IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 1 May 2023, accepted 14 May 2023, date of publication 17 May 2023, date of current version 24 May 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3277218

RESEARCH ARTICLE

Analysis and Design of Secure Sampled-Data Control Subject to Denial-of-Service Attacks

HIRA SANA[1], GHULAM MUSTAFA[1], (Senior Member, IEEE), OWAIS KHAN[2], NOUMAN ASHRAF[3], ABDUL QAYYUM KHAN[1], (Senior Member, IEEE), MUHAMMAD ABID[1], AND HAROON UR RASHID KHAN[1], (Senior Member, IEEE)

[1]Department of Electrical Engineering, Pakistan Institute of Engineering and Applied Sciences (PIEAS), Islamabad 45650, Pakistan
[2]School for Engineering of Matter, Transport, and Energy, Arizona State University, Tempe, AZ 85287, USA
[3]School of Electrical and Electronic Engineering, Technological University Dublin, Dublin, D07 EWV4 Ireland

Corresponding authors: Nouman Ashraf (nouman.ashraf@tudublin.ie) and Ghulam Mustafa (gm@pieas.edu.pk)

This work was supported in part by the Higher Education Commission (HEC) of Pakistan; and in part by the Ministry of Planning, Development and Special Initiatives under the National Centre for Cyber Security.

ABSTRACT This study addresses the issue of secure control design for cyber-physical systems (CPS) against denial of service (DoS) attacks. We take into account a continuous-time linear system with a convex quadratic performance measure and a sampled linear state feedback control. DoS attacks impose constraints on the CPS, where packets may be jammed between the sensor and controller by a malicious entity, potentially resulting in system instability and performance degradation. We assume that the attacker can perform DoS attacks with a limited time and frequency due to energy restrictions. We devise an efficient procedure using the linear matrix inequality approach to compute an upper bound on the performance degradation brought on by the DoS attack. We also propose a redesign of the controller to minimize this performance degradation. Finally, a simulation example illustrates the computation of the performance degradation under a bounded DoS attack and the design of a secure controller. Simulation results show that the designed controller effectively keeps the feedback loop's performance and stability under attack.

INDEX TERMS Cyber-physical systems, denial-of-service attacks, secure control, linear quadratic cost, performance degradation.

I. INTRODUCTION

Cyber-physical systems embody computational, communication, and physical components. This embodiment results in enormous benefits, for example, increased interoperability and mobility. The remarkable advancement of CPSs facilitates a broader range of services and applications comprising smart homes, smart grids, supply chain, transportation, oil, and gas; however, joining the cyber and physical worlds make them an attractive target for demolishing the availability, integrity, and confidentiality of CPSs. Malicious attackers frequently research CPS weaknesses and initiate attacks that can harm system performance and even cause the feedback loop to become unstable, e.g., in Supervisory Control and Data Acquisition Systems (SCADA) [1], [2] and power grids [3], [4]. It is therefore, essential to secure CPSs from malicious activities to support their extensive implementation and deployment.

There are two main categories for cyberattacks on CPSs [5]. DoS attacks are the first category, which aim to prevent legitimate network agents from communicating with one another. DoS attacks frequently impede communication and target routing protocols [6]. Attacks that involve deception make up the second category. By obtaining the private key, the attacker in these attacks aims to change the data or compromise certain cyber components [7], [8].

The security tools using information technology security techniques only are insufficient to securely control CPSs because they cannot capture the physical behavior. They should be supplemented with secure control techniques. These techniques utilize attack models for control design, and therefore, designing a secure controller is a real challenge

The associate editor coordinating the review of this manuscript and approving it for publication was Engang Tian.

due to the unpredictable and peculiar features of attack models [9].

The problem of secure control design has received considerable attention from researchers recently. One group of researchers utilized the game theoretic methodology to attain a resilient control under cyber attacks [10], [11], [12], [13]. Another group presented attack-tolerant control techniques [14], [15]. Fault tolerant control was also applied for the design of resilient control and estimation algorithm in [16], [17], and [18]. However, fault-tolerant control is not very adequate for secure control as cyber-attacks are intentionally designed by attackers to harm the CPSs.Yet another group of researchers used model predictive control techniques for the resilient control of CPSs [19], [20].

Due to advancements in digital technology, most modern controllers are sampled-data based, which are implemented via discrete-time control schemes [21]. In contrast to continuous control, in sampled-data control, process measurements are discretized via a sampler and communicated to control node for the purpose of calculating the control signal. In this research direction, authors in [22] studied when to block communication channel of the LQR controller so that maximumm performance degradation occurs. In [23], a stabilizing controller for networked systems subject to stochastic false-data injection attacks using a hybrid aperiodic sampling technique was studied. In [24], the performance of a CPS was investigated under reset attacks. In [25], an $\mathcal{H}_\infty$ controller using the sampled-data approach is designed for networked systems experiencing a combination of DoS and deception attacks. The overall system was represented as a switching stochastic time-delay system with state feedback controller and a criteria was developed using the piecewise Lyapunov-Krasovskii functional to assure the $\mathcal{H}_\infty$ performance level of the resultant feedback loop. In [26], a resilient control design problem of an NCS under DoS attacks was presented. By capturing the time-span of the attack, the feedback system was modeled as a non-uniformly sampled system. A state-feeback controller was then designed to preserve closed-loop stability. To the authors' best knowledge, the existing results about secure control of CPSs address the stability analysis and control design problem only. The problem of investigating how much performance degradation a successful cyber-attack can cause to a feedback loop has not be studied.

The goal of this paper is to address this problem. We consider a linear time-invariant plant and a sampled-data state feedback control with linear quadratic performance criterion. Assuming that the feedback loop is already stable, we first develop a numerical procedure to study the performance degradation if a finite-energy DoS attack occurs in the feedback loop. We then develop a controller design procedure so that the performance degradation due to the DoS attack is minimized. An example of pendulum on a cart is system is then presented to illustrate the advantage of the proposed technique. This paper's major contributions are as follows:

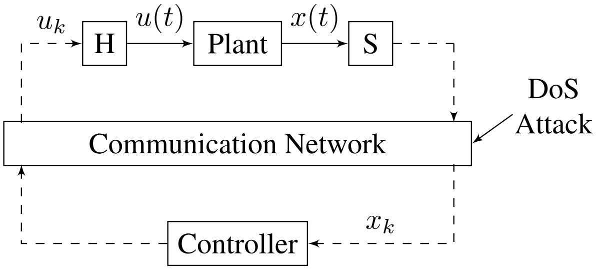


FIGURE 1. A cyber-physical system under denial-of-service attacks.

- We develop an efficient procedure in the form of a semi-definite program (SDP), to study the performance degradation caused by a finite-energy DoS attacks. The procedure can be easily solved by modern SDP solvers.
- We then develop a secure control design procedure that ensures feedback stability suffering from DoS attacks and minimizes performance degradation.

It is pertinent to mention that although the procedures for performance analysis and control design are developed for linear time-invariant systems and linear quadratic control, the approach presented here can be applied to more complex classes of systems and other performance criteria, such as $\mathcal{H}_\infty$ performance. In this context, the results presented in this paper are expected to stimulate further research on performance degradation of feedback loops under different cyber attacks.

The rest of this paper is organized as follows. Section II introduces the problem along with the plant, controller, and attack models. Section III presents the key results about performance analysis and proposes a secure control design procedure. Section IV gives an example of inverted pendulum system. Finally, conclusions are drawn in Section V.

II. PROBLEM FORMULATION

Figure 1 shows a cyber physical system. The following are the components of this system.

A. PLANT

Consider a plant with dynamics

$$\dot{x}(t) = Ax(t) + Bu(t), \quad x(0) = x_0 \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the plant state and $u(t) \in \mathbb{R}^m$ is the plant input. The matrices $A \in \mathbb{R}^{n\times n}$ and $B \in \mathbb{R}^{n\times m}$ are constant system and input matrices; respectively, and $x_0 \in \mathbb{R}^n$ is the initial state of the plant. We assume that the model in (1) is controllable.

B. SAMPLER

The measurement from the plant is sampled by the sampler S. Let t_k denote the sampling instants, then

$$x(t_k) = x(t)|_{t=t_k}$$

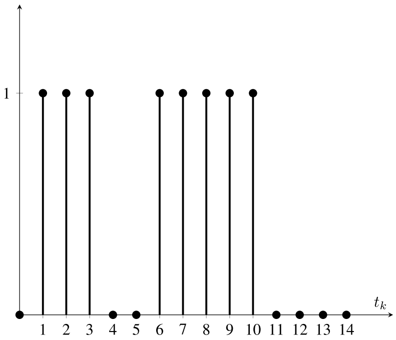


FIGURE 2. Example of a DoS attack with bounded duration and frequency.

We assume that the sampler samples periodically with a period h, that is

$$t_k = kh, \quad k \in \mathbb{Z}_{\geq 0}$$

where $\mathbb{Z}_{\geq 0}$ represents the set of non-negative integers.

C. NETWORK COMMUNICATION AND DoS ATTACK

A communication network is used to connect sensors to controllers and controllers to actuators. Let the network be real-time and network communication effects such as packet dropout and delays do not occur. We assume, however, that an attacker has gained access to the communication network. The attacker can obstruct communication between the sensor and the controller. We assume the attacker is sneaking and has finite energy, i.e, the attack duration and frequency are bounded. Such a DoS attack can be mathematically described as follows.

Let δ_k denotes the sequence of attack, where

$$\delta_k = \begin{cases} 1, & \text{when the DoS attack is active} \\ 0, & \text{otherwise.} \end{cases}$$

The j-th DoS attack interval is defined as

$$H_j \triangleq \{\delta_j\} \cup \{\delta_j, \tau_j\}$$

where $\tau_j \geq 0$ is the duration of the j-th DoS attack. Note $\tau_j = 0$ represents that the attack duration is a single instant. Let $N(k_0, k)$ denotes the number of DoS attacks and $D(k_0, k)$ denotes the union of intervals of DoS attacks during (k_0, k)

$$D(k_0, k) \triangleq \bigcup_{j \in N} H_j \bigcap (k_0, k)$$

where $\bigcup$ denotes the union operation and $\bigcap$ denote the intersection operation on sets. Let $|D(k_0, k)|$ symbolizes the total span of all attacks. We make the following assumptions about $N(k_0, k)$ and $D(k_0, k)$.

Assumption 1: There is a positive constant $T_f > 1$ satisfying

$$N(k_0, k) \leq \frac{k - k_0}{T_f} \tag{2}$$

Assumption 2: There exists $T_d > 0$ such that

$$|D(k_0, k)| \leq \frac{k - k_0}{T_d} \tag{3}$$

Assumptions 1 and 2 state that the DoS attack has a finite frequency and duration [27]. An example of a DoS attack with bounded duration and frequency is shown in Figure 2 where $N(0, 14) = 2$ and $|D(0, 14)| \leq 5$.

D. CONTROLLER

The controller is taken to be a state feedback one. Let s_k denotes the DoS-free instants, i.e., the sampling instants when successful transmission of state occurs, then

$$u(s_k) = Kx(s_k) \tag{4}$$

E. HOLD

We assume

$$u(t) = u(s_k), \quad t \in [s_k, s_{k+1}), \quad t \geq 0. \tag{5}$$

F. PERFORMANCE MEASURE

The control action is computed as

$$u(t) = \min_{u \in \mathbb{R}^m} J(x, u)$$

where

$$J(x, u) = \int_0^\infty \left(x^T(t) Q_c x(t) + u^T(t) R_c u(t) \right) dt$$

Here $Q_c \in \mathbb{R}^{n \times n}$ and $R_c \in \mathbb{R}^{m \times m}$ are parameters in our cost function. We take that R_c is positive-definite and symmetric, and Q_c is symmetric and positive semi-definite. $J(x, u)$ depends on x and u.

G. CLOSED-LOOP SYSTEM

Let $h_k = s_{k+1} - s_k$ be the duration between successful transmission instants. The behaviour of the feedback loop can then be described using (5) as follows.

$$x(t) = \Phi(t, s_k) x(s_k) + \Gamma(t, s_k) u(s_k), \quad t \in [s_k, s_{k+1}) \tag{6}$$

The state evolves at successful transmission instants s_k as

$$x(s_{k+1}) = \Phi(h_k) x(s_k) + \Gamma(h_k) u(s_k)$$

where

$$\Phi(\rho) = e^{\rho A}, \quad \Gamma(\rho) = \int_0^\rho e^{sA} ds B$$

Using (5) and (6), the cost function can be indicated in sampled form as

$$J(x, u) = \sum_{k=0}^{\infty} \begin{bmatrix} x(s_k) \\ u(s_k) \end{bmatrix}^T \Psi(h_k) \begin{bmatrix} x(s_k) \\ u(s_k) \end{bmatrix}$$

where

$$\Psi(h_k) = \begin{bmatrix} Q(h_k) & S(h_k) \\ S^T(h_k) & R(h_k) \end{bmatrix}$$
$$Q(h_k) = \int_0^{h_k} \Phi^T(s) Q_c \Phi(s) ds$$
$$S(h_k) = \int_0^{h_k} \Phi^T(s) Q_c \Gamma(s) ds$$
$$R(h_k) = \int_0^{h_k} (\Gamma^T(s) Q_c \Gamma(s) + R_c) ds \tag{7}$$

Recall that if there is no DoS attack, then $s_k = t_k$ and $h_k = t_{k+1} - t_k = h$. The feedback system becomes LTI and the state vector evolves as

$$x(k+1) = (\Phi + \Gamma K) x(k)$$

where $\Phi = \Phi(h)$, $\Gamma = \Gamma(h)$, and the performance index becomes a function of the state and h only.

$$J(x) = \sum_{k=0}^{\infty} x^T(k) \begin{bmatrix} I \\ K \end{bmatrix}^T \Psi(h) \begin{bmatrix} I \\ K \end{bmatrix} x(k)$$

The matrix K can be designed as

$$K = -(\Gamma^T P_0 \Gamma + R)^{-1} (\Gamma^T P_0 \Phi + S^T)$$

where P_0 is the solution to the equation

$$\Phi^T P_0 \Phi - P_0 - (\Phi^T P_0 \Gamma + S)(\Gamma^T P_0 \Gamma + R)^{-1} \times (\Gamma^T P + 0\Phi + S^T) + Q = 0$$

and $Q = Q(h)$, $S = S(h)$, and $R = R(h)$. The corresponding minimum value of the cost function is

$$J_{nom}(x_0) = x_0^T P_0 x_0$$

When the attack takes place, the plant's input is updated intermittently, resulting in a time-varying feedback loop and performance degradation. Let $J_{DoS}(x_0)$ denote performance measure under the DoS attack and let η denote the worst-case relative performance degradation w.r.t attack-free case. Then η can be written as

$$\eta = \sup_{x_0 \neq 0} \frac{J_{DoS}(x_0) - J_{nom}(x_0)}{J_{nom}(x_0)} \tag{8}$$

Now, we define the problem addressed in this paper.

H. PROBLEM STATEMENT

Given the process model in (1), DoS attack model in (2)-(3), controller in (4), and the feedback loop in (6),

1) what is the maximum performance degradation that a sneaking DoS attack, satisfying Assumptions (2)-(3), can cause.
2) design the controller K such that the worst-case performance degradation η is minimized. We refer to such a K as a secure controller.

III. PRIMARY OUTCOMES

We share our key findings in this section. We show how to formulate the performance degradation analysis as a maximum eigenvalue minimization problem. The controller gain is then calculated in order to minimise the maximum eigenvalue.

A. PERFORMANCE ANALYSIS OF LQ CONTROL UNDER DoS ATTACKS

We state the main result in this theorem.

Theorem 1: Given the plant in (1), the DoS attack in (2)-(3), the state feedback control in (4), and the closed-loop system in (6), the maximum performance degradation η can be calculated by solving the optimization problem below.

$$\eta = \min_P \lambda_{\max}(P, P_0) - 1$$
$$\text{s.t} \begin{bmatrix} I \\ K \end{bmatrix}^T (F(ih) + \Psi(ih)) \begin{bmatrix} I \\ K \end{bmatrix} \leqslant 0, \tag{9}$$

where $i = 1, \ldots, M$, $P \geqslant 0$, $\Psi(ih)$ is defined in (7), and $F(ih)$ is defined in (11).

Proof: Define $x_k = x(s_k)$ and consider a Lyapunov function

$$V(x_k) = x_k^T P x_k, \quad P \geq 0 \tag{10}$$

Since $P \geq 0$, therefore $V(x_k) \geq 0$, $\forall x_k \in \mathbb{R}^n$. For any k

$$\begin{aligned} \Delta V(x_k) &= V(x_{k+1}) - V(x_k) \\ &= \|(\Phi(h_k) + \Gamma(h_k)K)x_k\|_P^2 - \|x_k\|_P^2 \\ &= x_k^T \begin{bmatrix} I \\ K \end{bmatrix}^T F(h_k) \begin{bmatrix} I \\ K \end{bmatrix} x_k. \end{aligned}$$

where $\|.\|_W$ denotes the weighted norm of a respective variable. For example, for any variable $x \in \mathbb{R}^n$ and matrix $W \in \mathbb{R}^{n \times n}$, $\|x\|_W^2 = x^T W x$.

$$F(h_k) = \begin{bmatrix} \Phi^T(h_k) P \Phi(h_k) - P & \Phi^T(h_k) P \Gamma(h_k) \\ \Gamma^T(h_k) P \Phi(h_k) & \Gamma^T(h_k) P \Gamma(h_k) \end{bmatrix} \tag{11}$$

For stability, we require that $\Delta V(x_k) \leq 0$, which is satisfied if $F(h_k) \leq 0$. For performance, we require that

$$\Delta V(x_k) + J_{DoS,k}(x_0) \leq 0.$$
$$\begin{aligned} J_{DoS,k}(x_0) &= \begin{bmatrix} x_k \\ u_k \end{bmatrix}^T \Psi(h_k) \begin{bmatrix} x_k \\ u_k \end{bmatrix} \\ &= x_k^T \left(\begin{bmatrix} I \\ K \end{bmatrix}^T \Psi(h_k) \begin{bmatrix} I \\ K \end{bmatrix} \right) x_k. \end{aligned}$$
$$\begin{aligned} &V(x_{k+1}) - V(x_k) + J_{DoS,k}(x_0) \\ &\quad = x_k^T \left(\begin{bmatrix} I \\ K \end{bmatrix}^T (F(h_k) + \Psi(h_k)) \begin{bmatrix} I \\ K \end{bmatrix} \right) x_k \end{aligned}$$

Summing from $k = 0$ to $k = \infty$

$$\begin{aligned} &V(x_\infty) - V(x_0) + \sum_{k=0}^{\infty} J_{DoS,k}(x_0) \\ &= \sum_{k=0}^{\infty} x_k^T \left(\begin{bmatrix} I \\ K \end{bmatrix}^T (F(h_k) + \Psi(h_k) \begin{bmatrix} I \\ K \end{bmatrix} \right) x_k \end{aligned}$$

If

$$\begin{bmatrix} I \\ K \end{bmatrix}^T (F(h_k) + \Psi(h_k)) \begin{bmatrix} I \\ K \end{bmatrix} \leq 0, \tag{12}$$

then

$$V(x_\infty) - V(x_0) + J_{DoS}(x_0) \leq 0.$$

Since, the system is stable; therefore

$$V(x_\infty) = 0 \text{ and } J_{DoS}(x_0) \leq V(x_0).$$

Now

$$\frac{J_{DoS}(x_0) - J_{nom}(x_0)}{J_{nom}(x_0)} \leq \frac{V(x_0) - J_{nom}(x_0)}{J_{nom}(x_0)}$$

Therefore

$$\eta \leq \sup_{x_0 \neq 0} \frac{V(x_0) - J_{nom}(x_0)}{J_{nom}(x_0)}$$

$$= \lambda_{\max}(P, P_0) - 1$$

For positive-definite and symmetric matrices P and P_0, $\lambda_{\max}(P, P_0)$ is defined as

$$\begin{aligned} \lambda_{\max}(P, P_0) &= \max\{\lambda |\det(P - \lambda P_0) = 0\} \\ &= \inf\{\lambda | P \leq \lambda P_0\} \end{aligned}$$

The condition in (12) can not be directly checked because we do not know for how long the attacker will be active. However, since the attacker is sneaking and will be active for finite duration, we can take advantage of the duration bound of the DoS attack. Since the transmission instants s_k are subsets of sampling instants, therefore

$$s_k = kt_k \quad \text{for some} \quad k \in \{1, \ldots .M\}$$

where $M < T_d$, the maximum DoS attack duration. If the DoS attack is not active, then

$$s_{k+1} - s_k = t_{k+1} - t_k = h$$

otherwise

$$s_{k+1} - s_k = ih, \quad i \in \{1, \ldots, M\}.$$

The condition in (12) can be efficiently checked at $h_k = ih$ where $i \in \{1, \ldots, M\}$. This concludes the proof. ■

B. DESIGN OF THE SECURE LINEAR QUADRATIC CONTROL

In previous subsection, we assumed that the feedback control is already designed and formulated an analysis problem to study performance degradation that may occur due to the DoS attack. In this subsection, we present a method to design the controller so that the performance degradation caused by the DoS attack is minimized. This controller is called the secure controller, and the corresponding method is referred to as the secure controller design method. The following theorem expresses the result.

Theorem 2: Given the plant in (1) and the DoS attack in (2)-(3), then a secure controller K as in (4) can be computed so that the feedback loop in (6) is stable by solving the following convex optimization problem.

$$\begin{aligned} &\max_{Y, W_i, V} \lambda_{\min}(Y, P_0^{-1}) \\ &\text{s.t} \begin{bmatrix} Y & (\Phi(ih)Y + \Gamma(ih)V)^T \\ \Phi(ih)Y + \Gamma(ih)V & Y \end{bmatrix} \geq \begin{bmatrix} W_i & 0 \\ 0 & 0 \end{bmatrix} \end{aligned} \tag{13}$$

and

$$\begin{bmatrix} W_i & \begin{bmatrix} Y & V^T \end{bmatrix} \\ \begin{bmatrix} Y \\ V \end{bmatrix} & \Psi^{-1}(ih) \end{bmatrix} \geq 0$$

where $i = 1, \ldots, M$, $Y \geq 0 \in \mathbb{R}^{n \times n}$, $W_i \geq 0 \in \mathbb{R}^{n \times n}$, and matrix $V \in \mathbb{R}^{m \times n}$. The controller gain K is obtained by

$$K = VY^{-1}.$$

Proof: For the secure control design, we convert the analysis problem into the synthesis problem. The objective function involves maximization of the smallest generalized eigenvalue of matrices Y, and P_0^{-1}, which is defined as

$$\begin{aligned} \lambda_{\min}\left(Y, P_0^{-1}\right) &= \min\{\lambda | \det(Y - \lambda P_0^{-1}) = 0\} \\ &= \sup\{\lambda | Y \geq \lambda P_0^{-1}\} \end{aligned}$$

The matrix inequality condition in (9) requires that

$$\begin{bmatrix} I \\ K \end{bmatrix}^T F(ih) \begin{bmatrix} I \\ K \end{bmatrix} \leq - \begin{bmatrix} I \\ K \end{bmatrix}^T \Psi(ih) \begin{bmatrix} I \\ K \end{bmatrix}$$

using the Schur complement, we can write

$$\begin{bmatrix} -P & * \\ \Phi(ih) + \Gamma(ih)K & -P^{-1} \end{bmatrix} \leq - \begin{bmatrix} \Theta(ih) & 0 \\ 0 & 0 \end{bmatrix}$$

where $*$ denotes the corresponding symmetric term, and

$$\Theta(ih) - \begin{bmatrix} I \\ K \end{bmatrix}^T \Psi(ih) \begin{bmatrix} I \\ K \end{bmatrix} \geq 0.$$

Perform congruence transformation with $\text{diag}(P^{-1}, I)$, we obtain

$$\begin{bmatrix} P^{-1} & * \\ (\Phi(ih) + \Gamma(ih)K)\, P^{-1} & P^{-1} \end{bmatrix} \geq - \begin{bmatrix} P^{-1}\Theta(ih)P^{-1} & * \\ 0 & 0 \end{bmatrix}$$

Let $Y = P^{-1}$, $V = KP^{-1}$, and $W_i = P^{-1}\Theta(ih)P^{-1}$, then

$$\begin{bmatrix} Y & * \\ \Phi(ih)Y + \Gamma(ih)V & Y \end{bmatrix} \geq \begin{bmatrix} W_i & 0 \\ 0 & 0 \end{bmatrix}$$

Now

$$\Theta(ih) - \begin{bmatrix} I \\ K \end{bmatrix}^T \Psi(ih) \begin{bmatrix} I \\ K \end{bmatrix} \geq 0$$

Using the Schur complement, we can obtain the matrix inequality shown below.

$$\begin{bmatrix} \Theta(ih) & \begin{bmatrix} I & K^T \end{bmatrix}^T \\ * & \Psi^{-1}(ih) \end{bmatrix} \geq 0$$

Using the congruence transformation with diag(P^{-1}, I), this will result in

$$\begin{bmatrix} P^{-1}\Theta(ih)P^{-1} & * \\ \begin{bmatrix} I \\ K \end{bmatrix} P^{-1} & \Psi^{-1}(ih) \end{bmatrix} \geq \qquad 0.$$

which can be expressed as

$$\begin{bmatrix} W_i & \begin{bmatrix} Y & V^T \end{bmatrix} \\ \begin{bmatrix} Y \\ V \end{bmatrix} & \Psi^{-1}(ih) \end{bmatrix} \geq 0.$$

This completes the proof. ■

Theorem 2Â presents the secure control design procedure as a convex optimization problem that can be solved proficiently by modern state-of-the-art semi-definite solvers. We used YALMIP in conjunction with the SDPT3 solver for this paper [28], [29].

Remark 1: Sampled-data control systems have been studied in the recent past with time-varying sampling periods due to their applications in networked and embedded control systems [30]. The proposed mathematical framework can be extended to study sampled-data control design with time-varying sampling periods and denial-of-service attacks, but at the cost of more complex mathematical machinery. The matrix inequalities in Theorem 1 and 2 will become uncertain and require robust optimization tools for solution.

IV. SECURE CONTROL OF INVERTED PENDULUM UNDER DoS ATTACK

The inverted pendulum is a classic benchmark system for testing control techniques [31], [32]. Figure 3 shows a diagram of the system. It consists of a pendulum mass attached to a cart via a beam. The beam is pivoted to the cart and can freely rotate. The beam angle at the pivot point is denoted by θ. The cart only moves in the horizontal plane, at position x. The control input acting on the cart is the external force F. A nonlinear model of the system can be obtained using the Euler-Lagrange equations.

$$(M_c + m_p)\ddot{x} + b\dot{x} + m_pL\ddot{\theta}\cos\theta - m_pL\dot{\theta}^2\sin\theta = F$$
$$(l + m_pL^2)\ddot{\theta} + m_pgL\sin\theta + m_pL\ddot{x}\cos\theta = 0$$

Assume θ is small, then a linear model can be written as

$$(M_c + m_p)\ddot{x} + b\dot{x} + m_pL\ddot{\theta} = F$$
$$(l + m_pL^2)\ddot{\theta} + m_pgL\theta + m_pL\ddot{x} = 0$$

where M_c is the cart's mass, m_p is the pendulum's mass, b is the friction coefficient, and L is the length of the pendulum's center of mass. The pendulum's total length is $2L$, $I = \frac{1}{3}m_p(2L)^2$ is the pendulum's inertia, and F is the input force to the system. Define $x_1 = x$, $x_2 = \dot{x}$, $x_3 = \theta$, $x_4 = \dot{\theta}$, the states space model of the pendulum system can be expresses in the form of (1) with

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & A_{22} & A_{23} & 0 \\ 0 & 0 & 0 & 1 \\ 0 & A_{42} & A_{43} & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ B_2 \\ 0 \\ B_4 \end{bmatrix}$$

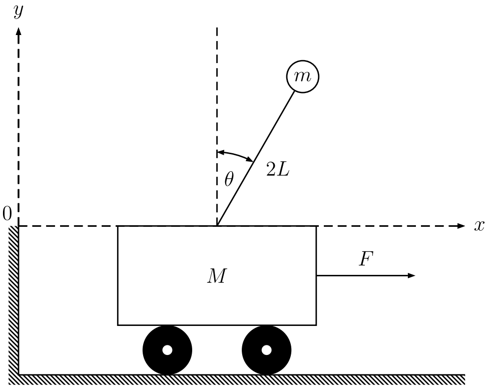


FIGURE 3. Inverted pendulum on cart system.

TABLE 1. Parameter of pendulum system.

Parameter	Value	Unit
M_c	0.5	Kg
m_p	0.5	Kg
b	0.1	Ns/m
L	0.3	m
l	0.06	Kgm^2

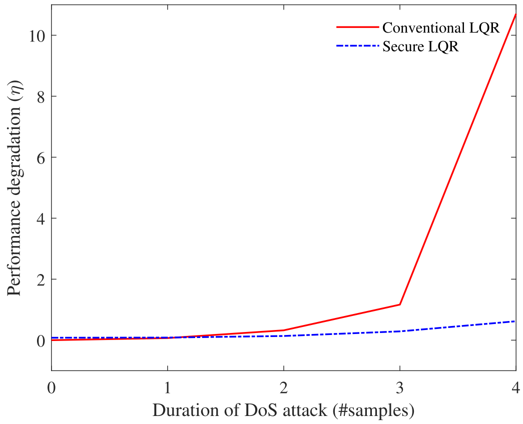


FIGURE 4. Performance degradation of LQ control under DoS attack.

where

$$\Delta_1 = 1 + m_pL^2 - \frac{m_p^2L^2}{M_c + m_p}$$

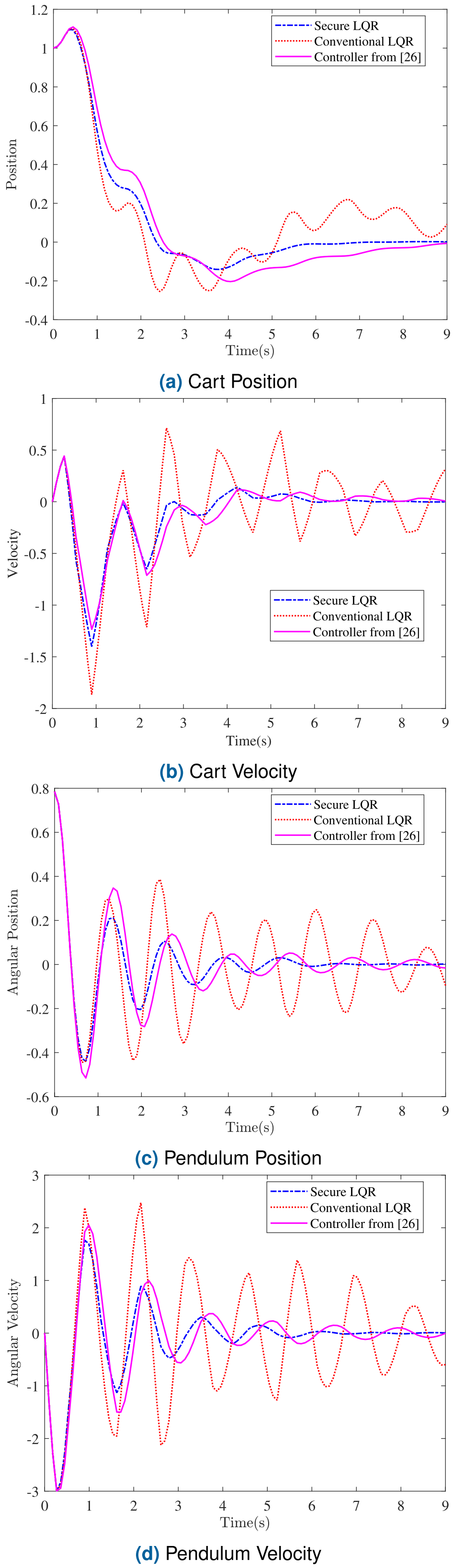
$$\Delta_2 = M_c + m_p - \frac{m_p^2L^2}{1 + m_pL^2}$$

$$A_{22} = -\frac{b}{\Delta_2}, \quad A_{23} = \frac{m_p^2L^2g}{\Delta_2(I + m_pL^2)}$$

$$A_{42} = \frac{m_pLb}{\Delta_1(M_c + m_p)}, \quad A_{43} = -\frac{m_pgL}{\Delta_1}$$

$$B_2 = \frac{1}{\Delta_1}, \quad B_4 = -\frac{m_pL}{\Delta_1(M_c + m_p)}$$

Table 1 shows the parameter values for the pendulum system.



(a) Cart Position

(b) Cart Velocity

(c) Pendulum Position

(d) Pendulum Velocity

FIGURE 5. State response of Inverted pendulum under secure (dashed-dotted curve) conventional (dotted curve), and resilient control (solid curve).

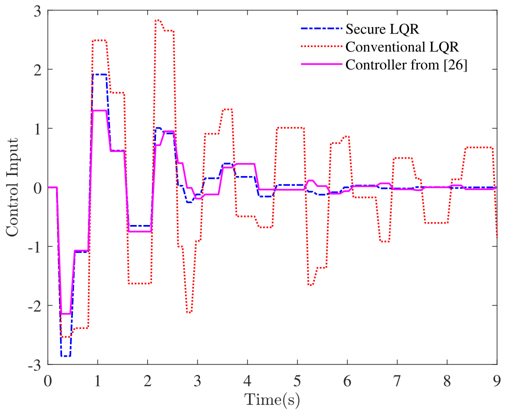


FIGURE 6. Control input.

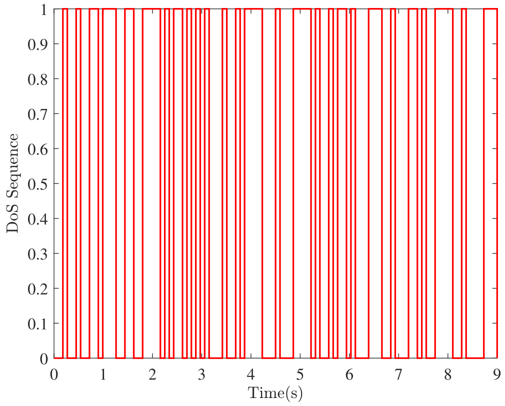


FIGURE 7. DoS sequence.

Assuming a sampling period of 0.09 seconds and $Q_c = I_4$ and $R_c = 1$, an LQR control can be designed to stabilize the feedback loop. The resulting controller gain matrix is shown below.

$$K_{\text{conv}\_\text{LQR}} = \begin{bmatrix} -0.8593 & -1.5027 & 0.5522 & 0.6387 \end{bmatrix}$$

For the same parameters, Q_c, R_c, and sampling period, we also design a secure LQ control using Theorem 2. The resulting secure controller gain matrix is shown below.

$$K_{\text{sec}\_\text{LQR}} = \begin{bmatrix} -0.4961 & -0.9557 & -1.7492 & 0.4526 \end{bmatrix}$$

We use Theorem 1 to compute the performance degradation when a malicious attacker blocks the communication of the state information to the controller. We make the assumption that the attacker cannot block more than four consecutive packets. Figure 4 shows the relative performance degradation of the LQ control under DoS attacks. We see that the performance is significantly deteriorated if the attacker blocks more than three consecutive transmissions. The performance degradation of the closed-loop sampled-data system when secure control is used is also shown in Figure 4. It can be easily seen that the secure control exhibits significant resilience as compared to the conventional LQ control. Table 2 gives percentage relative performance degradation as a function of the Dos attack duration. The resilience of the proposed secure

TABLE 2. Relative performance degradation of inverted pendulum system under DoS attacks.

DoS Attack Duration (M)	Conventional LQR η (%)	Secure LQR η (%)
1	6.96%	8.55%
2	32.35%	13.77%
3	116.67%	28.91%
4	1070.49%	62.10%

control is evident. These demonstrate the efficacy of the proposed method. Following that, we compute the feedback system's response with initial condition $x_0 = \begin{bmatrix}1 & 0 & \pi/4 & 0\end{bmatrix}^T$. In addition to the conventional LQR and secure LQR controllers, we also design a DoS resilient controller using the Proposition 3 in [26] with $N = 2$, $\epsilon_1 = 1$, $\epsilon_2 = 1$, $h_m = T = 0.09$s, and $h_M = 5T$. The resulting controller gain is

$$K_{26} = \begin{bmatrix}-0.4388 & -0.7554 & -1.1849 & 0.3348\end{bmatrix}$$

Figures 5a-5d, 6, and 7 show the state, control input and DoS attack sequence. Figure 7 shows that the attacker frequently blocks the communication channel, resulting in disruption of measurements sent to the controller. The conventional LQR controller is unaware of the DoS attack, as shown in Figures 5a-5d; as a result, the state of the feedback system suffers from undesirable transients. The controller in [26] exhibits better performance because it is DoS resilient; however, it ensures asymptotic stability only and does not optimize performance. On the other hand, it can be seen that the secure controller is very effective in dealing with transients caused by communication channel blocking. The conventional LQR controller's inability to handle a DoS attack is also evident from the significant control effort required to keep the closed-loop stable, as shown in Figure 6. In contrast to the conventional control and the control in [26], the secure control requires significantly less energy.

V. CONCLUSION

We have presented an efficient technique to numerically evaluate the performance degradation of cyber-physical systems modelled by linear time-invariant plants and subjected to sneaking DoS attacks. The procedure is in the form of a semi-definite program that can be efficiently solved using modern solvers. We also presented a method for designing a secure controller that minimizes the performance degradation caused by a DoS attack. A simulation example of the benchmark inverted pendulum system demonstrated the effectiveness of the proposed technique. The proposed method can be applied to more complex models of CPSs, such as hybrid systems. Also, other types of control structures, such as $\mathcal{H}_\infty$ control, can be considered.

REFERENCES

[1] A. Rahman, G. Mustafa, A. Q. Khan, M. Abid, and M. H. Durad, "Launch of denial of service attacks on the modbus/TCP protocol and development of its protection mechanisms," *Int. J. Crit. Infrastruct. Protection*, vol. 39, Dec. 2022, Art. no. 100568.

[2] S. Huda, J. Yearwood, M. M. Hassan, and A. Almogren, "Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks," *Appl. Soft Comput.*, vol. 71, pp. 66–77, Oct. 2018.

[3] C. Pu, P. Wu, and Y. Xia, "Vulnerability assessment of power grids against link-based attacks," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 10, pp. 2209–2213, Oct. 2020.

[4] S. Lai, B. Chen, T. Li, and L. Yu, "Packet-based state feedback control under DoS attacks in cyber-physical systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 66, no. 8, pp. 1421–1425, Aug. 2019.

[5] Z.-H. Pang, L.-Z. Fan, H. Guo, Y. Shi, R. Chai, J. Sun, and G.-P. Liu, "Security of networked control systems subject to deception attacks: A survey," *Int. J. Syst. Sci.*, vol. 53, no. 16, pp. 3577–3598, Dec. 2022.

[6] X. Wang and G. Yang, "Cooperative attack strategy design via H_I/H_∞ scheme for linear cyber-physical systems," *Int. J. Robust Nonlinear Control*, vol. 30, no. 1, pp. 33–50, Jan. 2020.

[7] H. Sun, Y. Cui, L. Hou, and K. Shi, "Adaptive finite-time control for cyber-physical systems with injection and deception attacks," *Appl. Math. Comput.*, vol. 430, Oct. 2022, Art. no. 127316.

[8] N. He, K. Ma, and H. Li, "Resilient predictive control strategy of cyber–physical systems against FDI attack," *IET Control Theory Appl.*, vol. 16, no. 11, pp. 1098–1109, Jul. 2022.

[9] M. S. Mahmoud and Y. Xia, *Cloud Control Systems: Analysis, Design and Estimation*. New York, NY, USA: Academic, 2020.

[10] J. Sun, P. Li, and C. Wang, "Optimise transient control against DoS attacks on ESS by input convex neural networks in a game," *Sustain. Energy, Grids Netw.*, vol. 28, Dec. 2021, Art. no. 100535.

[11] Y. Yuan, H. Yuan, L. Guo, H. Yang, and S. Sun, "Resilient control of networked control system under DoS attacks: A unified game approach," *IEEE Trans. Ind. Informat.*, vol. 12, no. 5, pp. 1786–1794, Oct. 2016.

[12] R. Meira-Góes, E. Kang, R. H. Kwong, and S. Lafortune, "Synthesis of sensor deception attacks at the supervisory layer of cyber–physical systems," *Automatica*, vol. 121, Nov. 2020, Art. no. 109172.

[13] L. Xue, B. Ma, J. Liu, and Y. Yu, "Jamming attack against remote state estimation over multiple wireless channels: A reinforcement learning based game theoretical approach," *ISA Trans.*, vol. 130, pp. 1–9, Nov. 2022.

[14] S. Bezzaoucha Rebaï, H. Voos, and M. Darouach, "Attack-tolerant control and observer-based trajectory tracking for cyber-physical systems," *Eur. J. Control*, vol. 47, pp. 30–36, May 2019.

[15] J.-W. Zhu, Y.-P. Yang, W.-A. Zhang, L. Yu, and X. Wang, "Cooperative attack tolerant tracking control for multi-agent system with a resilient switching scheme," *Neurocomputing*, vol. 409, pp. 372–380, Oct. 2020.

[16] G. Wen, X. Zhai, Z. Peng, and A. Rahmani, "Fault-tolerant secure consensus tracking of delayed nonlinear multi-agent systems with deception attacks and uncertain parameters via impulsive control," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 82, Mar. 2020, Art. no. 105043.

[17] J. Li, Z. Yang, X. Mu, and X. Wu, "Passivity-based event-triggered fault tolerant control for nonlinear networked control system with actuator failures and DoS jamming attacks," *J. Franklin Inst.*, vol. 357, no. 14, pp. 9288–9307, Sep. 2020.

[18] M.-Y. Su and W.-W. Che, "Fault-tolerant control for model-free networked control systems under DoS attacks," *J. Franklin Inst.*, vol. 358, no. 17, pp. 9023–9033, Nov. 2021.

[19] Q. Sun, K. Zhang, and Y. Shi, "Resilient model predictive control of cyber–physical systems under DoS attacks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 7, pp. 4920–4927, Jul. 2020.

[20] B. Zhang and Y. Song, "Asynchronous constrained resilient robust model predictive control for Markovian jump systems," *IEEE Trans. Ind. Informat.*, vol. 16, no. 11, pp. 7025–7034, Nov. 2020.

[21] J. Skaf and S. Boyd, "Analysis and synthesis of state-feedback controllers with timing jitter," *IEEE Trans. Autom. Control*, vol. 54, no. 3, pp. 652–657, Mar. 2009.

[22] J. Zhou, J. Shang, Y. Li, and T. Chen, "Optimal DoS attack against LQR control channels," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 4, pp. 1348–1352, Apr. 2021.

[23] K. Bansal and P. Mukhija, "Aperiodic sampled-data control of distributed networked control systems under stochastic cyber-attacks," *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 4, pp. 1064–1073, Jul. 2020.

[24] Y. Ni, Z. Guo, Y. Mo, and L. Shi, "On the performance analysis of reset attack in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 65, no. 1, pp. 419–425, Jan. 2020.

[25] P. Zeng, F. Deng, X. Gao, and X. Liu, "Sampled-data resilient H_∞ control for networked stochastic systems subject to multiple attacks," *Appl. Math. Comput.*, vol. 405, Sep. 2021, Art. no. 126265.

[26] X. Zhang, Q. Han, X. Ge, and L. Ding, "Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3616–3626, Aug. 2020.

[27] C. De Persis and P. Tesi, "Input-to-State stabilizing control under denial-of-service," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 2930–2944, Nov. 2015.

[28] J. Lofberg, "YALMIP: A toolbox for modeling and optimization in MATLAB," in *Proc. IEEE Int. Conf. Robot. Autom.*, 2004, pp. 284–289.

[29] K.-C. Toh, M. J. Todd, and R. H. Tütüncü, "SDPT3—A MATLAB software package for semidefinite programming, version 1.3," *Optim. Methods Softw.*, vol. 11, nos. 1–4, pp. 545–581, 1999.

[30] O. Khan, G. Mustafa, A. Q. Khan, and M. Abid, "Robust observer-based model predictive control of non-uniformly sampled systems," *ISA Trans.*, vol. 98, pp. 37–46, Mar. 2020.

[31] X. Wang, E. E. Yaz, S. C. Schneider, and Y. I. Yaz, "H_2–H_∞ control of continuous-time nonlinear systems using the state-dependent Riccati equation approach," *Syst. Sci. Control Eng.*, vol. 5, no. 1, pp. 224–231, 2017.

[32] X. Wang, J. Long, W. Sun, and W. Lian, "The generalized state dependent Riccati equation control of continuous time nonlinear systems," in *Proc. ASME Int. Mech. Eng. Congr. Expo.*, vol. 46476, 2014, pp. 1–14.

HIRA SANA received the B.Sc. degree in electrical engineering from International Islamic University Islamabad, Pakistan, in 2011, and the M.S. degree in electrical engineering from the Center for Advanced Studies in Engineering, University of Engineering and Technology (UET) Taxila, Taxila, Pakistan, in 2016. She is currently pursuing the Ph.D. degree in electrical engineering with specialization in control systems engineering with the Pakistan Institute of Engineering and Applied Sciences (PIEAS), Islamabad, Pakistan. Her research interests include sampled data control, robust control, and the security of industrial control systems.

GHULAM MUSTAFA (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from UET Lahore, Lahore, Pakistan, in 2002, the M.Sc. degree in systems engineering from the Pakistan Institute of Engineering and Applied Sciences (PIEAS), Islamabad, Pakistan, in 2004, and the Ph.D. degree in control systems from the University of Alberta, Edmonton, Canada, in 2012. Since 2020, he has been a Professor with the Department of Electrical Engineering, PIEAS. He is the author of a book chapter, more than 50 articles, and an invention. His current research interests include sampled-data control, robust control, and the security of industrial control systems. He is the Chair of the IEEE Control Systems Society's Lahore-Karachi-Islamabad Joint Chapter, and a Life-Member of the Pakistan Engineering Council and the Golden Key International Honor Society.

OWAIS KHAN received the B.Sc. degree in electronics engineering from UET, Peshawar, Pakistan, in 2011, the M.S. degree in electrical engineering with specialization in control systems from COMSATS University, Islamabad, Pakistan, in 2016, and the Ph.D. degree in electrical engineering with specialization in control systems from the Pakistan Institute of Engineering and Applied Sciences (PIEAS), Islamabad, in 2020. After his Ph.D. degree, he joined the Control Systems Engineering Laboratory, Arizona State University, Tempe, USA, as a Postdoctoral Research Scholar. His research interests include robust model predictive control, fault diagnosis, LMI-based optimal control, state estimation, and the application of control system theory to different dynamical systems related to (but not limited to) robotics, chemical processes, and behavioral medicine.

NOUMAN ASHRAF received the Ph.D. degree in electrical engineering from Frederick University, Cyprus, under the Erasmus Mundus Scholarship Program. He was with the Turku University of Applied Sciences, Finland, the TSSG, Waterford Institute of Technology, Ireland and University of Cyprus. Currently, he is with Technological University Dublin, Ireland. His research interests include the application of control theory for management of emerging networks with applications in the Internet of Things, 5G and beyond communication networks, electric vehicles, and smart grid.

ABDUL QAYYUM KHAN (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Duisburg-Essen, Germany, in December 2010. He is currently a Professor with the Department Electrical Engineering, Pakistan Institute of Engineering and Applied Sciences (PIEAS). He is the Secretary of the IEEE Control System Society's Karachi-Lahore-Islamabad Joint Chapter. His research interests include fault diagnosis in technical processes, linear and nonlinear observer design, the robust control of nonlinear systems, and LMI-based optimal design.

MUHAMMAD ABID received the M.Sc. degree in systems engineering from the Pakistan Institute of Engineering and Applied Sciences (PIEAS), Islamabad, in 2004, and the Ph.D. degree from the Institute of Automatic Control and Complex Systems, University of Duisburg Essen, Germany, in 2010. Currently, he is a Professor with PIEAS. His research interests include model-based fault detection in nonlinear systems, robust, and optimal control.

HAROON UR RASHID KHAN (Senior Member, IEEE) received the bachelor's degree in electrical engineering from the University of Engineering and Technology, Lahore, Pakistan, in 1990, the M.S. degree in electrical engineering from Iowa State University (ISU), USA, in 1999, and the Ph.D. degree from the School of Computer Science and Technology, Beijing Institute of Technology (BIT), in 2009. He is currently a Senior Faculty Member with the Department of Electrical Engineering, Pakistan Institute of Engineering and Applied Sciences (PIEAS). His research interests include digital design in Verilog, digital communication, microprocessor-based design, and digital image processing.