Enhancing the Resilience of Cyber-Physical Systems to DoS Attacks by Adopting Latency-Reducing TCP Variants

Journal:	*Transactions on Dependable and Secure Computing*
Manuscript ID	TDSC-2024-05-0599
Manuscript Type:	Regular Paper (S1)
Date Submitted by the Author:	31-May-2024
Complete List of Authors:	Barchinezhad, Soheila; University of Tehran, School of Electrical and Computer Engineering Sayad Haghighi, Mohammad; University of Tehran, School of Electrical and Computer Engineering; Swinburne University of Technology, Farivar, Faezeh; Islamic Azad University Science and Research Branch; Institute for Research in Fundamental Sciences, Khonsari, Ahmad; University of Tehran College of Engineering, School of Electrical and Computer Engineering; Institute for Research in Fundamental Sciences, School of Computer Science
Keywords:	Cyber Physical Systems, Transmission Control Protocol, Denial of Service, System Stability, C.2.0.f Network-level security and protection < C.2.0 General < C.2 Communication/Networking and Information Technology < C Comp
Note: The following files were submitted by the author for peer review, but cannot be converted to PDF. You must view these files (e.g. movies) online.	
Latex_Source_Code.zip	

Enhancing the Resilience of Cyber-Physical Systems to DoS Attacks by Adopting Latency-Reducing TCP Variants

Soheila Barchinezhad, Mohammad Sayad Haghighi, *Senior Member, IEEE*,
Faezeh Farivar, *Senior Member, IEEE*, Ahmad Khonsari.

***Abstract*—In this paper, we investigate the resilient control of cyber-physical systems (CPSs) under denial of service (DoS) attacks, with a focus on communication network properties. We propose innovative Transmission Control Protocol (TCP) strategies to boost CPS resilience against DoS attacks by enhancing packet delivery rates and minimizing communication latency. Our approach includes the introduction of Modified TCP (MCP) and backoff mitigating MCP (bMCP) strategies, tailored to adapt to network and attack situations. We also present latency-reducing extensions for both strategies to further enhance CPS resilience. Additionally, we derive a sufficient stability condition based on the outcomes of these approaches. Through theoretical analysis and simulation experiments, we demonstrate the effectiveness of these strategies in reducing latency, improving packet delivery rates, and enhancing system resilience. Furthermore, we evaluate the maximum tolerable DoS attack rates under various TCP strategies, providing empirical evidence for their effectiveness in strengthening CPS performance against adversarial attacks and network-related challenges.**

***Index Terms*—Cyber Physical Systems, Transmission Control Protocol, Denial of Service, System Stability, Security.**

I. Introduction

A. Motivation

CYBER-physical systems (CPSs) integrate control, physical processes and communication networks [1]. Communication networks interconnect both controller and physical plant through a forward and a feedback stream. This integration aims to enhance operational and management capabilities in CPSs. However, it also introduces various challenges, including cyber attacks, resource bottlenecks, packet drop, disordering, and delay. These challenges far surpass those encountered in standard control systems, demanding a focused effort on security aspects such as intrusion detection [2], compensation [3], stability analysis [4], stabilization and controller design [5], with an emphasis on the cyber aspects.

Among the most pressing security concerns for CPSs is the vulnerability of communication links to compromise by malicious entities, leading to cyberattacks [6]–[9]. These attacks, including deception attacks that manipulate sensor or controller data trustworthiness, and Denial of Service (DoS) attacks that aim to disrupt CPS network resources, pose significant threats [10]–[14]. DoS attacks, seek to degrade the efficiency of physical systems or destabilize them by inducing extensive packet drops and delays. Effectively mitigating these threats require the development of new transmission mechanisms tailored to the time-sensitive nature of CPSs, involving the intricate modeling and integration of network entities from real communication networks with the control system.

B. Related work

In the literature, there are two general approaches for analysis and enhancing CPSs resilience in the presence of DoS attacks and delay. The first approach considers any network delay and packet drops in general form without dealing with network specifications. This approach can be seen in [15] and [16] which focus on the controller design of networked control systems considering both the network-induced delay and the data packet dropout. In these studies, the feedback control gain, the maximum allowable delay value and the maximum allowable transfer interval (MATI) can be derived by solving a set of Linear Matrix Inequalities (LMI). In both references, the considered system consists of a clock-driven sensor and event-driven controller and actuator which always discard the old data and use the new received samples. Similarly, in [17], some stabilization conditions for a continuous-time process are found, where the process is considered as a system with input delays and the Zero-Order Hold (ZOH), to choose the newest control input packet.

The second approach to enhancing CPS resilience involves considering network parameters alongside control systems, primarily focusing on optimizing network transmission control strategies to improve CPS resilience under DoS attacks. Recent advancements in modeling network protocols, particularly Transmission Control Protocol (TCP), have been instrumental in this area. Studies such as [18], [19] have delved into the dynamics of networks with TCP-supported routers, emphasizing congestion control through active queue management (AQM) policies like random early detection (RED). Using this kind of modelings, some works have explored CPS resilience by treating the network as a feedback control problem and designing stabilizing controllers as AQM for internet routers supporting TCP [20]–[23]. For example, [24] presents an augmented model for a control system and corresponding TCP communication, transformed into a state-dependent differential

S. Barchinezhad, M. Sayad Haghighi and A. Khonsari are with the School of Electrical and Computer Engineering, University of Tehran, Iran, emails: {s.barchinezhad, sayad, a_khonsari}@ut.ac.ir.

F. Farivar is with Science and Research Branch, Islamic Azad University, Tehran, Iran, and also with the School of Computer Science, Institute for Research in Fundamental Sciences (IPM), Tehran 19395-5746, Iran, email: f.farivar@srbiau.ac.ir.

equation, with stability conditions expressed in LMIs. Similarly, [25] introduces an augmented control system under TCP in communication networks as a multiple-delay system, incorporating different delays for plant-to-controller and controller-to-plant, with stability and stabilization conditions derived in terms of LMIs. The first limitation of the discussed research is that, contrary to their assumptions, it is not feasible to control intermediate routers along with the sender. The sender window size is the only thing that can be controlled. The second constraint lies in the simplistic representation of TCP in these studies, lacking the incorporation of slow-start in the model. Thirdly, these works assume that network-induced delay is only propagation delay and queueing delay, which may not hold true in practice. In CPS design, it is crucial to address both network delay and packet drop simultaneously, as they are critical factors that impact system performance and resilience.

C. Contributions

In response to the intricate challenges posed by network disruptions and DoS attacks in the domain of CPS, this paper presents a novel and comprehensive set of contributions aimed at enhancing the resilience and stability of CPSs. Stability implies that the system does not experience excessive oscillations or diverge infinitely under inputs or disturbances. Our work significantly advances the field by introducing tailored TCP strategies that minimize communication latency and improve packet delivery rates. These strategies are designed to adapt to varying network conditions and attack scenarios. The main contributions of this paper are the following:

- In CPSs, reliable transmission protocols are essential. Our model for control system design incorporates TCP flow dynamics, addressing packet loss detection via triple duplicate acknowledgements (TD) and timeouts (TO). Our approach includes both TO and TD dropouts in the TCP model, yielding results that closely align with NS2 (Network Simulator Ver.2) outputs, surpassing simpler TD-only models found in the literature.
- A new delay model for CPSs in the presence of DoS attacks by considering TCP as data transmission protocol is proposed. This model incorporates both network delay and packet dropout/retransmission delay, providing a comprehensive understanding of the communication delays that impact CPS performance.
- Acknowledging the unique requirements of CPS, we introduce two innovative TCP strategies: the Packet Replicating Strategy within the Modified TCP (MCP) protocol and the Backoff mitigating strategy (bMCP). These strategies are meticulously designed to address specific challenges of TCP transmission reliability and retransmission delay. By tailoring the strategies to CPS characteristics, we establish a robust foundation for CPS communication networks that can withstand DoS attacks.
- We further elevate the efficacy of the proposed strategies by introducing two enhancements. These refinements are carefully crafted to counteract the negative effects of DoS attacks by controlling the sending window size. By fine-tuning the strategies, we fortify the stability and reliability of CPS under adverse network conditions.

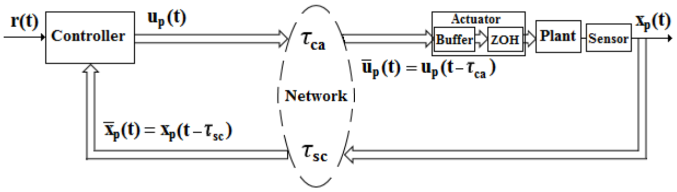

Fig. 1. A simple form of closed loop CPS.

- Additionally, we derive a sufficient stability condition based on the results of the proposed TCP strategies. This condition serves as a guideline for ensuring the stability of CPS under DoS attacks, providing a theoretical foundation for the effectiveness of the proposed approaches.
- To show the practical implications of our work, we conduct extensive simulations in Matlab and NS2. The results demonstrate the tangible benefits of employing the proposed methods in terms of packet delivery rate, latency reduction, and system stability in DoS attack scenarios.

II. MODEILNG

A. Delay dependent control oriented model

A simple form of closed loop of a CPS is shown in Fig.1. The sensor measurement and control signal data packets are transmitted through communication network. All of these packets has a delay before arrival at the destination.

In this paper, the following assumptions are considered for the closed-loop system.

Assumption 1: Control and output data are transmitted using a reliable transmission protocol (i.e., TCP), and data are transmitted in a single packet.

Assumption 2: The path that include the congested router is the one that leads from the controller to the actuator of plant (τ_{ca}), whereas the feedback path is subject only to a fixed propagation and queuing delay (τ_{sc}).

Assumption 3: The states of the plant are either directly available or can be estimated accurately.

Consider a linear continuous system as the plant. Accounting for the assumptions mentioned earlier along with the effects of network delay and packet dropout, the plant and the controller are modeled as follows:

$$\begin{cases} \dot{x}_p(t) = A_p x_p(t) + B_p \bar{u}_p(t), \\ \bar{u}_p(t) = -K_p x_p(t - \tau_p(t)), \\ x_p(s) = \varphi_p(s), \; s \in [-h_p, 0] \end{cases} \tag{1}$$

where A_p and B_p are known system matrices, $x_p(t)$ represents the system state, and $\bar{u}_p(t)$ is the delayed control input. The state feedback gain matrix is denoted by K_p. $\varphi_p(.)$ represents the functional initial condition, and $\tau_p(t)$ denotes the total delay in time t, encompassing both forward and backward delays ($\tau_{sc} + \tau_{ca}$). This delay includes factors such as packet dropout, retransmissions, propagation, and queuing. A comprehensive modeling of this delay will be expounded upon in the subsequent subsection. The subscript p is used to specify the matrices and signals related to the plant.

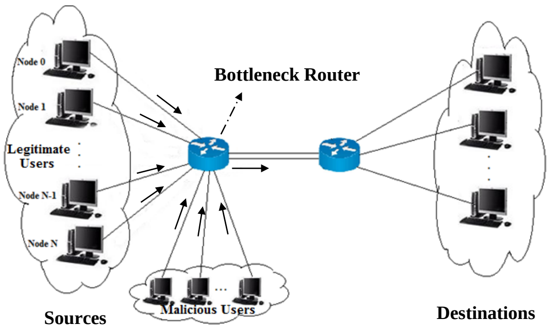

Fig. 2. Network Topology.

B. Network modeling

The TCP behavior was modeled by means of numerically solvable differential equations in [18]. These equations model the complete system connecting packet drops and the TCP sending window. The TCP model under consideration is Reno, a widely used scheme in congestion control applications and research. The behavior of most of other TCP variants are similar to it [26].

Let consider a classic topology where TCP flows passed through a bottleneck router as illustrated in Fig. 2. The buffer of this bottleneck router is distributed among the various flows. This setup gives rise to the subsequent equation, capturing the relationship between the window size and the queue size of the bottleneck router [18]:

$$\begin{cases} \dot{w}(t) = \frac{1}{\tau_n(t)} - (1-Q(w(t)))(\frac{w(t)w(t-\tau_n(t))}{2\tau_n(t-\tau_n(t))})p_r(t-\tau_n(t)) \\ \quad +(Q(w(t)))(1-w(t))(\frac{w(t-\tau_n(t))}{\tau_n(t-\tau_n(t))})p_r(t-\tau_n(t)) \\ \dot{q}(t) = -C + \frac{N}{\tau_n(t)}w(t) \end{cases} \tag{2}$$

The equation includes the following variables: N, which represents the network load factor or the number of TCP sessions; $w(t)$, the TCP window size in the range $[1 \quad w_m]$ where w_m is the maximum window size; $p_r(t)$ representing the data packet loss probability within the interval $[0 \quad 1]$; $q(t)$, the queue length in the range $[0 \quad q_m]$ with q_m being the size of the router buffer; and $\tau_n(t)$, depicting the network delay given by $T_p + \frac{q(t)}{C}$. Here, C denotes the output capacity of the bottleneck router in packets per second, and T_p signifies the round trip propagation delay of the channel. The term $\frac{q(t)}{C}$ effectively models the queueing delay.

In TCP, the receiver sends an acknowledgement (ACK) immediately after receiving a packet. This protocol guaranties reliability by waiting for ACKs of packets sent, and retransmitting them if they not acknowledged. The data packet loss can be realized in two ways: triple duplicate ACKs and retransmission time out [27]. In the first case, if the sender receives three duplicate ACKs, congestion window is halved and fast retransmission is done. In addition to this, the sender uses a retransmission timer to ensure packet delivery in the absence of any feedback from the receiver. In this case that TO happens, the window size is reduced to one and packets are retransmitted after a period of a specified retransmission time out (RTO).

In [28], Padhye et al. report that, in many cases, the majority of window decreases are due to timeouts rather than triple duplicate ACKs. Consequently, an effective TCP model should incorporate timeout-induced packet loss. In equation (2), $Q(w(t))$ represents the probability of packet loss due to timeout. This probability is calculated as $Q(w(t)) = \min(1, 3/w(t))$ in [28], where $w(t)$ is the window size at the time of loss.

Remark 1: The expected latency of duplicate ACK detection and fast retransmission is derived in [29]:

$$E(L_{TD}) = RTT \tag{3}$$

where L_{TD} denotes the latency of a triple duplicate ACK drop and RTT is average round trip time between two hosts.

Remark 2: During the retransmission process of consecutively lost packets, a waiting time is introduced before reattempting the retransmission. This delay is often controlled using an exponential backoff algorithm. In this scheme, the sender increases the waiting time with each unsuccessful retransmission, starting with a brief period after the initial failure. The interval between retransmission attempts is incrementally extended, doubling from the previous duration for up to six iterations. Beyond this point, the waiting time remains constant. As detailed in [29] and [28], this strategy leads to specific probabilities and durations associated with encountering k consecutive packet losses within a single timeout (TO). The probabilities and lengths of such consecutive drop events are outlined as follows:

$$prob(N_d = k) = p^{k-1}(1-p) \tag{4}$$

and,

$$L_k = \begin{cases} (2^k - 1)T_0 & if\ k \leq 6 \\ (63 + 64(k-6))T_0 & if\ k > 6 \end{cases} \tag{5}$$

when N_d represents the count of consecutive drops, p denotes the drop probability, and T_0 stands for the duration of the initial retransmission timeout (RTO). The expected latency associated with a timeout is then computed as follows:

$$E(L_{TO}) = \sum_{k=1}^{\infty} prob(N_d = k)L_k \tag{6}$$

where L_{TO} denotes the latency of a timeout drop. Subsequently,

$$E(L_{TO}) = \frac{(1 + p + 2p^2 + 4p^3 + 8p^4 + 16p^5 + 32p^6)T_0}{1-p} \tag{7}$$

According to [30], TCP achieves near-maximal throughput when T_0 is 1 second. Thus, the latency of a timeout event for the system of equation (2) at time t can be given as:

$$E(L_{TO}(t)) = \frac{G(p_r(t))}{1-p_r(t)}, \quad G(p_r(t)) = 1 + p_r(t) + 2p_r(t)^2 + 4p_r(t)^3 + 8p_r(t)^4 + 16p_r(t)^5 + 32p_r(t)^6 \tag{8}$$

It can be rewritten as follows:

$$\begin{aligned} E(L_{TO}(t)) &= (1 + p_r(t).\frac{1-64p_r(t)^6}{(1-2p_r(t))}).\frac{1}{(1-p_r(t))} \\ &= \frac{1-p_r(t)-64p_r(t)^7}{1-3p_r(t)+2p_r(t)^2} \end{aligned} \quad (9)$$

Therefore, formulation of delay, considering packet drops, can be expressed as follows:

$$\begin{aligned} \tau'(t) = (1-p_r(t)).\tau_n(t)+p_r(t).[\tau_n(t)+(1-Q(w(t))).RTT \\ + Q(w(t)).\frac{1-p_r(t)-64p_r(t)^7}{1-3p_r(t)+2p_r(t)^2}] \end{aligned} \quad (10)$$

Alternatively, it can be written as:

$$\begin{aligned} \tau'(t) = \tau_n(t) + p_r(t).[(1-Q(w(t))).RTT \\ + Q(w(t)).\frac{1-p_r(t)-64p_r(t)^7}{1-3p_r(t)+2p_r(t)^2}] \end{aligned} \quad (11)$$

Now, by incorporating the TCP protocol and the control system (1), we can derive:

$$\begin{cases} \dot{x}_p(t) = A_p x(t) - B_p K_p x(t-\tau_p(t)) \\ x_p(s) = \varphi_p(s),\ s \in [-h_p, 0] \end{cases} \quad (12)$$

where $\tau_p(t) = \tau'(t) + T'_p$ with T'_p as the sensor to controller channel delay (τ_{sc}).

The network model described in (2) includes a solitary bottleneck router; it is improbable to encounter multiple congestion points along a single path [26]. In our modeling, the AQM policy adopted in routers adheres to the RED policy. In the following we will model the probability of packet drop for CPS under burst DoS attack.

C. Assessing the feasibility of DoS attacks and introducing a new delay model

In the communication path between the plant and the controller, the routers' queue buffers might become overwhelmed by an attacker. The attack's sudden influx of data saturates the queue, resulting in dropped packets. Consequently, the affected flows enter a timeout and slow start phase [31]. Notably, in the context of CPS, this type of DoS attack leads to extended delay jitter for both control and output packet flows. Let's consider a classic network topology, depicted in Fig. 2, accommodating N eligible sessions. Also assume that a malicious third-party node intends to induce packet drops in the network bottleneck by initiating a burst flow (in a Distributed Denial of Service - DDoS - attack, all malicious nodes can be considered as an aggregate node). Under this scenario, the average queue length can be expressed as:

$$\dot{q}(t) = -C + \frac{Nw(t)}{\tau_n(t-\tau'(t))} + R_{DoS} \quad (13)$$

where R_{DoS} (packets/s) represents the aggregated rate of the attacker's flow.

TCP regulates packet flow by waiting for an acknowledgment before feeding more packets to the channel. This mechanism is valid for legitimate senders, but the attackers might send data to the router without waiting for acknowledgment. Consequently, the bottleneck router becomes the recipient of data packets from three sender groups: the attacker, the controller, and $N-1$ other legitimate senders. The aggregated attacker aims to flood the queue's buffer, thereby diminishing the chances of successful packet delivery for the legitimate senders. On the other hand, the service rate of the queue is C packets/s. Once a packet leaves the queue, all three sender groups contend to occupy the available space. Consequently, the likelihood of packet's success for any packet competing for the bottleneck router's queue, is determined by $\frac{1}{\frac{Nw(t)}{\tau_n(t-\tau'(t))}+R_{DoS}}$. Thus, the probability of a packet being dropped during a DoS attack on the network can be expressed as follows:

$$p_r(t) = 1 - \frac{C}{\frac{Nw(t)}{\tau_n(t-\tau'(t))} + R_{DoS}} \quad (14)$$

Incorporating the drop probability introduced in (14) reduces the likelihood that the plant will receive the packet dispatched by the controller. This reduction in probability, coupled with the delay arising from sequential packet drops and subsequent retransmissions, exerts a pronounced negative impact on system performance and stability. Given these circumstances, it becomes imperative to adopt different transmission control protocols tailored to real-time applications.

In response to this challenge, we propose some modifications on TCP for delay-sensitive systems. The aim is to enhance the CPS's probability of achieving successful packet transmission and reception under DoS attacks.

III. Latency-Reducing TCP Modifications for CPSs Under DoS Attacks

In this section, we will investigate three TCP modifications. Each of these modifications has been successfully implemented and extensively tested within the network simulator-NS2.

A. Enhancing transmission reliability: Replicating packets

In this model, the controller employs a modified TCP variant referred to as MCP. This novel TCP variant includes an additional component that duplicates each ready-to-send packet, generating n identical copies that are subsequently transmitted over the channel. The receiver eliminates duplicate packets. This TCP variant is employed in real-time CPSs. The other $N-1$ sessions using the shared router adhere to the traditional TCP protocol, while the attacker maintains a constant packet rate to maximize its resource utilization.

This approach augments the probability of successful packet delivery to the controller, thus reducing the average delay in closed-loop systems. Nevertheless, the potential for packet drops still persists. Moreover, this approach introduces a novel delay for the other $N-1$ nodes.

The probability of encountering packet drops at the bottleneck, when the controller adopts MCP, is governed by the following formula:

$$p_m(t) = 1 - \frac{C}{\frac{(N-1)w_1(t)}{\tau_n(t-\tau_{tcp}(t))} + R_{DoS} + \frac{nw_2(t)}{\tau_n(t-\tau_{mcp}(t))}} \quad (15)$$

where w_1 represents the window size of TCP sessions, and w_2 is the window size of the MCP session. It's important to note that due to the differing probabilities of packet drop for the controller and the other $N-1$ nodes, the couple $(w_1(t), \tau_n(t-\tau_{tcp}(t)))$ and $(w_2(t), \tau_n(t-\tau_{mcp}(t)))$ has different values. Specifically, $w_1(t)$ and $\tau_n(t-\tau_{tcp}(t))$ adhere to the formulation of (2) with a drop probability of $p_m(t)$. Similarly, $w_2(t)$ and $\tau_n(t-\tau_{mcp}(t)))$ adhere to the same equation, but with a drop probability of $(p_m(t))^n$. This adjustment is due to the fact that the node implementing MCP will experience packet loss when all n duplicas of a packet are lost within the bottleneck queue buffer. In (15), delay for TCP and MCP sessions are as follows:

$$\begin{aligned}\tau_{tcp}(t) = \tau_n(t) + p_m(t).[(1 - Q(w(t))).RTT \\ + Q(w(t)).\frac{1 - p_m(t) - 64p_m(t)^7}{1 - 3p_m(t) + 2p_m(t)^2}]\end{aligned} \quad (16)$$

and,

$$\begin{aligned}&\tau_{mcp}(t) = \tau_n(t) + p_c(t).[(1 - Q(w(t))).RTT \\ &+ Q(w(t)).\frac{1 - p_c(t) - 64p_c(t)^7}{1 - 3p_c(t) + 2p_c(t)^2}], \qquad p_c(t) = (p_m(t))^n\end{aligned} \quad (17)$$

It should be noted that with the incorporation of MCP into the controller, the formulation for the delay in the control system can be redefined as follows:

$$\tau_p(t) = \tau_{mcp}(t) + T_p' \quad (18)$$

Furthermore, in this new TCP version, we can establish the following formulation for the queue buffer.

$$\dot{q}(t) = -C + \frac{(N-1)w_1(t)}{\tau_n(t-\tau_{tcp}(t))} + \frac{nw_2(t)}{\tau_n(t-\tau_{mcp}(t))} + R_{DoS} \quad (19)$$

B. Enhancing stability: Latency-reducing strategy in MCP

As discussed in the introduction, the emergence of DoS attacks in CPS introduces new challenges in terms of stability analysis. The aim of this section is to establish some conditions for enhancing the stability of the time delay system (12) in the presence of burst DoS attack by considering MCP as the transmission control protocol. In equation (12), we are dealing with two distinct yet interconnected systems: the control system and the dynamic communication network. The impact of communication network, characterized by delays, directly influences the behavior of the control system. To maintain stability within the control system, it is imperative to minimize the delay. To address this concern, we introduce the subsequent proposition.

Proposition 1: Consider the time-delayed system (12). Let's assume that the transmission control protocol employed in this system is MCP with parameter n. Additionally, consider $N-1$ TCP sessions that share the same bottleneck with this system. Let $p_c(t)$ denote the probability of packet drop for controller-to-plant packets, $w_2(t)$ represent the window size of MCP sessions, and $w_1(t)$ indicate the window size of TCP sessions. Under this situation, a set of conditions on TCP/MCP can be established to keep the system from transitioning into an unstable mode due to prolonged delays arising from severe DoS attacks (the situation in which $w_1(t) = 1$, $q(t)$ is in steady state).

a) When $w_2(t) > 3$, consider increasing $w_2(t)$ if $\Delta_1 \leqslant 0$, and conversely, decrease $w_2(t)$ if $\Delta_1 > 0$.

$$\begin{aligned}\Delta_1 = &\frac{np_m^{n-1}\frac{nC}{\tau_n(t-\tau_{mcp}(t))}}{(\frac{(N-1)}{\tau_n(t-\tau_{tcp}(t))} + R_{DoS} + \frac{nw_2(t)}{\tau_n(t-\tau_{mcp}(t))})^2} \\ &((1 - \frac{3}{w_2(t)})RTT + \frac{3}{w_2(t)}\frac{1 - p_c(t) - 64p_c(t)^7}{1 - 3p_c(t) + 2p_c(t)^2}) \\ &+ p_c(t)(\frac{3RTT}{w_2(t)^2} - \frac{3}{w_2(t)^2}\frac{1 - p_c(t) - 64p_c(t)^7}{1 - 3p_c(t) + 2p_c(t)^2} \\ &+ \frac{3}{w_2(t)}\frac{np_m^{n-1}\frac{nC}{\tau_n(t-\tau_{mcp}(t))}}{(\frac{(N-1)}{\tau_n(t-\tau_{tcp}(t))} + R_{DoS} + \frac{nw_2(t)}{\tau_n(t-\tau_{mcp}(t))})^2} \\ &\frac{2(1 - p_c(t)^2 - 224p_c(t)^6 + 578p_c(t)^7 - 576p_c(t)^8 - 2p_c(t))}{(1 - 3p_c(t) + 2p_c(t)^2)^2})\end{aligned} \quad (20)$$

b) If $w_2(t) \leqslant 3$, consider increasing $w_2(t)$ if $\Delta_2 \leqslant 0$, and conversely, decrease $w_2(t)$ if $\Delta_2 > 0$.

$$\begin{aligned}\Delta_2 = &\frac{np_m^{n-1}\frac{nC}{\tau_n(t-\tau_{mcp}(t))}}{(\frac{(N-1)}{\tau_n(t-\tau_{tcp}(t))} + R_{DoS} + \frac{nw_2(t)}{\tau_n(t-\tau_{mcp}(t))})^2} \\ &\frac{1}{(1 - 3p_c(t) + 2p_c(t)^2)^2}(1 - 2p_c(t) + p_c(t)^2 - 4p_c(t)^3 \\ &- 512p_c(t)^7 + 1348p_c(t)^8 - 1300p_c(t)^9)\end{aligned} \quad (21)$$

Proof. The objective is to ensure stability while minimizing delay. To achieve this, the aim is to have $\dot{\tau}_p(t) < 0$. Referring to equation (18), it can be observed that $\dot{\tau}_p(t) = \dot{\tau}_{mcp}(t)$.

a) For the case where $w_2(t) > 3$, with $Q(w(t)) = \frac{3}{w(t)}$, the control signals delay can be described as follows:

$$\begin{aligned}\tau_{mcp}(t) = \tau_n(t) + p_c(t)((1 - \frac{3}{w_2(t)})RTT \\ + \frac{3}{w_2(t)}\frac{1 - p_c(t) - 64p_c(t)^7}{1 - 3p_c(t) + 2p_c(t)^2})\end{aligned} \quad (22)$$

Then, considering this delay, the expression for the derivative of $\tau_{mcp}(t)$ is:

$$\begin{aligned}&\dot{\tau}_{mcp}(t) = \dot{\tau}_n(t) \\ &+ \dot{p}_c(t)((1 - \frac{3}{w_2(t)})RTT + \frac{3}{w_2(t)}\frac{1 - p_c(t) - 64p_c(t)^7}{1 - 3p_c(t) + 2p_c(t)^2}) \\ &+ p_c(t)(\frac{3\dot{w}_2(t)RTT}{w_2(t)^2} - \frac{3\dot{w}_2(t)}{w_2(t)^2}\frac{1 - p_c(t) - 64p_c(t)^7}{1 - 3p_c(t) + 2p_c(t)^2} + \frac{6\dot{p}_c(t)}{w_2(t)} \\ &\frac{1 - p_c(t)^2 - 224p_c(t)^6 + 578p_c(t)^7 - 576p_c(t)^8 - 2p_c(t)}{(1 - 3p_c(t) + 2p_c(t)^2)^2})\end{aligned} \quad (23)$$

where,

$$\begin{aligned}&\dot{p}_c(t) = np_m^{n-1}(t)\dot{p}_m(t), \\ &\dot{p}_m(t) = \frac{dp_m}{dw_2}\dot{w}_2(t) + \frac{dp_m}{dw_1}\dot{w}_1(t) + \frac{dp_m}{dq}\dot{q}(t)\end{aligned} \quad (24)$$

Considering the burst DoS attack scenario, where the queue buffer size reaches a steady state ($\dot{q}(t) = 0$), and all $N-1$

nodes using classic TCP have reduced their window size to $w_1(t) = 1$, we can establish the following equations:

$$p_m(t) = 1 - \frac{C}{\frac{(N-1)}{\tau_n(t-\tau_{tcp}(t)))} + R_{DoS} + \frac{nw_2(t)}{\tau_n(t-\tau_{mcp}(t))}} \tag{25}$$

and,

$$\dot{p}_m(t) = \frac{dp_m}{dw_2}\dot{w}_2(t) = \frac{\frac{nC}{\tau_n(t-\tau_{mcp}(t))}\dot{w}_2(t)}{(\frac{(N-1)}{\tau_n(t-\tau_{tcp}(t))} + R_{DoS} + \frac{nw_2(t)}{\tau_n(t-\tau_{mcp}(t))})^2} \tag{26}$$

Our main objective in ensuring the stability of the control system under DoS attacks is to minimize delays within the communication network. This leads us to aim for $\dot{\tau}_p(t) < 0$, indicating a decrease in communication network delay. Thus, we derive the following inequality:

$$\begin{aligned}&\dot{\tau}_n(t) + \dot{p}_c(t)((1 - \frac{3}{w_2(t)})RTT + \frac{3}{w_2(t)}\frac{1 - p_c(t) - 64p_c(t)^7}{1 - 3p_c(t) + 2p_c(t)^2})\\ &+p_c(t)(\frac{3\dot{w}_2(t)RTT}{w(t)^2} - \frac{3\dot{w}_2(t)}{w_2(t)^2}\frac{1 - p_c(t) - 64p_c(t)^7}{1 - 3p_c(t) + 2p_c(t)^2} + \frac{6\dot{p}_c(t)}{w_2(t)}\\ &\frac{1 - p_c(t)^2 - 224p_c(t)^6 + 578p_c(t)^7 - 576p_c(t)^8 - 2p_c(t)}{(1 - 3p_c(t) + 2p_c(t)^2)^2}) < 0\end{aligned} \tag{27}$$

Simplifying further, this leads to:

$$\dot{w}_2(t)\Delta_1 < 0 \tag{28}$$

This inequality highlights the correlation between the change in the MCP session's window size $\dot{w}_2(t)$ and the factor Δ_1. This relationship signifies the direction that needs to be upheld in order to diminish communication network delay. This inequality signifies that when the probability of packet loss ($p_c(t)$) is increased, a reduction in delay can be accomplished by ensuring that $\dot{w}_2(t) > 0$. In the context of MCP, this suggests that under conditions of high packet loss probability, increasing the window size of MCP session can effectively contribute to a reduction in delay.

b) In cases where $w_2(t) \leqslant 3$, the queue size function is $Q(w(t)) = 1$. Consequently, the delay in control signals can be expressed as:

$$\tau_{mcp}(t) = \tau_n(t) + p_c(t)(\frac{1 - p_c(t) - 64p_c(t)^7}{1 - 3p_c(t) + 2p_c(t)^2}) \tag{29}$$

Additionally, we have the following equation:

$$\begin{aligned}\dot{\tau}_{mcp}(t) = \dot{\tau}_n(t) + \dot{p}_c(t)&\frac{1}{(1 - 3p_c(t) + 2p_c(t)^2)^2}\\ (1 - 2p_c(t) + p_c(t)^2 &- 4p_c(t)^3 - 512p_c(t)^7\\ &+ 1348p_c(t)^8 - 1300p_c(t)^9)\end{aligned} \tag{30}$$

In a manner analogous to case (a), we apply the principles discussed earlier to this scenario. Our focus is on reducing the derivative of equation (29). Therefore, $\dot{\tau}_{mcp}(t) < 0$ signifies a decrease in communication network delay over time. Taking these factors into account, we reach a conclusion similar to that of case (a), resulting in the following inequality:

$$\dot{w}_2(t)\Delta_2 < 0 \tag{31}$$

This inequality highlights that when the factor Δ_2 is negative, an increase in the MCP session's window size ($\dot{w}_2(t)$) leads us in the direction that ensures a reduction in communication network delay, thus results in upholding control system stability in the face of DoS attacks. □

An important observation arises when the MCP session's window size ($w_2(t)$), reaches its maximum limit and becomes unalterable. In such cases, $\dot{w}_2(t)$ converges to zero. This indicates the control of the window size becomes insufficient for reducing delay of CPS packets. Then controller must be adept at mitigating the repercussions of substantial delays and formulating an appropriate strategy to effectively counteract the disruptive impact of DoS attacks.

Building upon the aforementioned challenges and observations, we further addressed network delay by introducing significant modifications to the transmission protocol. These adaptations yielded a substantial reduction in overall delay; however, it is noteworthy that residual time-varying delay fluctuations persist within a certain range and satisfy $0 \leq h_1 \leq \tau_p(t) \leq h_2$ and $\dot{\tau}_p(t) \leq \mu$ where $\mu = sup\{\dot{\tau}_p(t)\}$. To achieve a more stable and predictable network performance, it becomes imperative to establish conditions under which the system maintains stability.

Theorem 1: From the system (1), let $A = A_p$ and $A_1 = -B_pK_p$. For given $0 \leq h_1 \leq h_2$ and μ, if there exist positive definite matrices P, Q_1, Q_2, Z_1, Z_2, such that the following LMI holds

$$\Xi_1 = \Xi - \begin{bmatrix}0 & -I & I & 0\end{bmatrix}^T Z_2 \begin{bmatrix}0 & -I & I & 0\end{bmatrix} < 0 \tag{32}$$

and

$$\Xi_2 = \Xi - \begin{bmatrix}0 & I & 0 & -I\end{bmatrix}^T Z_2 \begin{bmatrix}0 & I & 0 & -I\end{bmatrix} < 0 \tag{33}$$

where, $\Xi = \begin{bmatrix}\Xi_{11} & \Xi_{12} & Z_1 & 0\\ * & \Xi_{22} & Z_2 & Z_2\\ * & * & -Q_1 - Z_1 - Z_2 & 0\\ * & * & * & -Q_2 - Z_2\end{bmatrix}$

with

$$\Xi_{11} = PA + A^TP + \sum_{i=1}^{3} Q_i - Z_1 + A^T(h_1^2Z_1 + h_{12}^2Z_2)A$$
$$\Xi_{12} = PA_1 + A^T(h_1^2Z_1 + h_{12}^2Z_2)A_1$$
$$\Xi_{22} = -(1 - \mu)Q_3 + A_1^T(h_1^2Z_1 + h_{12}^2Z_2)A_1 - 2Z_2$$

and $h_{12} = h_2 - h_1$, then the delay-dependent system (1) is asymptotically stable.

Proof. The result is obtained by the following Lyapunov-Krasovskii functional and Jensen's inequality. The choice of V is inspired from [32]–[35] and adopted to the current problem.

$$\begin{aligned}V(x(t)) = x(t)^TPx(t) + \int_{t-\tau_p(t)}^{t} x(\theta)^TQ_3x(\theta)d\theta\\ + \int_{t-h_1}^{t} x(\theta)^TQ_1x(\theta)d\theta + \int_{t-h_2}^{t} x(\theta)^TQ_2x(\theta)d\theta\\ +h_1\int_{-h_1}^{0}\int_{t+\theta}^{t} \dot{x}(\eta)^TZ_1\dot{x}(\eta)d\eta d\theta\end{aligned}$$

$$+h_{12}\int_{-h_2}^{-h_1}\int_{t+\theta}^{t}\dot{x}(\eta)^T Z_2 \dot{x}(\eta) d\eta d\theta \tag{34}$$

This Lyapunov function is positive definite. Its derivative is,

$$\begin{aligned}\dot{V}(x(t)) &= \dot{x}(t)^T P x(t) + x(t)^T P \dot{x}(t)\\ &+x(t)^T Q_3 x(t) - (1-\dot{\tau}_p(t))x(t-\tau_p(t))^T Q_3 x(t-\tau_p(t))\\ &+x(t)^T Q_1 x(t) - x(t-h_1)^T Q_1 x(t-h_1))\\ &+x(t)^T Q_2 x(t) - x(t-h_2)^T Q_2 x(t-h_2))\\ &+h_1(h_1\dot{x}(t)^T Z_1 \dot{x}(t) - h_1\int_{t-h_1}^{t}\dot{x}(\eta)^T Z_1 \dot{x}(\eta)d\eta)\\ &+h_{12}(h_{12}\dot{x}(t)^T Z_2 \dot{x}(t) - h_{12}\int_{t-h_2}^{t-h_1}\dot{x}(\eta)^T Z_2 \dot{x}(\eta)d\eta)\end{aligned} \tag{35}$$

By using the Leibniz-Newton model transformation, $\int_{t-\tau_p(t)}^{t}\dot{x}(\theta)d\theta = x(t) - x(t-\tau_p(t))$, the following holds.

$$\begin{aligned}&-h_1\int_{t-h_1}^{t}\dot{x}(\eta)^T Z_1 \dot{x}(\eta)d\eta \leq\\ &-[x(t)-x(t-h_1)]^T Z_1 [x(t)-x(t-h_1)]\end{aligned} \tag{36}$$

Moreover, borrowing from the proof of theorem 1 in [32], and by defining $\alpha = (\tau_p(t) - h_1)/h_{12}$, we have:

$$\begin{aligned}&-h_{12}\int_{t-h_2}^{t-h_1}\dot{x}(\eta)^T Z_2 \dot{x}(\eta)d\eta \leq\\ &-[x(t-\tau_p(t)) - x(t-h_2)]^T Z_2 [x(t-\tau_p(t)) - x(t-h_2)]\\ &-[x(t-h_1) - x(t-\tau_p(t))]^T Z_2 [x(t-h_1) - x(t-\tau_p(t))]\\ &-\alpha[x(t-\tau_p(t)) - x(t-h_2)]^T Z_2 [x(t-\tau_p(t)) - x(t-h_2)]\\ &-(1-\alpha)[x(t-h_1)-x(t-\tau_p(t))]^T Z_2 [x(t-h_1)-x(t-\tau_p(t))]\end{aligned} \tag{37}$$

Therefore,

$$\begin{aligned}&\dot{V}(x(t)) \leq\\ &x(t)^T[PA + A^T P + \sum_{i=1}^{3} Q_i - Z_1 + A^T(h_1^2 Z_1 + h_{12}^2 Z_2)A]x(t)\\ &+x(t)^T[PA_1 + A^T(h_1^2 Z_1 + h_{12}^2 Z_2)A_1]x(t-\tau_p(t))\\ &+x(t)^T Z_1 x(t-h_1) + x(t-\tau_p(t))^T\\ &[-(1-\mu)Q_3 + A_1^T(h_1^2 Z_1 + h_{12}^2 Z_2)A_1 - 2Z_2]x(t-\tau_p(t))\\ &+x(t-\tau_p(t))^T Z_2 x(t-h_1) + x(t-\tau_p(t))^T Z_2 x(t-h_2)\\ &+x(t-h_1)^T[-Q_1 - Z_1 - Z_2]x(t-h_1)\\ &+x(t-h_2)^T[-Q_2 - Z_2]x(t-h_2)\\ &-\alpha[x(t-\tau_p(t)) - x(t-h_2)]^T Z_2 [x(t-\tau_p(t)) - x(t-h_2)]\\ &-(1-\alpha)[x(t-h_1)-x(t-\tau_p(t))]^T Z_2 [x(t-h_1)-x(t-\tau_p(t))]\\ &= X(t)^T \Xi X(t)\\ &-\alpha[x(t-\tau_p(t)) - x(t-h_2)]^T Z_2 [x(t-\tau_p(t)) - x(t-h_2)]\\ &-(1-\alpha)[x(t-h_1)-x(t-\tau_p(t))]^T Z_2 [x(t-h_1)-x(t-\tau_p(t))]\end{aligned} \tag{38}$$

where $X(t) = [x(t)^T, x(t-\tau_p(t)^T, x(t-h_1)^T, x(t-h_2)^T]^T$ and $\Xi = \begin{bmatrix}\Xi_{11} & \Xi_{12} & Z_1 & 0\\ * & \Xi_{22} & Z_2 & Z_2\\ * & * & -Q_1 - Z_1 - Z_2 & 0\\ * & * & * & -Q_2 - Z_2\end{bmatrix}$ with

$$\Xi_{11} = PA + A^T P + \sum_{i=1}^{3} Q_i - Z_1 + A^T(h_1^2 Z_1 + h_{12}^2 Z_2)A$$
$$\Xi_{12} = PA_1 + A^T(h_1^2 Z_1 + h_{12}^2 Z_2)A_1$$
$$\Xi_{22} = -(1-\mu)Q_3 + A_1^T(h_1^2 Z_1 + h_{12}^2 Z_2)A_1 - 2Z_2$$

By setting $\Xi_1 = \Xi - \begin{bmatrix}0 & -I & I & 0\end{bmatrix}^T Z_2 \begin{bmatrix}0 & -I & I & 0\end{bmatrix}$ and $\Xi_2 = \Xi - \begin{bmatrix}0 & I & 0 & -I\end{bmatrix}^T Z_2 \begin{bmatrix}0 & I & 0 & -I\end{bmatrix}$, we obtain the following quadratic inequality:

$$\dot{V}(x(t)) \leq X(t)^T((1-\alpha)\Xi_1 + \alpha\Xi_2)X(t) \tag{39}$$

Since $0 \leq \alpha \leq 1$, $\dot{V}(x(t)$ is negative if Ξ_1 and Ξ_2 are. This completes the proof. □

Continuing our efforts from the first upgrade on TCP (Section III-A), we try tackling the challenges of network delay by another enhancement to our transmission protocol. These modifications further improve our proposed approach.

C. Mitigating Exponential Backoff Factor

A significant challenge in the presence of DoS attacks lies in the exponential backoff mechanism, which can lead to increased latency and reduced packet delivery rates. In scenarios where a severe DoS attack is present, the likelihood of packet drops significantly increases. In (17), the term $\frac{1-p_c(t)-64p_c(t)^7}{1-3p_c(t)+2p_c(t)^2}$ constitutes the predominant factor contributing to delays, which consequently leads to significant latency. As a result, another effective approach to reduce latency in control systems can be optimizing the exponential backoff within the retransmission process and minimizing this term. We delve into a strategy that aims to mitigate the impact of exponential backoff within the MCP protocol, hereby referred to as the Backoff mitigating strategy (bMCP). A reduction in the exponential backoff factor yields a noteworthy reduction in latency. Noteworthy outcomes are observed when the backoff factor is set to 1. This adjustment is well-suited for time-sensitive systems. Consequently, in scenarios characterized by consecutive packet drops, the waiting time for retransmission remains constant, and equation (5) simplifies to:

$$L_k = kT_0, \quad k = 1,2,3,4,... \tag{40}$$

Subsequently, the expected latency of a timeout (TO) can be expressed as follows,

$$E(L_{TO}) = \sum_{k=1}^{\infty} prob(N_d = k)L_k = \frac{T_0}{1-p_c} \tag{41}$$

The delay by considering the optimized backoff factor and packet replication strategy can be modeled as:

$$\tau_b(t) = \tau_n(t) + p_c(t).[(1-Q(w(t))).RTT + \frac{Q(w(t))}{1-p_c(t)}] \tag{42}$$

Building upon the foundation laid out in the previous part, we continue to assume the adoption of the MCP with a parameter n as the transmission control protocol which uses backoff factor 1.

D. Enhancing stability: Latency-reducing strategy in bMCP modifications

As mentioned, maintaining stability within the control system is contingent upon the minimization of delays. In light of this, we present a proposition to address the issue.

Proposition 2: Assume the bMCP with a parameter n as the transmission control protocol for CPS (12). Additionally, consider $N-1$ TCP sessions that share a common bottleneck with our CPS. Let $p_c(t)$ denote the probability of packet drop for controller-to-plant packets, $w_2(t)$ symbolize the window size of MCP session, and $w_1(t)$ represent the window size of TCP sessions. These parameters include a new condition that serve to avert the potential destabilization of the system under the prolonged delays induced by severe DoS attacks. It is noteworthy that within this proposition, we assume $w_1(t) = 1$, and the queue $q(t)$ has reached a steady state.

a) When $w_2(t) > 3$, consider increasing $w_2(t)$ if $\Delta_3 \leqslant 0$, and conversely, decrease $w_2(t)$ if $\Delta_3 > 0$.

$$\begin{aligned}\Delta_3 = & \frac{np_m^{n-1}\frac{nC}{\tau_n(t-\tau_b(t))}}{(\frac{(N-1)}{\tau_n(t-\tau_{tcp}(t))}+R_{DoS}+\frac{nw_2(t)}{\tau_n(t-\tau_b(t))})^2} \\ & ((1-\frac{3}{w_2(t)})RTT+\frac{3}{(1-p_c(t))w_2(t)})+(\frac{3p_c(t)}{w_2(t)^2}RTT \\ & +\frac{\frac{nC}{\tau_n(t-\tau_{mcp}(t))}}{(\frac{(N-1)}{\tau_n(t-\tau_{tcp}(t))}+R_{DoS}+\frac{nw_2(t)}{\tau_n(t-\tau_b(t))})^2}\frac{3p_c(t)w_2(t)}{(1-p_c(t))^2w_2(t)^2} \\ & -\frac{3(1-p_c(t))p_c(t)}{(1-p_c(t))^2w_2(t)^2}) \qquad (43)\end{aligned}$$

b) Conversely, when $w_2(t) \leqslant 3$, to decrease delay, $w_2(t)$ should decrease.

Proof. As previoues section, we need to have $\dot{\tau}_p(t) < 0$. By the fact $\dot{\tau}_p(t) = \dot{\tau}_b(t)$,

a) For the situations where $w > 3$,

$$\tau_b(t) = \tau_n(t) + p_c(t).[(1-\frac{3}{w_2(t)}).RTT+\frac{3}{w_2(t)}\frac{1}{1-p_c(t)}] \qquad (44)$$

and,

$$\begin{aligned}\dot{\tau}_p(t) = & \dot{\tau}_n(t)+\dot{p}_c(t)((1-\frac{3}{w_2(t)})RTT+\frac{3}{(1-p_c(t))w_2(t)}) \\ & +p_c(t)(\frac{3\dot{w}_2(t)}{w_2(t)^2}RTT-\frac{3(-\dot{p}_c(t)w_2(t)+(1-p_c(t))\dot{w}_2(t))}{(1-p_c(t))^2w_2(t)^2}) \qquad (45)\end{aligned}$$

To achieve $\dot{\tau}_p(t) < 0$, we should have

$$\dot{w}_2(t)\Delta_3 < 0 \qquad (46)$$

b) On the other hand, if $w < 3$,

$$\tau_b(t) = \tau_n(t) + p_c(t).\frac{1}{1-p_c(t)} \qquad (47)$$

and,

$$\dot{\tau}_p(t) = (\dot{\tau}_n(t)+\frac{\dot{p}_c(t)}{(1-p_c(t))^2})(\tau_n(t)+\frac{p_c(t)}{1-p_c(t)}+T_p') \qquad (48)$$

to achieve a reduction in delay, it is necessary to ensure that

$$\dot{w}_2(t)\frac{np_m^{n-1}\frac{nC}{\tau_n(t-\tau_b(t))}}{(\frac{(N-1)}{\tau_n(t-\tau_{tcp}(t))}+R_{DoS}+\frac{nw_2(t)}{\tau_n(t-\tau_b(t))})^2}\frac{1}{(1-p_c(t))^2} < 0 \qquad (49)$$

In this inequality, all terms except $\dot{w}_2(t)$ are positive. Therefore, in order to make the entire expression negative, the value of $w_2(t)$ should be decreased. □

Despite the above advancements, it remains evident that residual time-varying delay fluctuations persist within a specified range, adhering to the conditions

$$0 \leq h_3 \leq \tau_p(t) \leq h_4, \quad \dot{\tau}_p(t) \leq \mu_1 \qquad (50)$$

where $\mu_1 = \sup \dot{\tau}_p(t)$ in backoff mitigation advancement.

To achieve a more robust and predictable network performance, we establish conditions to ensure system stability.

Considering the recent enhancements made to our protocol, the previously stated Theorem 1 results in the following proposed corollary:

Corollary 1: System (1) subject to (50) is asymptotically stable for given $0 \leq h_3 \leq h_4$, $(h_{34} = h_4 - h_3)$, and μ_1 if there exist positive definite matrices P, Q_1, Q_2, Z_1, Z_2, such that the following LMI holds

$$\Xi_1 = \Xi - \begin{bmatrix}0 & -I & I & 0\end{bmatrix}^T Z_2 \begin{bmatrix}0 & -I & I & 0\end{bmatrix} < 0 \qquad (51)$$

and

$$\Xi_2 = \Xi - \begin{bmatrix}0 & I & 0 & -I\end{bmatrix}^T Z_2 \begin{bmatrix}0 & I & 0 & -I\end{bmatrix} < 0 \qquad (52)$$

where, $\Xi \ = \begin{bmatrix}\Xi_{11} & \Xi_{12} & Z_1 & 0 \\ * & \Xi_{22} & Z_2 & Z_2 \\ * & * & -Q_1-Z_1-Z_2 & 0 \\ * & * & * & -Q_2-Z_2\end{bmatrix}$

with

$$\Xi_{11} = PA + A^TP + \sum_{i=1}^{3} Q_i - Z_1 + A^T(h_1^2Z_1 + h_{12}^2Z_2)A$$

$$\Xi_{12} = PA_1 + A^T(h_3^2Z_1 + h_{34}^2Z_2)A_1$$

$$\Xi_{22} = -(1-\mu_1)Q_3 + A_1^T(h_3^2Z_1 + h_{34}^2Z_2)A_1 - 2Z_2$$

IV. Experimental verification

A. Simulation results for TCP modelings

To verify the performance and effectiveness of the complete form of Reno TCP protocol in modeling, we consider the network topology in Fig. 1, and simulate it using $NS2$ with network parameteres given in [24]. The maximum window size is 20 (default value in $NS2$), the queue buffer capacity is set to 300 packets, the nominal propagation delay is considered $0.2s$ and capacity of single bottleneck is $4400packet/s$. Also we assume 100 legitimate and zero malicious sessions. On senders, the size of one packet is $500Bytes$. The application command of sessions on this simulation is CBR and TCP is used as the protocol. In previous works [24], [25], [36], the desired queue length for 100 sessions was specified as 100. Therefore, the network parameters were selected to maintain the queue length close to 100 in non-attack scenarios.

The outcomes from the NS2 network simulator and the application of both the simplified and complete TCP models are as follows: In all three scenarios, is over the desired queue length of 100 and exhibits oscillatory behavior. However, the mean queue length and the amplitude of oscillation in the simplified form of TCP, as used in [24], [36], are larger than those of the complete form. The mean and standard deviation (SD) of the queue length are as follows:

Simplified TCP: Mean = 106.16, SD = 4.35

Complete TCP: Mean = 104.98, SD = 4.12

NS2: Mean = 102.04, SD = 3.06

Following these results, it can be inferred that adopting the complete TCP model is more realistic and practical. In the subsequent sections, we will demonstrate the performance of proposed TCP modification strategies and the resilience of CPS against DoS attacks when utilizing these strategies.

B. *Performance of TCP modification strategies*

In this section, we evaluate the effectiveness of the novel TCP strategies introduced in this paper, focusing specifically on their ability to reduce latency in control system communication during DoS attacks. Additionally, we investigate their impact on packet delivery rates for controller-to-plant packets. The network parameters align closely with the specifications outlined in Section IV-A. Throughout our simulation experiments, we systematically assess the system under varying levels of DoS attack rates. The attackers consist of multiple nodes utilizing UDP sessions that continuely transmit data through the bottleneck router. The time interval for sending in all TCP and UDP sessions is set to 0.01 seconds.

1) Packet replicating strategy (MCP): In this subsection, we thoroughly explore the core of our proposed enhancement, the packet replicating strategy within the modified TCP (MCP) protocol. A key feature of MCP is its innovative packet replication strategy. To demonstrate its effectiveness, we conduct a comparative analysis of the packet delivery rate and latency experienced by control packets within the classic TCP setup ($n = 1$) and the MCP-enhanced protocol. The tangible impact of this enhancement is visualized in Fig. 3, which clearly illustrates the improvement in packet delivery rate achieved through MCP's packet replication strategy.

MCP's packet replication substantially elevates the rate of successful packet delivery, leading to an overall enhancement in the control system's performance. It is crucial to choose an appropriate replication factor (n) since an excessively high factor can negatively impact both network and CPS performance. Our experiments demonstrate that, for the given network parameters, a replication factor of $n = 3$ strikes an optimal balance. As depicted in Fig. 3, as the attack rate rises, the packet delivery rate of all TCP sessions decreases due to a reduction in their sending window size. Consequently, the packet delivery rate of MCP shows a slight increase because the decreased window size of TCP sessions enhances the probability of success for MCP packets. However, when the attack rate exceeds a certain threshold (greater than 5000 in Fig. 3), the success rate of MCP packets also decreases.

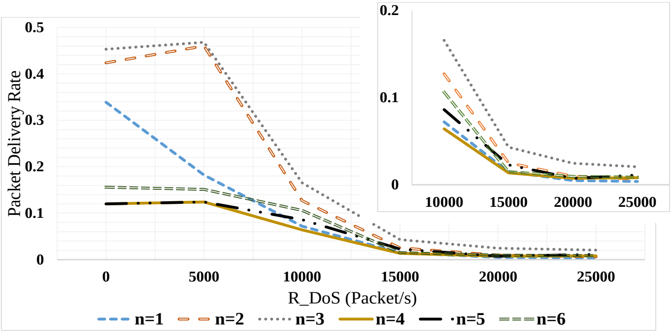

Fig. 3. Packet delivery rate of MCP with different values for n.

The effectiveness of the packet replication strategy is further confirmed by analyzing the sending window size and packet latency of the CPS when employing either TCP or MCP (with $n = 3$) under various DoS attack rates. Fig. 4, 5, and 6 illustrate MCP's clear role in enhancing system robustness and reducing latency. When MCP is employed, the system demonstrates better sending window size and packet latency compared to classic TCP during DoS attacks. Under excessively high attack rates, such as $R_{DoS} = 10000$ p/s, the performance of MCP may diminish; however, in general, the adoption of MCP enhances CPS resilience against DoS attacks.

2) Backoff mitigating strategy (bMCP): Here, we explore the strategy designed to mitigate the impact of exponential backoff within the MCP protocol (bMCP). We aim to elucidate how this strategy enhances the packet delivery rate, thereby strengthening the performance and resilience of control systems operating under severe DoS attacks.

To assess the effectiveness of the bMCP strategy, we conducted a series of simulations comparing the performance of TCP, MCP (with and without enhancement in Proposition 1), and bMCP (with and without enhancement in Proposition 2). These simulations covered varying levels of DoS attack rates, enabling a comprehensive evaluation of the strategy's impact

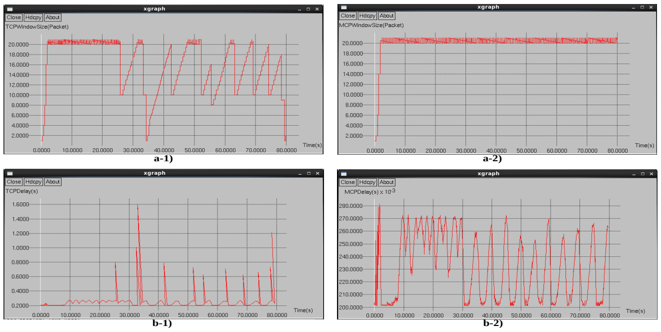

Fig. 4. Comparison of a-1) Sending window size in TCP and a-2) Sending window size in MCP (with $n = 3$), and b-1) Network latency in TCP and b-2) Network latency in MCP (with $n = 3$), for $R_{DoS} = 1000$ (packet/s).

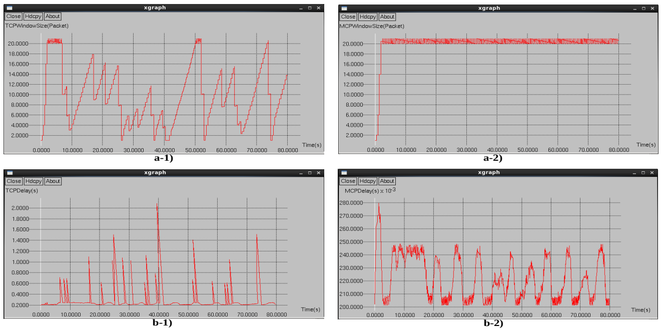

Fig. 5. Comparison of a-1) Sending window size in TCP and a-2) Sending window size in MCP (with $n = 3$), and b-1) Network latency in TCP and b-2) Network latency in MCP (with $n = 3$), for $R_{DoS} = 5000$ (packet/s).

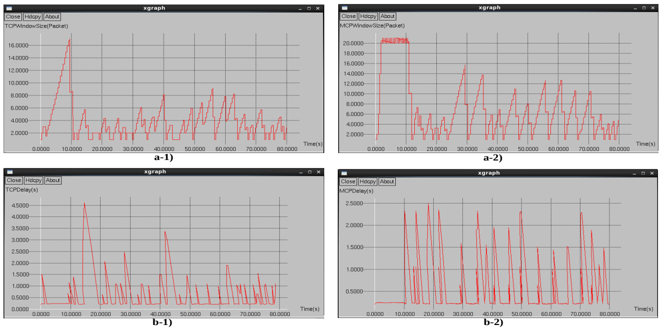

Fig. 6. Comparison of a-1) Sending window size in TCP and a-2) Sending window size in MCP (with $n = 3$), and b-1) Network latency in TCP and b-2) Network latency in MCP (with $n = 3$), for $R_{DoS} = 10000$ (packet/s).

across network conditions. The results are depicted in Fig. 7, which illustrates the packet delivery rate for classic TCP and the proposed modified strategies under various DoS attack rates. Remarkably, the results demonstrate an improvement in packet delivery rate when employing the proposed strategies.

C. Resilience of CPSs with the proposed TCP to DoS attacks

The observed conformity of the results serves as a compelling validation of the effectiveness of the new strategies in fortifying the resilience of control systems against adversarial network conditions. In this section, we examine the proposed TCP strategies, focusing on their role in enhancing the resilience of CPS against DoS attacks and network conditions.

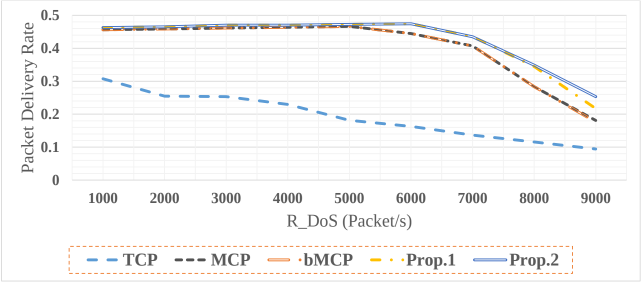

Fig. 7. Packet delivery rate for modified TCP strategies under different DoS attack rates.

Our aim is to investigate how these strategies contribute to maintaining system stability and overall performance under varying levels of network disruptions. We conduct simulations of DoS attacks spanning a range of attack rates and intensities. For each simulated attack scenario, we evaluate the impact of the proposed TCP strategies on system resilience.

As an example, we consider an Unmanned Ground Vehicle (UGV) system under DoS attacks. Through extensive analysis, we assess the stability of the closed-loop system leveraging the proposed TCP strategies. Our goal is to ascertain the tolerable DoS attack rates that ensure the system's stability.

Example: Considering the UGV under DoS attack, which is used in [24], [37]–[40],

$$\begin{bmatrix} \dot{x} \\ \dot{v} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & -0.1 \end{bmatrix} \begin{bmatrix} x \\ v \end{bmatrix} + \begin{bmatrix} 0 \\ 0.1 \end{bmatrix} F \tag{53}$$

where x, v and F denote the position, velocity, and input force of the system, respectively. It has $u_p(t) = -K_p x(t)$ with gain matrix $K_p = [3.75 \quad 11.5]$ and initial values $x_0 = [1 \quad 1]^T$.

A comprehensive evaluation was conducted using both the classic TCP and the proposed TCP variants in the communication network for the UGV system, employing the parameters specified in Section IV-A. The goal was to determine the maximum tolerable DoS attack rates that would keep the system stable, while also considering network constraints. To achieve this, simulations were done for the classic TCP and the proposed approaches in NS2. For each scenario and under varying DoS attack rates, the range of delay was calculated. The minimum delay values (h_1 and h_3) for each approach under each DoS attack rate were found to be 0.202064, while the maximum values (h_2 and h_4) are summarized in Table I. These delay values offer valuable insights into the resilience of the system under different TCP strategies. Notably, the proposed approaches show an improvement in the maximum delay compared to the classic TCP, as shown in Table I. The results were used alongside Theorem 1 and Corollary 1 to identify the DoS attack rates under which system stability is guaranteed. This determination is shown in Table II. The results demonstrate substantial improvements achieved by the proposed strategies in their resilience to disruptive attacks. As shown in the table, the maximum DoS attack rate under which system stability can be guaranteed is 900 when using the classic TCP. However, this threshold increases significantly to 5900 for MCP and bMCP, and even further to 7500 and 7600 for their enhanced versions presented in Proposition 1 and 2.

The notable increase in the maximum tolerable DoS attack rates (see Table II), underscores the effectiveness of our proposed approaches in enhancing the stability and performance of the UGV system, especially under demanding network conditions. The energy stored in the system (53), as per the Simulink results, is depicted in Fig. 8 when employing the modified TCP strategies under various attack rates. Restating the results, it is obvious that the system's energy remains relatively stable, even amidst escalating DoS attack rates, showcasing the effectiveness of the proposed TCP enhancements in maintaining system functionality and efficiency.

TABLE I
MAXIMUM RANGE OF DELAY FOR CLASSIC TCP AND PROPOSED TCP APPROACHES IN THE PRESENCE OF DOS ATTACK WITH DIFFERENT RATE.

R_{DoS}(packets/s)	TCP	MCP	bMCP	Prop. 1	Prop. 2
1000	1.702	0.479	0.479	0.481	0.481
2000	2.055	0.477	0.477	0.478	0.478
3000	2.171	0.476	0.476	0.476	0.476
4000	2.196	0.471	0.471	0.469	0.469
5000	2.182	0.471	0.471	0.470	0.470
6000	2.251	1.729	1.729	0.472	0.472
7000	2.845	2.514	2.514	0.982	0.982
8000	3.155	2.62	2.531	1.274	1.18
9000	3.701	3.282	2.953	1.472	1.317

TABLE II
MAXIMUM TOLERABLE DOS ATTACK RATE FOR CLASSIC TCP AND PROPOSED TCP APPROACHES ACCORDING TO THEOREM 1 AND COROLLARY 1 .

Transmission strategy	TCP	MCP	bMCP	Prop. 1	Prop. 2
R_{DoS}(packets/s)	900	5900	5900	7500	7600

D. Results & Discussion

The results of our investigations into the proposed TCP strategies are summarized here, shedding light on their impact on the resilience of CPSs. Our evaluations reveal several notable improvements achieved by the proposed TCP variants.

Improved packet delivery: Comparative analysis shows that the packet delivery rate is significantly enhanced when employing the proposed TCP strategies compared to the baseline. This enhancement ensures the reliable and timely delivery of crucial control information, vital for the effective functioning of CPS.

Latency reduction: One of the most significant achievements of the proposed strategies is the substantial reduction in communication latency. This latency reduction enhances the system's overall responsiveness and robustness, making it better equipped to handle abrupt changes in network conditions.

Stability enhancement: Our stability analysis underscores the effectiveness of the proposed TCP strategies in bolstering the stability of CPS. Even under the influence of severe DoS attacks, the strategies exhibit robustness, counteracting the potential destabilizing effects caused by disruptions in communication networks.

The results of our evaluation offer valuable insights into the resilience and stability enhancement achieved through the proposed TCP strategies. By improving packet delivery rates, reducing latency, and enhancing stability, our approaches address critical challenges faced by CPS operating in dynamic and potentially hostile network environments. The combination of these benefits strengthen the overall performance and reliability of CPS, ensuring their effectiveness even in the presence of challenging network conditions.

V. Conclusion

We introduced novel TCP variants aimed at enhancing the resilience and stability of Cyber-Physical Systems in challenging network conditions and against Denial of Service (DoS) attacks. Our study addresses the critical need to ensure the reliability and robustness of CPS, which often operate in dynamic and unpredictable network environments. By mitigating communication delays, packet drops, and disruptions, our proposed strategies offer significant improvements to CPS performance and reliability.

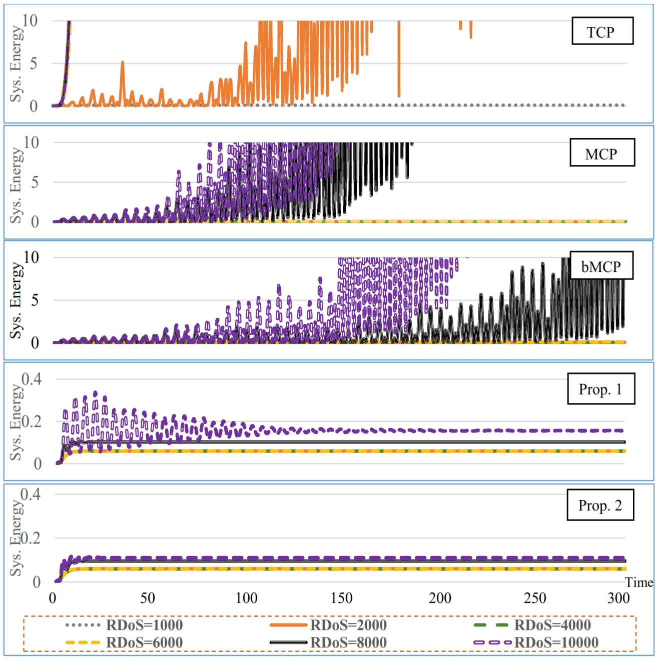

Fig. 8. Energy srored in the system (53) when utilize modified TCP strategies under different DoS attack rates.

We have introduced four improved TCP approaches for CPS. The first approach involves a modified TCP variant known as MCP, which duplicates each ready-to-send packet to increase the likelihood of successful packet delivery to the controller. The second approach focuses on enhancing MCP to minimize delay in the presence of burst DoS attacks, crucial for maintaining stability within the control system. The third approach tackles the impact of TCP's exponential backoff mechanism on latency and packet delivery rates, proposing the Backoff Mitigating Strategy (bMCP) to reduce latency. Finally, the fourth approach emphasizes minimizing delays to sustain stability within the control system through Latency-Reducing Strategy in bMCP Modifications.

Our findings contribute valuable solutions to the challenges posed by network constraints and DoS attacks in CPSs. These strategies not only improve CPS operational efficiency, but also enhance its resilience in unpredictable network environments. Future research could further enhance these strategies and evaluate their performance in real-world CPS implementations.

References

[1] P. M. Lima, M. V. Alves, L. K. Carvalho, and M. V. Moreira, "Security of cyber-physical systems: Design of a security supervisor to thwart attacks," *IEEE Transactions on Automation Science and Engineering*, 2021.

[2] M. Catillo, A. Pecchia, and U. Villano, "Cps-guard: Intrusion detection for cyber-physical systems and iot devices using outlier-aware deep autoencoders," *Computers & Security*, vol. 129, p. 103210, 2023.

[3] S. Barchinezhad and M. S. Haghighi, "Compensation of linear attacks to cyber physical systems through arx system identification," in *the 10th Information and Knowledge Technology Conference*, 2019.

[4] S. Barchinezhad, M. S. Haghighi, and V. Puig, "Identification and analysis of stochastic deception attacks on cyber physical systems," *Journal of the Franklin Institute*, vol. 361, no. 8, p. 106774, 2024.

[5] J. Liu, Z.-G. Wu, D. Yue, and J. H. Park, "Stabilization of networked control systems with hybrid-driven mechanism and probabilistic cyber attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 2, pp. 943–953, 2019.

[6] R. R. Maiti, C. H. Yoong, V. R. Palleti, A. Silva, and C. M. Poskitt, "Mitigating adversarial attacks on data-driven invariant checkers for cyber-physical systems," *IEEE Transactions on Dependable and Secure Computing*, 2022.

[7] M. Sayad Haghighi, F. Farivar, A. Jolfaei, A. B. Asl, and W. Zhou, "Cyber attacks via consumer electronics: Studying the threat of covert malware in smart and autonomous vehicles," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 4, pp. 825–832, 2023.

[8] B. K. Chejerla and S. K. Madria, "Information fusion architecture for secure cyber physical systems," *Computers & Security*, vol. 85, pp. 122–137, 2019.

[9] O. Stan, R. Bitton, M. Ezrets, M. Dadon, M. Inokuchi, Y. Ohta, T. Yagyu, Y. Elovici, and A. Shabtai, "Extending attack graphs to represent cyber-attacks in communication protocols and modern it networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 3, pp. 1936–1954, 2020.

[10] F. Farivar, M. S. Haghighi, S. Barchinezhad, and A. Jolfaei, "Detection and compensation of covert service-degrading intrusions in cyber physical systems through intelligent adaptive control," in *IEEE International Conference on Industrial Technology*. IEEE, 2019, pp. 1143–1148.

[11] Q. Zhang, K. Liu, Y. Xia, and A. Ma, "Optimal stealthy deception attack against cyber-physical systems," *IEEE transactions on cybernetics*, vol. 50, no. 9, pp. 3963–3972, 2019.

[12] M. Sayad Haghighi, F. Farivar, A. Jolfaei, and M. H. Tadayon, "Intelligent robust control for cyber-physical systems of rotary gantry type under denial of service attack," *The Journal of Supercomputing*, vol. 76, no. 4, pp. 3063–3085, 2020.

[13] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Communications surveys & tutorials*, vol. 13, no. 2, pp. 245–257, 2010.

[14] S. Barchinezhad and V. Puig, "Switching lpv approach for analysis and control of tcp-based cyber-physical systems under dos attack," *arXiv preprint arXiv:2312.02939*, 2023.

[15] D. Yue, Q.-L. Han, and C. Peng, "State feedback controller design of networked control systems," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 51, no. 11, pp. 640–644, 2004.

[16] B. Tang, G.-P. Liu, and W.-H. Gui, "Improvement of state feedback controller design for networked control systems," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 55, no. 5, pp. 464–468, 2008.

[17] J. Xiong and J. Lam, "Stabilization of networked control systems with a logic zoh," *IEEE Transactions on Automatic Control*, vol. 54, no. 2, pp. 358–363, 2009.

[18] V. Misra, W.-B. Gong, and D. Towsley, "Fluid-based analysis of a network of aqm routers supporting tcp flows with an application to red," in *Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, 2000, pp. 151–160.

[19] J. Wang, D. X. Wei, and S. H. Low, "Modelling and stability of fast tcp," in *Proc. of the Annual Joint Conference of the IEEE Computer and Communications Societies.*, vol. 2, 2005, pp. 938–948.

[20] M. Kishi, Y. Funatsu, T. Azuma, and K. Uchida, "Gain-scheduling controller design for tcp/aqm considering router queue length and time-delay," in *Annual Conference of IEEE Industrial Electronics Society*, 2005, pp. 5–pp.

[21] C.-K. Chen, Y.-C. Hung, T.-L. Liao, and J.-J. Yan, "Design of robust active queue management controllers for a class of tcp communication networks," *Information Sciences*, vol. 177, no. 19, pp. 4059–4071, 2007.

[22] C. V. Hollot, V. Misra, D. Towsley, and W. Gong, "Analysis and design of controllers for aqm routers supporting tcp flows," *IEEE Transactions on automatic control*, vol. 47, no. 6, pp. 945–959, 2002.

[23] K. B. Kim, "Design of feedback controls supporting tcp based on the state-space approach," *IEEE Transactions on Automatic Control*, vol. 51, no. 7, pp. 1086–1099, 2006.

[24] M. Azadegan, M. T. Beheshti, and B. Tavassoli, "Using aqm for performance improvement of networked control systems," *International Journal of Control, Automation and Systems*, vol. 13, no. 3, pp. 764–772, 2015.

[25] M. Azadegan and M. T. Beheshti, "Robust stability and stabilization of tcp-networked control systems with multiple delay system modeling," *Asian Journal of Control*, vol. 19, no. 3, pp. 1034–1045, 2017.

[26] V. Havary-Nassab, A. Koulakezian, and Y. Ganjali, "Denial of service attacks in networks with tiny buffers," in *IEEE INFOCOM Workshops 2009*. IEEE, 2009, pp. 1–6.

[27] M. Welzl, *Network congestion control: managing internet traffic*. John Wiley & Sons, 2005.

[28] J. Padhye, V. Firoiu, D. Towsley, and J. Kurose, "Modeling tcp throughput: A simple model and its empirical validation," in *Proc. of the ACM SIGCOMM conference on Applications, technologies, architectures, and protocols for computer communication*, 1998, pp. 303–314.

[29] N. Cardwell, S. Savage, and T. Anderson, "Modeling tcp latency," in *Proceedings IEEE INFOCOM*, vol. 3. IEEE, 2000, pp. 1742–1751.

[30] M. Allman and V. Paxson, "On estimating end-to-end network path properties," *ACM SIGCOMM Computer Communication Review*, vol. 29, no. 4, pp. 263–274, 1999.

[31] A. Kuzmanovic and E. W. Knightly, "Low-rate tcp-targeted denial of service attacks and counter strategies," *IEEE/acm transactions on networking*, vol. 14, no. 4, pp. 683–696, 2006.

[32] H. Shao, "New delay-dependent stability criteria for systems with interval delay," *Automatica*, vol. 45, no. 3, pp. 744–749, 2009.

[33] C. Briat, O. Sename, and J.-F. Lafay, "Memory-resilient gain-scheduled state-feedback control of uncertain lti/lpv systems with time-varying delays," *Systems & Control Letters*, vol. 59, no. 8, pp. 451–459, 2010.

[34] C. Briat, "Linear parameter-varying and time-delay systems," *Analysis, observation, filtering & control*, vol. 3, pp. 5–7, 2014.

[35] Q.-L. Han, "Absolute stability of time-delay systems with sector-bounded nonlinearity," *Automatica*, vol. 41, no. 12, pp. 2171–2176, 2005.

[36] M. Azadegan, M. T. H. Beheshti, and B. Tavassoli, "Design of state feedback controller based on state-dependent delay modeling for congestion control in internet," in *2013 American Control Conference*. IEEE, 2013, pp. 2728–2732.

[37] A.-Y. Lu and G.-H. Yang, "Stability analysis for cyber-physical systems under denial-of-service attacks," *IEEE Transactions on Cybernetics*, vol. 51, no. 11, pp. 5304–5313, 2020.

[38] H. Shao and Q.-L. Han, "On stabilization for systems with two additive time-varying input delays arising from networked control systems," *Journal of the Franklin Institute*, vol. 349, no. 6, pp. 2033–2046, 2012.

[39] X. Jiang and Q.-L. Han, "Delay-dependent robust stability for uncertain linear systems with interval time-varying delay," *Automatica*, vol. 42, no. 6, pp. 1059–1065, 2006.

[40] D. Huang and S. K. Nguang, "State feedback control of uncertain networked control systems with random time delays," *IEEE Transactions on automatic control*, vol. 53, no. 3, pp. 829–834, 2008.

Soheila Barchinezhad received the B.Sc. degree in Computer Science from Shahid Bahonar University of Kerman, Iran, and the M.Sc. degree in IT Engineering from the Graduate University of Advanced Technologies, Iran. She is now a Ph.D. candidate at the University of Tehran, Iran. Her research interests include Cyber-Physical Systems, Cybersecurity, and Machine Learning.

Mohammad Sayad Haghighi is an Associate Professor at the School of Electrical and Computer Engineering, University of Tehran, Iran. He is the director of Advanced Networking and Cyber Security research Lab (ANSLab). His research interests include both distributed networks and network security.

Faezeh Farivar is an Associate Professor and the Head of the Department of Computer and Mechatronics Engineering at Science and Research Branch, IAU, Tehran, Iran. Her research is focused on nonlinear control systems, cyber physical systems, and intelligent systems.

Ahmad Khonsari Ahmad Khonsari received the Ph.D. degree in Computer Science from the University of Glasgow, UK, in 2003. He is currently an Associate Professor at the School of Electrical and Computer Engineering, University of Tehran, Iran and a researcher in the School of Computer Science, Institute for Research in Fundamental Sciences (I.P.M.), Iran.