This structured approach enhances the efficiency of communication within the network.

While NCS and TCP/IP offer numerous benefits, they also introduce security vulnerabilities. The dependency on networks makes NCS susceptible to cyber threats, and the security aspects of these networks present Difficulties that could lead to potential threats. Significant security concerns associated with TCP/IP networks encompass issues like IP Spoofing, Packet Sniffing, Eavesdropping, Denial of Service (DoS) attacks, MITM attacks. [1]-[4]

In this article, the DoS attack was implemented on NCS. DoS attacks impede the transmission of control and measurement data packets, potentially causing performance disruptions in NCS. Such attacks can manifest through communication channel jamming, compromising devices to hinder data transmission, or flooding the network. DoS attacks are categorized as strong or weak according to severity. Weak

2023 9th International Conference on Control, Instrumentation and Automation (ICCIA) | 979-8-3503-6601-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICCIA61416.2023.10506398

attacks marginally slow down network links of the controller and system, leading to increased packet loss and time delays. On the other hand, strong attacks involve complete shutdowns of the communication network due to DoS assaults. [5]-[7]

The article makes use of a robust PI controller that relies on Kharitonov's theorem. This controller is intended to minimize the impact of DoS attacks on the system's performance. Similar techniques can be found in references [8]-[10]. Designed controllers are applied to a liquid-level control system. The system exhibits nonlinearity and uncertainty, resulting in noticeable nonlinear behavior. In response to this, the Kharitonov method is employed to design a robust PI controller and determine the acceptable area of controller coefficients, always ensuring the stability of the system. The efficacy of the proposed robust PI controller is assessed through practical trials, which involve the execution of genuine DoS attacks on the system.

II. System Introduction

The system in use can be categorized as a cyber-physical system. This inherently nonlinear system employs a PI controller to regulate the liquid level. The system consists of a cylindrical tank with specific dimensions, a variable input voltage pump for liquid transfer, and an adjustable drainage valve. Liquid level measurement is accomplished through a five-kilogram load cell, which generates a voltage signal by translating the liquid's weight-induced force. The sensor's voltage output displays nonlinearity, altering nonlinearly with the ascending liquid level within a range of 0-10V. A physical interface panel facilitates communication between control systems and data loggers, and a Wi-Fi module is utilized for computer connectivity. The device incorporates two digital-to-analog converters (DACs), four analog-to-digital converters (ADCs), and eight digital inputs and outputs. The system is illustrated in Fig. 1.

Fig. 1. Components of the liquid-level control system.

The liquid-level control system operates within an NCS, a subset of broader control systems. NCSs achieve closed-loop control through serial communication networks. The NCS has the capability to communicate with other computers through a Wi-Fi network, facilitated by the TCP/IP protocol. This protocol enables the exchange of data across an Ethernet network. Visualize it as a network where numerous devices connect to a central router, utilizing the TCP/IP protocol for seamless communication. Every unit within this network has a distinct IP address, which enables it to interact with other networked units through TCP/IP. TCP/IP establishes a set of uniform regulations and methods for transmitting, directing, and acquiring data through the network.

III. System Control Structure

A. Kharitonov's Theorem

Kharitonov's theorem was employed in the paper to create a robust controller that can help counteract DoS attacks. Kharitonov's theorem can be applied by defining an interval polynomial. The interval polynomial is expressed as follows [11]:

$$P(s,u) = u_0 + u_1 s + u_2 s^2 + \cdots + u_n s^n$$
$$u_i \in \left[\underline{u_i}, \overline{u_i}\right] \quad \forall i \tag{1}$$
$$0 \notin \left[\underline{u_n}, \overline{u_n}\right]$$

The robust stability of an interval polynomial family *P(s, u)* is determined by the stability of four Kharitonov's polynomials. Kharitonov's four polynomials associated with *P(s, u)* are listed below.:

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

B. Robust PI Controller Design

Two SOPTD models were formulated for the system, encompassing both the primary system and the system with a maximum radius object inside the tank. Typically, the liquid-level control system behaves as a first-order system. Nevertheless, due to our system's restricted and low outflow rate, it takes on characteristics akin to an integrator. As a result, an additional pole is introduced to better capture the actual system dynamics. Additionally, the model accounts for delay, a consequence of the system's inherent traits (for instance, issues with the tube caused delays in connecting the pump to the tank, as well as connectivity problems with the Wi-Fi connection from the computer to the data logger). It's worth noting that in NCSs, time delays can be variable and uncertain, but in the context of this article, the communication network is a local one, rendering the time delay small and negligible in comparison to the inherent system delay (e.g., pipe delays connecting the pump to the tank). Consequently, we have derived the LTI system's discrete transfer function using a sample time of Ts=0.2 seconds [12], [13]. This is the transfer function we obtained as a result.

$$G_1(z^{-1}) = \frac{0.03217 z^{-5}}{1 - 0.9 z^{-1} - 0.09 z^{-2}} \tag{3}$$

Moreover, we calculated the NTI system discrete transfer function with the maximum radius object in the tank, resulting in the following transfer function:

$$G_2(z^{-1}) = \frac{0.0139 z^{-5}}{1 - 0.54 z^{-1} - 0.48 z^{-2}} \tag{4}$$

Parameter intervals to apply Kharitonov's theorem were obtained from these two transfer functions. The transfer functions identified as discrete-time, denoted by equations (3) and (4), have been converted to continuous-time transfer functions. Tustin's method and the first-order Pade approximation have been utilized to accomplish this conversion.

$$G_1(s)=\frac{-0.01777s^3-0.3199s^2-1.066s+3.555}{s^3+14.04s^2+24.64s+1.105} \quad (5)$$

$$G_2(s)=\frac{-0.01311s^3-0.236s^2-0.7868s+2.623}{s^3+29.92s^2+53.96s-3.774} \quad (6)$$

C. Kharitonov's Theorem Implementation

The system interval transfer function should be considered as:

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

Equations (5) and (6) define the ranges of parameters for the interval transfer function for this open-loop system. The parameters of the open-loop system are displayed in the table I with upper and lower bounds.

TABLE I. LIMITS FOR PARAMETERS IN THE TRANSFER FUNCTION OF THE OPEN-LOOP SYSTEM

Parameters of the open-loop transfer function		Parameter Bounds	
		Minimum	***Maximum***
Numerator	b_3	-0.01777	-0.01311
	b_2	-0.3199	-0.236
	b_1	-1.066	-0.7868
	b_0	2.626	3.555
Denominator	a_3	1	1
	a_2	14.04	29.92
	a_1	24.64	53.96
	a_0	-3.774	1.105

For a closed-loop system using PI controllers, the transfer function equals

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

Our interval polynomial is the denominator of our closed-loop system transfer function. Our design parameters are K_i and K_p. Based on the parameter ranges for the open-loop system in Table I, we can find the lower and upper bounds for coefficients of the interval polynomial in (9).

$$\begin{gathered}-0.01777k_p+1<(b_3k_p+a_3)s^4<-0.01311k_p+1\\ -0.3199k_p-0.01777k_i+14.04<(b_2k_p+b_3k_i+a_2)s^3<-0.236k_p-0.01311k_i+29.92\\ -1.066k_p-0.3199k_i+24.64<(b_1k_p+b_2k_i+a_1)s^2<-0.7868k_p-0.236k_i+53.96\\ 2.623k_p-1.066k_i-3.774<(b_0k_p+b_1k_i+a_0)s<3.555k_p-0.7868k_i+1.105\\ 2.623k_i<b_0k_i<3.555k_i\end{gathered} \quad (9)$$

By utilizing the upper and lower bounds of interval polynomial coefficients, it is possible to create four polynomials according to Kharitonov's theorem.

$$\begin{gathered}K_1(s)=0.4443k_i+(0.4443k_p-1.688k_i+0.1381)s+(-1.066k_p-0.3199k_i+24.64)s^2\\ +(-0.3199k_p-0.01777k_i+14.04)s^3+(-0.01777k_p+1)s^4\\ K_2(s)=3.555k_i+(3.555k_p-1.066k_i+1.105)s+(-1.688k_p-0.351k_i+3.564)s^2\\ +(-0.351k_p-0.01777k_i+12.29)s^3+(-0.01777k_p+1)s^4\\ K_3(s)=3.555k_i+(0.4443k_p-1.688k_i+0.1381)s+(-1.688k_p-0.351k_i+3.564)s^2\\ +(-0.3199k_p-0.01777k_i+14.04)s^3+(-0.01777k_p+1)s^4\\ K_4(s)=0.4443k_i+(3.555k_p-1.066k_i+1.105)s+(-1.066k_p-0.3199k_i+24.64)s^2\\ +(-0.351k_p-0.01777k_i+12.29)s^3+(-0.01777k_p+1)s^4\end{gathered} \quad (10)$$

To obtain reasonable values of K_p and K_i, it is necessary for four Kharitonov polynomials to be stable. In order to identify the acceptable range of K_p and K_i, a nested loop was used in which the values of K_p and K_p are changed in the specified interval, and the Hurwitz stability of all four Kharitonov terms is checked for the specific values of K_p and K_i. For the values of K_p and K_i that all four polynomials are stable, those values are added to the permissible range of K_p and K_i. Fig. 2. Depicts the acceptable region.

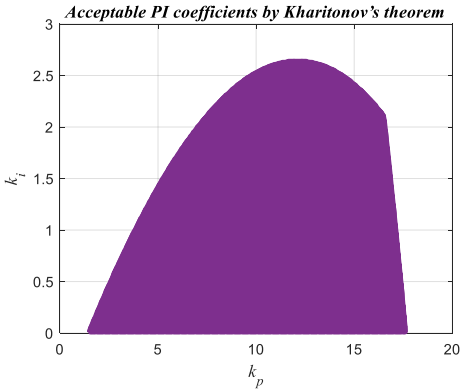

Fig. 2. The area of K_p and K_i which is suitable for robust closed-loop stabilization.

Two points were selected from the permissible range. We conducted a comparative analysis of their results in practical tests to reduce the impact of DoS attacks. The coefficients for the first controller are $K_p = 6.5$ and $K_i = 0.3$, and the second controller coefficients are $K_p = 1.6$ and $K_i = 0.015$. Practical testing will be carried out to determine which one demonstrates superior performance.

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

$$C(z)=k_p+k_i\frac{Ts}{z-1}=1.6+0.015\frac{0.2}{z-1}=\frac{1.6z-1.59}{z-1} \quad (12)$$

The PI controller developed is implemented using MATLAB/Simulink to regulate the system, facilitating straightforward verification of system robustness. This approach stands out for its versatility, proving effective even in managing intricate uncertainty scenarios. It integrates the value set principle with the zero-exclusion condition, enhancing its efficacy as a robust stability assessment tool. A polynomial

family $P=\{p(.,u):u\in U\}$ can be stated as value sets at frequency $\omega\in R$:

$$p(j\omega,U)=\{p(j\omega,U):u\in U\} \tag{13}$$

Therefore, $p(j\omega,U)$ is the representation of U under $p(j\omega,.)$. The zero-exclusion condition must be met for a continuous polynomial family to be Hurwitz stable. Suppose there is an invariant degree family of polynomials with pathwise connected bounding sets of uncertainties U and at least one stable member $P(s,u^0)$. Thus, if the complex plane origin is excluded from the value set $p(j\omega,U)$ at all frequencies $\omega\geq 0$, then the family is robustly stable.

$$0\notin p(j\omega,U)\quad \forall\omega\geq 0 \tag{14}$$

So, for stability verification, we must construct Kharitonov rectangles using the four Kharitonov polynomials derived from the denominator of our closed-loop system (10). The chosen values of K_p and K_i are put in (10), and the Kharitonov rectangles are drawn in Fig. 3.

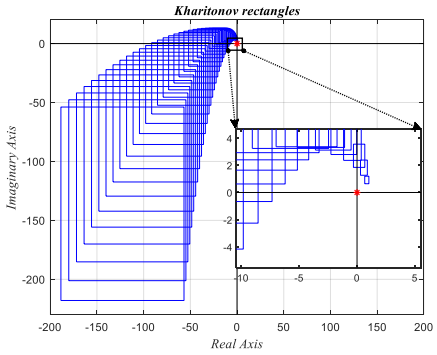

Fig. 3. Kharitonov rectangles of the closed-loop system with $K_p=6.5$ and $K_i=0.3$

The corners of the Kharitonov rectangles shown in Figure 5 correspond to four different Kharitonov polynomials. The stability of the closed-loop system containing $K_p=6.5$ and $K_i=0.3$ is robust, as the Kharitonov rectangles encircle the origin in a counterclockwise direction, with the complex plane origin being excluded from the Kharitonov rectangles.

IV. Experiment Design

A. Implementation of DoS Attack

DoS attacks are a significant category of cyber threats that can lead to severe downtime while often remaining inconspicuous. The TCP SYN Flood attack, a type of DoS, exploits the TCP protocol's three-way handshake to quickly disrupt services and networks. There are seven common types of DoS attacks, including TCP SYN Flood, UDP Flood, TCP FIN Flood, TCP RST Flood, PUSH and ACK Flood, ICMP Flood, and Smurf attack.

In TCP SYN Flood method, attackers inundate a server with numerous SYN packets, sometimes using fake IP addresses. The server responds with SYN-ACKs, leaving its ports partially open and expecting replies from non-existent hosts. In a more straightforward non-spoofed attack, the attacker uses firewall rules to block SYN-ACK packets, overwhelming the target with SYN packets. This strains the target's resources, leading to increased CPU and memory usage, eventually rendering the server incapable of servicing genuine client requests, and causing a DoS.

One of the most straightforward methods for executing a DoS attack involves utilizing Kali Linux, particularly making use of hping3, which is a widely used TCP penetration testing tool bundled with Kali Linux. Hping3 can be installed by Linux users in their current distribution. In most cases, random IP addresses are spoofed by attackers using tools like hping. The SYN flood attack is then directed to our target which is 192.168.1.50.

In the given code description, a total of 15,000 packets are being sent, each with a size of 120 bytes. The SYN Flag is actively enabled, and a TCP window size of 64 is configured. The victim's HTTP web server is the target, with packets being flooded onto the server as rapidly as possible. To obscure the identity and block the victim's SYN-ACK reply packets from reaching the attacker, the --rand-source flag is employed for generating spoofed IP addresses.

Algorithm 1. Implementation a DoS attack in Kali Linux

```
# Install hping3
sudo apt-get install hping3
# Run hping3 to initiate a SYN flood attack
hping3 -c 15000 -d 120 -S -w 64 -p 8080
--flood --rand-source 192.168.1.50
```

B. Assumptions

The effectiveness of the PI controllers in the NCS is assessed in this segment. The assessment entails two distinct scenarios: normal operation and a Denial-of-Service (DoS) attack targeting the control signal. By practically implementing the controllers within the NCS, their performance is measured and contrasted across both scenarios.

All experiments entail employing successive ascending steps as the reference input, each with a 2.5 cm amplitude and a duration of 100 seconds. Throughout each step, DoS attacks are initiated at specific time intervals (5, 30, 55, and 78 seconds after the commencement of each step), each lasting for six seconds, which is the maximum limit considered in the design of the robust PI controller. Attacks are executed in both the transient state, which is 5 seconds after each reference input step begins, and the steady state, which is 30, 55, and 78 seconds after each reference input step begins. If a DoS attack occurs, the NCS's communication network is disrupted, and the final signal value under attack is saved and used within the computer or data logger.

In all following visual depictions, the output and control efforts relate to the tangible aspects of the physical system, specifically involving the sensor output and pump voltage. This emphasis is placed on the actual signals originating from the system rather than those influenced by the control unit, particularly in instances such as DoS attacks.

Furthermore, it should be noted that the pump is safeguarded by restricting the maximum pump voltage to 3 V.

V. RESULTS

A. Normal Operation

The illustration depicts the system's reaction and the control effort of the PI controller based on the Kharitonov theorem during normal operation in Fig. 4, where $K_i = 0.3$ and $K_p = 6.5$, And for the second one where $K_i = 0.015$ and $K_p = 1.6$ is depicted in Fig. 5. It can be seen that the larger coefficients of the controller cause an aggressive reaction and bring the control signal to the limit of 3V. As a result, we have incomplete fast behaviors, and overshoot can be easily observed, which is not desirable.

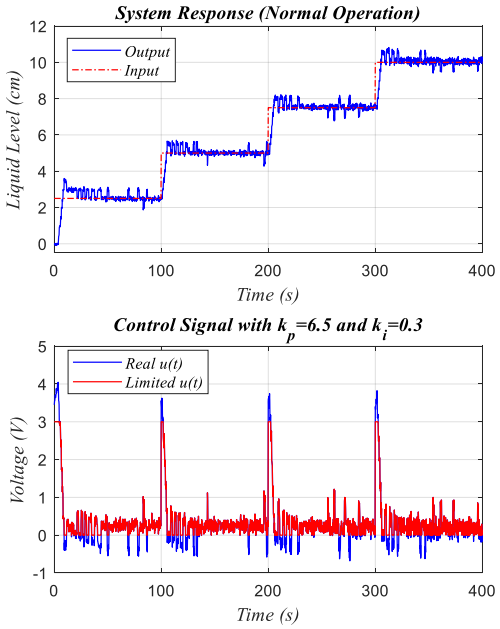

Fig. 4. The system's reaction and the control effort during normal state. ($K_i = 0.3$ and $K_p = 6.5$)

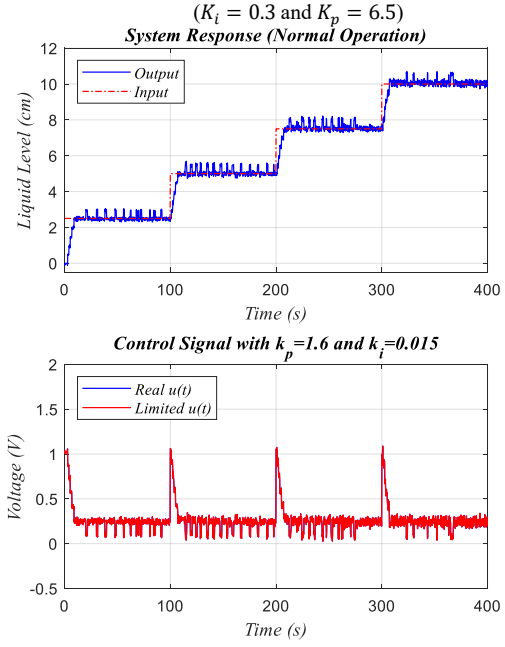

Fig. 5. The system's reaction and the control effort during normal state. ($K_i = 0.015$ and $K_p = 1.6$)

B. DoS Attack

In comparing the two PI controllers, it is evident that the first controller, equipped with lower coefficient values ($K_i = 0.015$ and $K_p = 1.6$), exhibits favorable transient response characteristics, particularly in terms of reduced overshoot, signifying superior performance compared to the second controller with higher coefficients ($K_i = 0.015$ and $K_p = 1.6$). The occurrence of the DoS attack on the control signal causes an increase in error, and the milder response of the first controller to this causes a smaller control signal and fewer fluctuations as if buffering the pump against reaching the critical danger range. Fig. 6 and Fig. 7 compare these two different controller behaviors under DoS attacks.

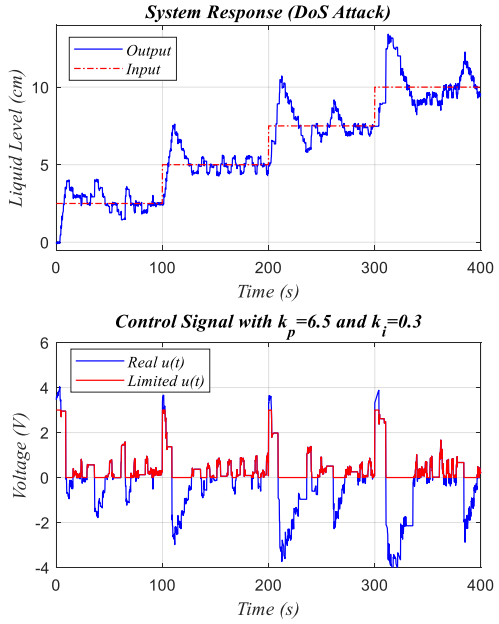

Fig. 6. The system's reaction and the control effort during the DoS attack. ($K_i = 0.3$ and $K_p = 6.5$)

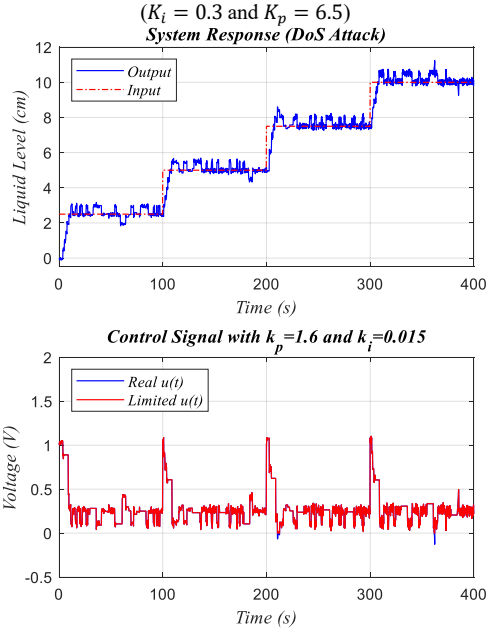

Fig. 7. The system's reaction and the control effort during the DoS attack. ($K_i = 0.015$ and $K_p = 1.6$)

Notably, the controller with lower coefficient values superiority is affirmed by its smaller control signal and minimal fluctuations, which provide a buffer against reaching the critical pump danger range. Therefore, the controller with larger coefficients yields a more substantial control signal and responds more aggressively to system variations.

VI. CONCLUSION

This paper adopts an empirical approach to formulate a resilient controller for NCSs, aiming to counteract DoS attacks by leveraging Kharitonov's theorem. Practical implementation of two PI controllers carried out on an NCS to assess their performance. We witnessed the stability and acceptable performance of the controllers in the presence of uncertainty, and the final findings reveal that the robust PI controller utilizing this theorem, equipped with lower coefficient values, proves to be more effective and dependable in mitigating DoS attacks compared to the version with higher coefficients.

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] H. Chavoshi, A. Salasi, O. Payam, and H. Khaloozadeh, "Man-in-the-Middle Attack Against a Network Control System: Practical Implementation and Detection," in *2023 IEEE 64th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*, 2023, pp. 1-6, doi: 10.1109/ITMS59786.2023.10317671.

[5] 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.

[6] 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.

[7] 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.

[8] H. Chavoshi, A. K. Sedgh, and H. Khaloozadeh, "Resilient Control for Cyber-Physical Systems Against Denial-of-Service Cyber Attacks Using Kharitonov's Theorem," in *2023 IEEE 64th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*, 2023, pp. 1-6, doi: 10.1109/ITMS59786.2023.10317694.

[9] 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.

[10] 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.

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

[12] 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, pp. 1-8, doi: 10.1109/ECAI58194.2023.10193928.

[13] H. R. Chavoshi, O. Payam, A. H. Salasi, and H. Khaloozadeh, "Robust control design of a nonlinear liquid-level networked control system: a comparative study between STR and Kharitonov analysis," *International Journal of Dynamics and Control,* 2023, doi: 10.1007/s40435-023-01328-w.