International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I5P223

Volume 70 Issue 5, 209-220, May 2022

Original Article

Mitigating Effect of Uncertain Exogenous Dynamics by Parametric Performance Improvement with Optimal Control Design

Brijraj Singh Solanki[1], Renu Kumawat[2], Seshadhri Srinivasan[3]

[1]*Research Scholar, Electronics and Communication Engineering, Manipal University Jaipur, Rajasthan, India*
[2]*Associate Professor, Computer and Communication Engineering, Manipal University Jaipur, Rajasthan, India*
[3]*Professor, Instrumentation and Control Engineering, Kalasalingam Academy of Research and Education, TamilNadu, India*

brij_raj_ic@yahoo.com

Received: 07 February 2022 Revised: 10 April 2022 Accepted: 23 April 2022 Published: 23 May 2022

Abstract - *Emerging development in networked control systems has been observed by integrating sensors, controllers, and actuators. The networked control systems (NCSs) are used in various fields due to ease of installation, reduced maintenance, system wiring, and diagnosis. However, the real-time communications via a network of NCS drive it towards vulnerable to the intended adversary attacks. The crucial information traveling through communication networks is more susceptible to being accessed by intruders to degrade the control performance of the networked system. This paper investigates the designing of an optimal controller through integrating principles of H-infinity loop-shaped design to improve the system performance under uncertain exogenous dynamics, i.e., network delay, packet loss (0, 5%, 15%, 20%, 25%, 30%), and other attacks. To detect the intrusive behavior in NCS, the Bernoulli distribution process is employed to model the packet loss probability. The proposed methodology presents the good tracking of reference, improved transient performance, and robust stability margin in a real-time system. Finally, to justify the proposed optimal control design methodology, a numerical simulation is performed whose result ensures mitigating the effects due to uncertain exogenous input.*

Keywords - *Networked control system, Uncertain exogenous input, Packet loss, H-infinity loop-shaped design procedure, Delays, and Attacks.*

1. Introduction

The networked control system has become an emerging field where components are connected remotely through a real-time communication network [1]. Many systems rely on the secure transmission of packets/data through a communication channel to improve the system's performance. The NCS has many applications such as oil and gas plants, energy distribution, water control management, robotics, process industries, vehicle transportation, space-craft, medical treatment, etc. [2], [3]. The packets/data containing confidential information are transmitted through a network that may be vulnerable to attack. The agent can access the information through various means such as breaching the network protocols and hacking, inducing denial of service (DoS), eavesdropping, and service-degradation (SD) attacks [4]. An agent may launch the uncertain exogenous inputs, i.e., delays, packet losses, and attacks in either direction of NCS, to degrade the performance.

In literature, various attacks such as Denial-of-Service, replay, and unwanted data injection attacks have been reported, intended to degrade the performance. The well-known examples of such attacks are the German Steel Mill, Maroochy Water, Stuxnet worm attack, Davis-Besse power plant attack, etc. [5], [6]. In the literature review process, the effect of uncertain exogenous dynamic inputs, i.e., packet losses, delay, and attack, on the performance of NCS is undertaken. The intruder aims to extract the information of NCS to design an intended attack and may interrupt the process.

This paper aims to achieve desired and robust performance with the following contributions.

- Design an optimal controller using H-infinity loop-shaping design procedure to improve the performance parameter of the Industrial networked control system (iNCS) against the uncertain exogenous condition.
- To detect the intrusive behavior in iNCS, the Bernoulli distribution process is used to model packet loss probability.

- The proposed design methodology incorporates the obtained robustness/performance tradeoff with the loop-shaping principle to guarantee stable conditions.

The rest of the paper is organized as follows: The extensive recent literature works are presented in section-2. Subsequently, section-3 describes the problem identification considering uncertain exogenous input and the proposed methodology to evaluate the optimal controller design using H-infinity loop-shaping theory. The section-4 discusses the simulation results obtained considering the optimal control design methodology. At the end of section-5, concluding remarks with the future scope is presented.

2. Literature Work

The effect on the stability due to disturbances caused by the packet loss in the networked system is framed with Lyapunov functions and designed the model-predictive controller, which showed the robustness and effectiveness of the presented methodology [7]. In [8], delays and packet losses in the control system are studied. By using protocols and security, reliable communication is possible while maintaining integrity, authenticity, and confidentiality. The estimation of the state was evaluated using the Kalman filtering approach, and the predictive controller is designed to determine the fault in the sensor node. The fault detection (FD) in the sensor is performed using the parity relation method while taking the effect of network uncertainty. Networked uncertainty was defined as packet loss, delays, and unwanted inputs [9], [10]. A filter was designed to detect a fault in the NCS which has undergone delay and time-varying sampling [11], [12]. Also, the stability condition is briefed using LMIs and the Lyapunov function to show the robustness and sensitivity against disturbance. An adaptive regulator was designed using the linear-quadratic (LQR) approach to compensate for time delays in NCS [13].

Issues related to the performance of the networked system with time-dependent sampling and packet dropout were discussed in [14], [15]. Further, the H-infinity controller was presented to show the method's effectiveness under defined uncertainty. The communication constraints, i.e., packet disorder, packet loss, and networked delay, play a critical role in degrading the performance of networked systems. To improve performance, a predictive control system (based on error) is designed considering the uncertainty and disturbance [16], [17]. For developing the optimal control algorithm to predict states – (i) input, (ii) output, and (iii) reference data were used, and the Riccati equation obtained the solution. The stability of a stochastic wireless networked system is proposed by defining the exponentially mean-square stability criteria with considerable delay and packet loss under a multiple transmission policy [18]. The ZigBee network for the closed-loop system showed the proposed method's effectiveness. A comparative analysis of adverse effects due to delay in the wireless network is simulated using conventional and fuzzy proportional-integral-derivative control. The fuzzy control action improved performance over conventional control action [19], [20]. To secure the NCS against cyber-attack (i.e., Denial of Service and Deception attacks), symmetric key encryption methodology and hash-based message authentication code are used [21]. The developed secure system showed improved performance indices and the identification of attacks. The attack model is designed for the estimated system to compromise the actual networked system using a system identification tool [22]. The networked-predictive control algorithm is employed to design an optimal predictive controller. It compensates for packet loss and denial of service attack, which is introduced in either direction of the networked-control system [23], [24]. Furthermore, in [25], [26], mitigation of effect due to denial of service attack was addressed, and detection/prediction of such attacks have been presented in [27], [28].

In [29], [30], authors have designed a controller using Linear Quadratic Gaussian (LQG) control method. They have incorporated imperfections and demonstrated the efficacy of the proposed technique through deriving stability conditions. The problem of packet dropout in the multi-hop NCS is discussed by designing the stochastic model-predictive control algorithm, which minimizes the quadratic cost function for the given control input and state [31]. Degradation of control performance problems related to communication resources and transmission energy wastage are discussed in [32]. A self-triggered control mechanism is developed using the model-predictive control method to overcome the problem. The performance can be improved further by employing the Kalman filter and state estimator while utilizing the network resources. In [33], the author presented an algorithm that detects the injection attack introduced by an agent. The designed algorithm introduces time-varying coding matrices to protect the measured data, which restricts the agent from doing good estimation using measured data for launching the attack. The parametric performance problem due to packet loss and induced delay in the NCS is investigated by designing the controller based on fuzzy logic and the Pade approximation method. The nonlinear characteristics of the system are approximated by fuzzy logic and delay with the Pade approximation. It has been observed that the designed adaptive controller expresses the robustness and effectiveness of the proposed methodology [34].

Furthermore, in [35], to compensate for the problem due to packet loss, a data-driven predictive control strategy using a dynamic linearization scheme is adopted, which predicts the system's output. It is shown that the proposed methodology applies to open-loop and nonlinear unstable systems. The delay and non-Gaussian disturbances are presented for NCS to evaluate the performance parameters and optimal control sequence using a linear quadratic performance index by minimizing the entropy [36]. The tracking control problem under the networked-induced delay using the Lyapunov functions is studied in [37], [38]. It is shown that using the proposed methodology and performance tracking can be improved by minimizing the networked-induced error. In [39], [40], the stability problem due to packet-dropout and networked delay in NCS are investigated by defining the mean-square stability conditions. The packet dropouts are modeled through the independent-identically distributed Bernoulli process, and stability theorems are also established by solving algebraic Riccati equations. In [41], [42] author briefed on the performance problem occurring due to attack and bandwidth constraints on the NCS. The author demonstrated that stability could be maintained against such uncertainty by designing the adaptive controller based on an event-triggered mechanism. By defining the Lyapunov-Krasovskii approach and LMIs solutions, suitable asymptotical-stability conditions are derived, which express the improved dynamical behavior of the system. The author in [43] designed a guaranteed-cost-control method for NCS experienced packet-loss through the Lyapunov function through quantization feedback. The term exponential stability is introduced to show the effect of packet loss and delay in a nonlinear-networked control system [44]. To synthesize the effect of quantized signal and packet loss in NCS, a quantized optimal controller is designed considering the mean-square stability (MSS) condition with the Lyapunov function [45]. The robust optimal control strategy deals with uncertainties in the nonlinear-networked system by solving the Hamilton-Jacobi-Bellman equation by approximation method [46]. The networked model-predictive control and neural network are used to evaluate the performance of nonlinear NCS under packet dropout and networked delay [47]. Herein, the packet dropouts are expressed using Bernoulli distribution and multi-rate sampling to showcase the efficacy of the introduced methodology. The performance issues in NCS were addressed through the design of LQG control while considering the effect of the data dropout on stability. Here, packet dropouts are evaluated assuming white process noise. The set of stability conditions and probability of arrival rate of the data packets are evaluated by solving the LMIs and algebraic-Riccati-equations [48]. Table 1 and 2 illustrates a comparative analysis of different techniques/tools used for NCS performance with uncertain dynamics and attacks.

Table 1. Comparative analysis of techniques/tools used for NCS performance with uncertain dynamics

Issues	Techniques/Tool	Achievement	Limitation/Gaps	References
Packet losses and uncertain delays	Bernoulli process, LMI, Markov jump linear system, MSS	Response convergence faster	Transient performance analysis not covered	[49], [50]
Uncertainty and disturbance	Predictive control system	Improved tracking performance	Improvement of transient and steady-state performance are area of concerns	[16], [17], [51], [52]
Packet loss and Time-varying delay	Pseudo-partial-derivative (PPD) method, Switched system approach	Compensating delay and packet loss	Performance improvement is the area of concern, including packet loss	[53], [54]
Nonlinear time delay	Neural network with predictive control, dynamic Bayesian network	Outstanding reference input tracing and rejection of disturbance	Slightly improvement in transient response, peak overshoot, and settling time reduces	[55], [56]
Network-delay dynamics	SOC system	Reduced overshoot, fast convergence time, reduction in the cost function	Mitigation of attacks not presented	[57]
Time delay and Packet dropout	Markov chain, linear matrix inequality method	Improved robustness and sensitivity against disturbance	Transient and steady-state terms to be considered for packet loss	[58], [59], [60]
Networked-Induced delay, packet dropouts	Round-trip delay (RTD), MFAC, LMI method	Compensate for the RTT delay, guarantee stability and steady-state tracking error to zero	Steady-state value is not encouraging as for local control system	[61], [62]

Table 2. Comparative analysis of techniques/tools used for NCS performance with attacks

Issues	Techniques/Tool	Achievement	Limitation/Gaps	References
System identification attacks	Random switching controller	Resisting attackers to accurate modeling of plant	Increase in settling time	[63]
DoS, FDI attack	NPC algorithm, LMIs, MSS, H-infinity controller	Detection and effect of attack studied	Uncertainty in NCS and transient performance not considered, design of optimal policy	[64], [65], [66], [67]
Deception attack and network constraints	NPC algorithm	Detect and compensate deception attack	Control goes worsens with increasing data loss	[68]
Adversary attack	Adaptive control	Demonstrated the impact of attacks	No uncertainty was included, and more deviation in transient performance	[69]

The maximum allowed DoS attack within the NCS communication channel is discussed in [70]. Using the Lyapunov function, a set of stability conditions is derived, which illustrates the efficacy of the designed approach. The presence of networked delay, modeled using the Markov chain, degraded the response of the networked system [71]. Feedback gain and stability conditions are derived by adopting the cone-complementarity-linearization (CCL) algorithm. The control performance and security issues in the growth of NCS are addressed using the term ‘control over networks and control of networks’ [72], and the wormhole attack detection algorithm was presented in [73].

Furthermore, performance index parameters for NCS under DoS attacks are evaluated by designing the switching-based event-triggered-control mechanism [1]. Subsequently, sufficient and suitable stability criterion conditions were also derived to show the effectiveness of the designed methodology, which effectively processed the transmission of data packets. The improved performance of the NCS (which has undergone uncertain exogenous dynamics) is investigated by designing a controller with the concept of the LQG control, Kalman filtering, and proportional-integral-derivative (PID) control action [74], [75]. Delays in discrete-NCS are modeled using the Markov process. Sufficient stability conditions are derived using LMI and Lyapunov stability function, which determined the gains of state-observer and stochastic-controller [76], [77]. In [78], the optimal control strategy was adopted for designing the optimal controller for an event-triggering-based networked-control system under the stochastic nature of delay using the Markov jump theory. The optimal manipulated variable was derived using the dynamic programming mechanism to show the improved performance index [79].

It is observed that the performance of the NCS is severely affected by the intrusion of the uncertain exogenous input. The intrusion may be classified as packet loss, delays, attacks, mainly denial of service (DoS) and service-degradation (SD) attacks. The above-mentioned exogenous inputs must be studied in detail from the point of stabilizing the networked system. In literature, it is noticed that exogenous input, i.e., packet losses, delays, and intended intrusive attacks, have not been reported altogether in the real-time communication network for estimation of the performance of the networked system. This study motivates the design of an optimal controller by employing the H-infinity loop-shaping design principles and considering all uncertain exogenous input.

3. Description of Problem Formulation and Controller Designing

3.1. iNCS Designing with Uncertain Exogenous Input Dynamics

The basic block diagram representation of iNCS with uncertain exogenous input dynamics is shown in Figure 1. In the design of iNCS, uncertain exogenous parameters such as packet losses, delay, and intended intrusive attacks are considered, which may severely affect the stability of the control system. These exogenous inputs may be presented in either direction of the control system when transmitting the signal to and from the controller through a real-time communication channel/network. The continuous-time plant dynamics with exogenous uncertainties is defined in equation (1) and (2)

$$\dot{x}(t) = Ax(t) + \xi(t)Bu(t-T) + \xi(t)D\omega(t-T) \quad (1)$$

$$y(t) = C\,x(t) \quad (2)$$

where the term $x(t) \in \Re^n$ is the input vector, control vector is $u(t) = \Re^m$, measured output vector is defined as $y(t) \in \Re^p$, and $\omega(t) \in \Re^l$ is the uncertain exogenous input. The total delay is represented by T $\xi(t)$ the packet arriving at t the instant. The system matrices A, B, C, D considered are inappropriate dimensions. The τ_1 τ_2 and are termed the delay from the sensor to controller and controller to the actuator, respectively. It is expected that packets can be transferred efficiently when the sampling time is larger than the processing delay and induced delay (i.e., $\tau_s > \tau_1 + \tau_2 +$ processing delay).

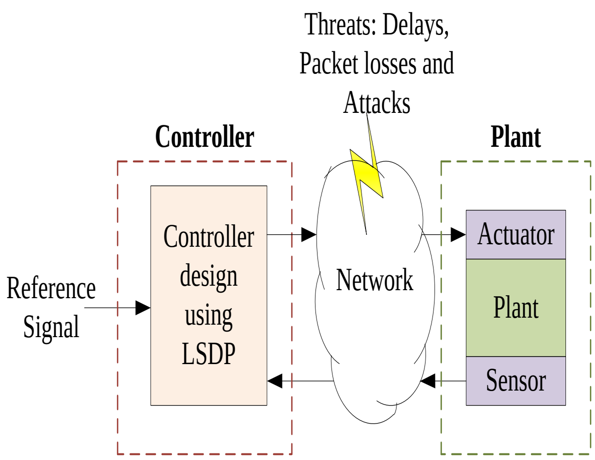

Fig. 1 iNCS design with LSDP

The controller and actuator work on the recent available signal/packet received through a communication network. So, the controller and actuator considered are event-based, which sample the signals in sampling intervals $[k\tau_s, (k+1)\tau_s) \forall k$. An intruder may intentionally drop the packet while transmitting via a communication channel. The probability of packet dropouts can be represented as

$$p_r(\xi_k) = \begin{cases} p_r, & if\ \xi_k = 1 \\ 1 - p_r, & if\ \xi_k = 0 \end{cases} \tag{3}$$

where $p_r \in [0 \quad 1]$ represent the packet lost probability and $\xi_k = 1$ for successful packet transmission, otherwise $\xi_k = 0$. In the sampling interval, $[k\tau_s, (k+1)\tau_s) \forall k$ the state equation with uncertain exogenous inputs is represented as [80]

$$\begin{aligned} x(k+1) = A_0 + \sum_{i=0}^{\sigma-1} \xi_{(k-i)} B_i^k u_{(k-i)} \\ + \sum_{i=0}^{\sigma-1} \xi_{(k-i)} D_i^k \omega_{(k-i)} \end{aligned} \tag{4}$$

where $A_0 = \exp(A\tau_s)$ $B_i^k = \int \exp[A(\tau_s - \tau)] d\tau B$ $D_i^k = \int \exp[A(\tau_s - \tau)] d\tau D$ delay bound is defined as σ $i = 0, 1, 2.....\sigma - 1$ and. Based on exogenous input, i.e., delays and packet losses augmented state and output are expressed as $h_{k+1} = \phi_{hk} h_k + \Gamma_{hk} u_k + D_{hk} \omega_k$, and $y_k = C_{hk} h_k$, respectively. Here h_k is the augmented state-vector, which is defined as $h_k = \begin{bmatrix} x_k^{'} & u_{k-\sigma}^{'} & \omega_{k-\sigma}^{'} \end{bmatrix}^{'}$. The augmented system matrices are defined as

$$\phi_{hk} = \begin{bmatrix} A_0 & \cdots & \xi_{k-\sigma} B_\sigma^k & \cdots & \xi_{k-\sigma} D_\sigma^k \\ 0 & \cdots & 0 & \cdots & 0 \\ 0 & I_m & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & I_m & 0 \end{bmatrix},$$

$$\Gamma_{hk} = \begin{bmatrix} \xi_k B_0^k \\ I_m \\ 0 \\ \vdots \\ 0 \end{bmatrix}, D_{hk} = \begin{bmatrix} \xi_k D_0^k \\ 0 \\ I_l \\ \vdots \\ 0 \end{bmatrix},$$

$$C_{hk} = diag\begin{bmatrix} C & I_m & I_l \end{bmatrix} \tag{5}$$

3.2. Proposed Optimal Controller Design using H-infinity Loop-Shaping Theory

In this section, H-infinity loop-shaping controller is used to confirm the system stability against uncertainty and provide robust stability to the iNCS. The loop-shaping theory is used to shape the frequency response within bounds. This improves the robust stability and performance of the system.

As shown in Figure 2, the following procedures are used for designing the controller using the loop-shaped design methodology.

3.2.1. Loop-Shaping

In the nominal plant P , singular values are shaped to extract the desired open-loop shape. This is done using the pre-compensator ω_{c1} and the post-compensator ω_{c2} , as shown in Figure 2(a). The nominal shaped plant is defined as $P_s = \omega_{c2} P \omega_{c1}$. The value of the pre-compensator ω_{c1} and the post-compensator ω_{c2} is chosen such that there are no hidden modes in the shaped plant, P_s

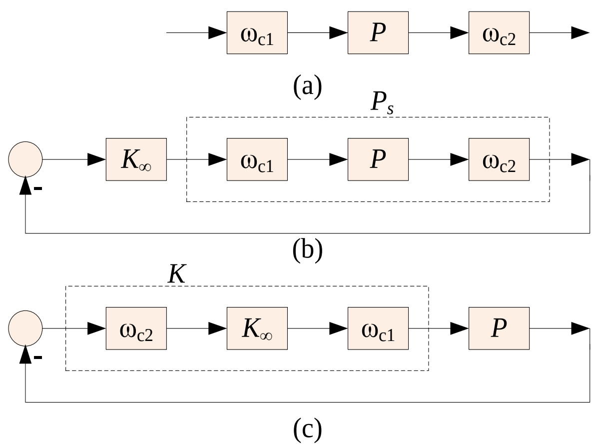

Fig. 2 Design of feedback controller using loop-shaping design procedure

3.2.2. Robust Stabilization

Maximum stability margin $\varepsilon_{\max}$: The following expression defines the calculation for maximum stability margin [81].

$$\varepsilon_{\max}^{-1} \triangleq \inf_{\text{K Stabilizing}} \left\| \begin{bmatrix} I \\ K \end{bmatrix} (I + P_s K)^{-1} \tilde{M}_s^{-1} \right\|_\infty \tag{6}$$

K Where is the stabilizing controller? Normalized co-prime factors $\tilde{M}_s^{-1} \tilde{N}_s$ are defined such that $P_s = \tilde{M}_s^{-1} \tilde{N}_s$ $\tilde{M}_s \tilde{M}_s^* + \tilde{N}_s \tilde{N}_s^* = I$ and. The term $\|\cdot\|_\infty$ is H_∞ the norm. If $\varepsilon_{\max} << 1$, then adjust the value of the pre-compensator ω_{c1} and the post-compensator ω_{c2} . The normalized left co-prime factorization $\tilde{M}_s$ $\tilde{N}_s$ is defined as

$$\begin{bmatrix} \tilde{N}_s & \tilde{M}_s \end{bmatrix} = \left[\begin{array}{c|cc} A + HC & B + HD & H \\ \hline R^{-1/2} C & R^{-1/2} D & R^{-1/2} \end{array} \right] \tag{7}$$

The $Z \geq 0$ and $X \geq 0$ are the solutions of two (generalized filter and control) algebraic Riccati equations as given below [82]

$$\begin{aligned} &\left(A - BR^{-1} D^T C\right) Z + Z \left(A - BR^{-1} D^T C\right)^T \\ &- ZC^T R^{-1} CZ + B\left(I - D^T R^{-1} D\right) B^T = 0 \end{aligned} \tag{8}$$

$$\begin{aligned} &\left(A - BS^{-1} D^T C\right)^T X + X \left(A - BS^{-1} D^T C\right) \\ &- XBS^{-1} B^T X + C^T \left(I - DS^{-1} D^T\right) C = 0 \end{aligned} \tag{9}$$

where $H = -\left(ZC^T + BD^T\right) R^{-1}$;
$R = I + DD^T$ and $S = I + D^T D$.

Now select $\varepsilon \leq \varepsilon_{\max}$ and synthesize K_∞ stabilizing controller, as shown in Figure 2(b), such that

$$\begin{aligned} &\left\| \begin{bmatrix} I \\ K_\infty \end{bmatrix} (I + P_s K_\infty)^{-1} \tilde{M}_s^{-1} \right\|_\infty \\ &= \left\| \begin{bmatrix} I \\ K_\infty \end{bmatrix} (I + P_s K_\infty)^{-1} \begin{bmatrix} I & P_s \end{bmatrix} \right\|_\infty \leq \varepsilon^{-1} \end{aligned} \tag{10}$$

The closed-loop robust stability is maximized by minimization of the above expression such that

$$\gamma_{\min} = \inf_{\text{K Stabilizing}} \left\| \begin{bmatrix} I \\ K \end{bmatrix} (I + P_s K)^{-1} \tilde{M}_s^{-1} \right\|_\infty \tag{11}$$

The expression can also be defined as

$$\gamma_{\min} = \frac{1}{\sqrt{\left(1 - \left\| \tilde{N}_s \quad \tilde{M}_s \right\|_H^2\right)}} \tag{12}$$

were the term $\|\cdot\|_H$ represents the Hankel norm and is expressed as

$$\left\| \tilde{N}_s \quad \tilde{M}_s \right\|_H^2 = \lambda_{\max}(ZX(I + ZX)^{-1}) \tag{13}$$

The $\lambda_{\max}(\cdot)$ denotes the maximum eigenvalue and $\gamma_{\min}$ can be represented as

$$\gamma_{\min} = \sqrt{\left(1+\lambda_{\max}\left(ZX\right)\right)} \tag{14}$$

The $\gamma > \gamma_{\min}$ following expression can derive the controller

$$K \triangleq \left[\begin{array}{c|c} A+BF+\gamma^2\left(L^T\right)^{-1} ZC^T\left(C+DF\right) & \gamma^2\left(L^T\right)^{-1} ZC^T \\ \hline B^T X & -D^T \end{array}\right] \tag{15}$$

where $F = -S^{-1}\left(D^T C + B^T X\right)$ $L = \left(1-\gamma^2\right)I + XZ$;

a) Feedback controller:

K As presented in Figure 2(c), the feedback controller is calculated using the loop-shaping compensator ω_{c1} and ω_{c2} an H-infinity controller K_∞ $K = \omega_{c1} K_\infty \omega_{c2}$.

4. Discussion of Result with Numerical Simulation

The proposed optimal control design methodology is presented in this section, along with numerical simulation work performed on the MATLAB Simulink and Control System toolbox. For a better understanding of the designing concept, an example of a DC motor is considered as a plant model. The continuous-time dynamical model of the DC motor plant is expressed as [83] $G_p = 4410/\mathrm{s}^2 + 439.7\mathrm{s} + 536.4$. The pre-compensator transfer function is defined as $G_c = (0.003416s^2 + 1.19s + 19.15)/s$, and the value of the post-compensator is one. The sampling period used in the simulation is 0.2 seconds. The plant dynamics are represented in differential equation form as

$$\begin{aligned} y(k) &= 0.783y(k-1) + 8.693e^{-17}y(k-2) \\ &+ 1.766u(k-1) + 0.01801u(k-2) \end{aligned} \tag{16}$$

$$e(k) = r(k) - y(k) \tag{17}$$

The system is stable with the eigenvalues -438.5096, -1.2232. The stability of iNCS is also analyzed in this section while considering the different uncertain exogenous inputs. An attacker may intentionally introduce the exogenous input into the system in either direction of iNCS. In this section, different exogenous input i.e. packet loss (0, 5%, 15%, 20%, 25%, 30%), delay and attacks are considered for performance degradation evaluation. The optimal controller for iNCS is designed using the H-infinity loop-shaping design procedure by incorporating different uncertain exogenous inputs (responsible for performance degradation). The proposed optimal control design for iNCS shows effective results under-considered detrimental conditions. The efficacy of the proposed design can be understood with various simulation results, which are graphically presented in Figures 3 to 8.

The response of the actual system and system under the influence (packet losses, attack, and delay) is shown in Figure 3. It can be inferred that the output trajectory/response of iNCS under exogenous input dynamics (packet losses such as 0, 5, 15%, introduced delays, and intended intrusive attack) is improved compared to the actual iNCS. Responses are of the same order due to employing the proposed design (loop-shaping design principles), indicating an efficient optimal controller design.

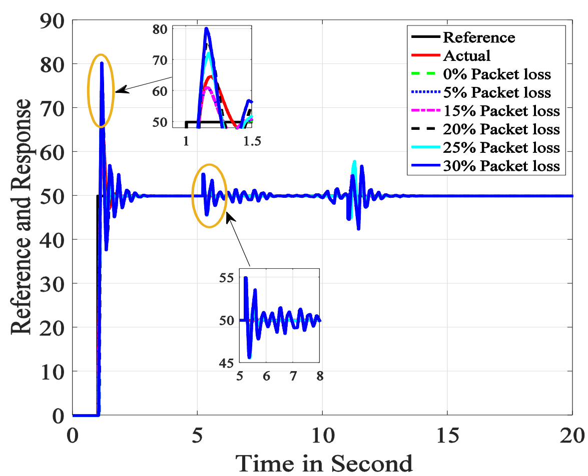

Fig. 3 iNCS output response with the proposed design

The iNCS performance is marginally degraded for packet stability due to disturbances caused by the packet loss losses of 20%, 25%, and 30%, introduced delay and attack, but output still converges soon. This is the indicator of the effectiveness of the proposed design and methodology. The parametric performance evaluation in terms of overshoot, rise time, peak value, and peak time are shown in Table 3. The attacks introduced into the iNCS at 5 and 11 seconds with different packet loss rates can be seen in Figure 3. After introducing attacks, the system gets slightly disturbed but tracks the reference signal well in a short period. This is due to the presence of the proposed optimal control design methodology. From Table 3, it is inferred that response of the system under attack and different packet losses such as 0, 5, and 15% is improved than that of the actual system and the same order. But as the packet loss rate further increased to 20%, 25%, and 30%, the response slightly degraded but was still in the acceptable range due to optimal control design.

The control signal computed under uncertain exogenous input with optimal control strategy shows better performance than an actual system, as shown in Figure 4. Still, control signal computation has somewhat deviated for packet losses of 20, 25, and 30% delay and attack. It is shown that under attack (at 5 and 11 seconds for a different packet loss rate), the control signal computation is still converging, and control performance is good.

Table 3. Statistical analysis of response under packet loss and attack employing optimal control design methodology

Parameters	Actual System	Packet loss with attack					
		0%	5%	15%	20%	25%	30%
Overshoot (%)	29.22	22.84	22.84	22.84	53.07	44.20	60.48
Rise time (m-sec)	73.41	64.21	64.21	64.21	35.4	47.66	49.54
Peak value	64.72	61.16	61.16	61.16	75.9	72.30	80.31
Peak time (sec)	1.18	1.15	1.15	1.15	1.16	1.17	1.15

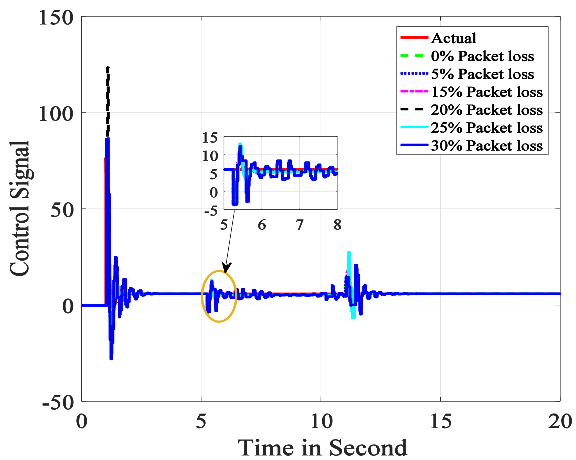

Fig. 4 Control signal under attack and different packet loss rate

Figure 5 shows the error curve for the networked system under different uncertain exogenous input conditions. It can be verified that the error curve converges fast, even after the application of attack and different packet loss, due to employing an optimal loop-shaping design procedure.

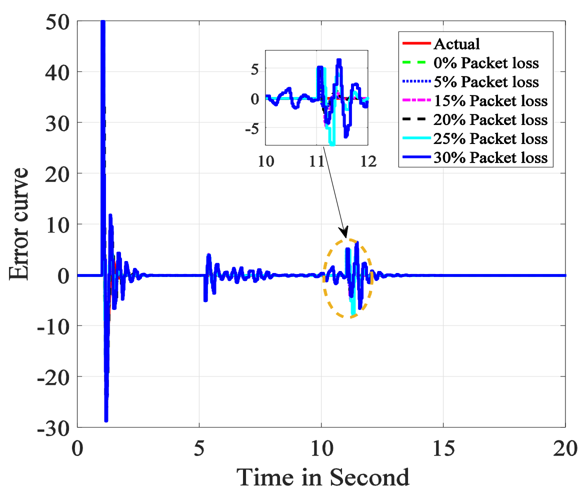

Fig. 5 Error curve with attack and packet loss

In Figure 6, packet losses in a real-time communication network are shown. Herein, only 15% and 25% packet loss is presented to show the clarity of packet loss rate in the networked system. The packet losses are represented in a selected shaded area.

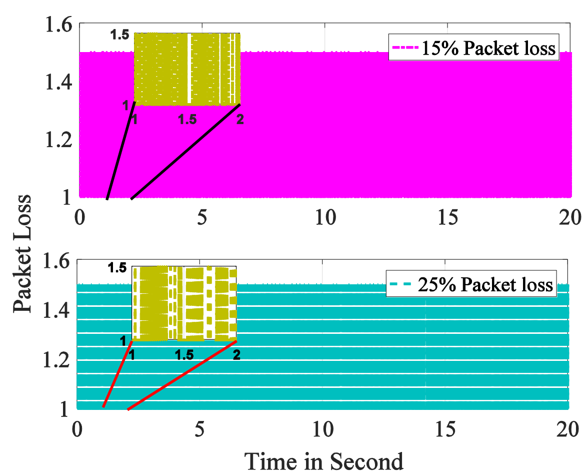

Fig. 6 Packet loss in the real-time communication network

To further analyze the effect of uncertain exogenous input on the performance of iNCS, frequency analysis for actual and computed response (in terms of power spectral density) is shown in Figure 7. The power spectral density of estimated output for a packet loss rate of 30% exhibits slight performance degradation. However, the system is still stable and converging due to the optimal control design.

Round trip time delays with different rates of packet losses and attacks are shown in Figure 8. It is inferred that the invalid packet rejection increases RTT delays but still shows better control performance.

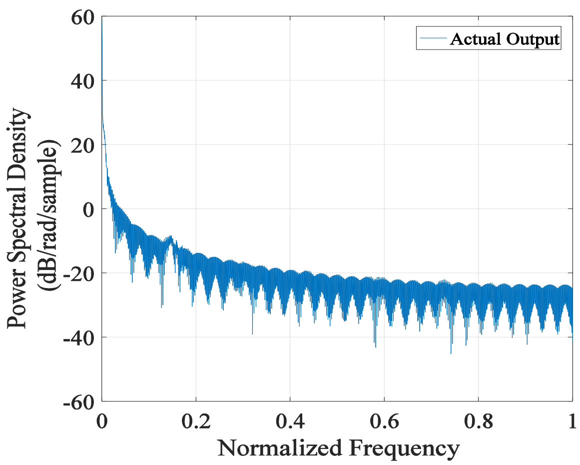

Fig. 7 (a)

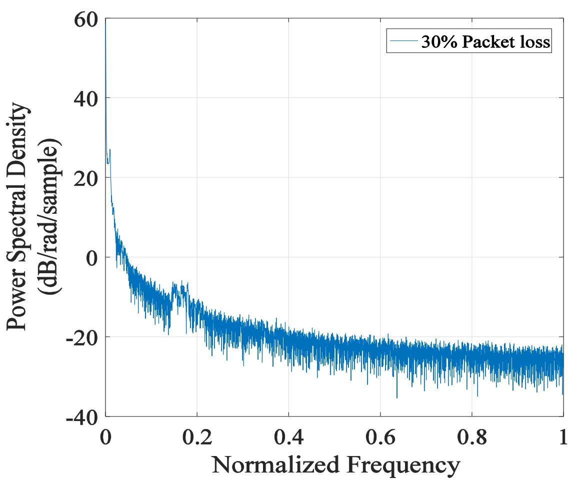

Fig. 7 (b)

Fig. 7 Power spectral density of (a) actual and (b) estimated output under uncertain exogenous input

5. Conclusion and future work

An optimal controller is investigated for an iNCS that has undergone uncertain exogenous dynamic input, i.e., network delay, packet loss (0, 5, 15, 20, 25, 30%), and attack. Herein, H-infinity loop-shaping design principles are used to design the controller, which mitigates effects due to uncertain exogenous intended intervention in iNCS. Uncertain exogenous input may be intentionally introduced into iNCS in either direction of the control system through a real-time communication network. Such interventions are designed to degrade the system performance, which drags the iNCS to the verge of instability.

The designed optimal controller improves performance with system response, control signal, and error curve under such uncertain exogenous conditions. The parametric performance in terms of overshoot, rise time, peak value, and peak time are shown in Table 3. It is inferred that the output trajectory/response of iNCS undergoing exogenous dynamics input (packet losses such as 0, 5, and 15%; introduced delays and intended intrusive attack) is improved over than actual iNCS, and responses are of the same order, due to employing proposed design (loop-shaping design principle) which is an indicator of efficient optimal controller design. The iNCS performance is marginally degraded with packet losses of 20, 25, and 30%, introduced delay and attack. But the output still converges soon, which indicates the effectiveness of the proposed design and methodology.

Future research will include the secure transmission of data packets under uncertain exogenous input conditions while maintaining the desired performance.

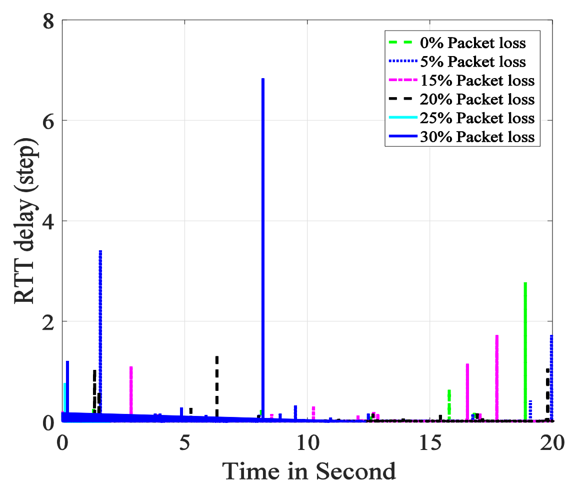

Fig. 8 RTT delay under different packet loss and attack

Conflicts of Interest

The author(s) declare(s) that there is no conflict of interest regarding the publication of this paper.

References

[1] R. Gupta and M. Y. Chow, Networked Control System: Overview and Research Trends, IEEE Transactions on Industrial Electronics. 57(7) (2009) 2527-2535.

[2] H. Zhang, P. Cheng, L. Shi, and J. Chen, Optimal DoS Attack Scheduling in Wireless Networked Control System, IEEE Transactions on Control Systems Technology. 24(3) (2016) 843–852.

[3] P. R. Dunaka and B. McMillin, Cyber-physical Security of a Chemical Plant, Proceedings of IEEE International Symposium on High Assurance Systems Engineering. (60) (2017) 33–40.

[4] J. Zhang and C. Peng, Guaranteed Cost Control of Uncertain Networked Control Systems with a Hybrid Communication Scheme, IEEE Transactions on Systems, Man, and Cybernetics: Systems. 50(9) (2020) 3126–3135.

[5] M. Pajic, J. Weimer, N. Bezzo, O. Sokolsky, G. J. Pappas, and I. Lee, Design and Implementation of Attack-Resilient Cyberphysical Systems: Focus on Attack-Resilient State Estimators, IEEE Control Systems. 37(2) (2017) 66–81.

[6] N. Zhao, P. Shi, W. Xing, and J. Chambers, Observer-Based Event-Triggered Approach for Stochastic Networked Control Systems Under Denial of Service Attacks, IEEE Transactions on Control of Network Systems. 65(9) (2020) 3943–3949.

[7] C. F. Caruntu and R. C. Rafaila, Robust MPC for Networked Control Systems with Data-Packet Dropouts Modeled as Disturbances, 21st International Conference on System Theory, Control and Computing, ICSTCC. (2017) 152–157.

[8] F. Y. Chemashkin and A. A. Zhilenkov, Problems in Network Control Systems and their Solutions, Proceedings of the 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus. (2019) 1165–1168.

[9] M. Atoui, K. Ibn Taarit, and M. Ksouri, Sensor Faults Detection Design for Networked Control Systems with Packet Dropout, 15th International Multi-Conference on Systems, Signals, and Devices, SSD. 1(1) (2018) 140–145.

[10] A. B. Ghosh and P. S. Lal Priya, Adaptive Discrete Sliding Mode Controller for Networked Control Systems, International Conference on Circuits and Systems in Digital Enterprise Technology, ICCSDET. (5) (2018). https://doi.org/10.1109/ICCSDET.2018.8821145

[11] Y. Cao, M. Gao, and D. Zhang, Fault Detection for Networked Control Systems with Uncertain Time-Varying Sampling Periods, Proceedings of the 28th Chinese Control and Decision Conference, CCDC. (1) (2016) 2956–2960.

[12] J. Liu, P. Wang, and J. Lin, Real-Time Scheduling for Wireless Mesh Networked Control Systems, 9th IEEE International Conference on Communication Software and Networks, ICCSN. (2017) 382–386.

[13] S. Srinivasan et al., Adaptive Controller for Networked Control Systems Subjected to Random Communication Delays, Advances in Intelligent Systems and Computing. 633(2) (2018) 78–94.

[14] L. Hongjie, Robust H, Infinity Control of Networked Control Systems with Randomly Varying Delay and Missing Measurements, Chinese Control Conference, CCC. (2012) 2753–2758.

[15] Z. Hu, F. Deng, M. Xing, and J. Li, Modeling and Control of Itô Stochastic Networked Control Systems with Random Packet Dropouts Subject to Time-Varying Sampling, IEEE Transactions on Automatic Control. 62(8) (2017) 4194–4201.

[16] M. Li and Y. Chen, Robust Tracking Control of Networked Control Systems with Communication Constraints and External Disturbance, IEEE Transactions on Industrial Electronics. 64(5) (2017) 4037–4047.

[17] I. Sakti and D. R. Prajitno, Experiment of Networked Control System (NCS) using Network Emulator, 3rd International Conference on Information Technology, Computer, and Electrical Engineering, ICITACEE. (2017) 100–105.

[18] L. Jianning, S. Hongye, W. Zhengguang, and C. Jian, Stabilization of Wireless Networked Control System with Multi-Packet Transmission Policy, Chinese Control Conference, CCC. (2012) 5770–5774.

[19] J. Ma, K. Liu, S. Sun, and G. Yang, Design and Simulation of Large Delay Wireless Network Control System, Proceedings - 8th International Conference on Instrumentation and Measurement, Computer, Communication and Control, IMCCC. (2018) 217–220.

[20] Y. Wang, S. X. Ding, D. Xu, and B. Shen, An H∞ Fault Estimation Scheme of Wireless Networked Control Systems for Industrial Real-Time Applications, IEEE Transactions on Control Systems Technology. 22(6) (2014) 2073–2086.

[21] J. Jithish and S. Sankaran, Securing Networked Control Systems: Modeling Attacks and Defenses, IEEE International Conference on Consumer Electronics-Asia, ICCE-Asia. (2018) 7–11.

[22] B. S. Solanki, R. Kumawat, and S. Srinivasan, An Impact of Different Uncertainties and Attacks on the Performance Metrics and Stability of Industrial Control System, Communication and Intelligent Systems. (2021) 557–574.

[23] C. Xiang, L. Qiu, J. Pan, B. Zhang, and R. Yang, Predictive Feedback Control Based on Dos Attacks Network Control System, IEEE International Conference on Control and Automation, ICCA. (2020) 1189–1192.

[24] Z. W. Wang and H. H. Gao, Linear Quadratic Optimal Control of Networked Control System, Proceedings of the 27th Chinese Control and Decision Conference, CCDC. (61263003) (2015) 2177–2182.

[25] N. Y, M. J. Gopinath, and G. L, DDoS Mitigation using Software Defined Network, International Journal of Engineering Trends and Technology. 24(5) (2015) 258–264.

[26] S. S. Chowriwar, M. S. Mool, P. P.Sabale, S. S.Parpelli, and M. N. Sambhe, Mitigating Denial-of-Service Attacks Using Secure Service Overlay Model, International Journal of Engineering Trends and Technology. 8(9) (2014) 479–483.

[27] V. Raghuwanshi and S. Jain, Denial of Service Attack in VANET: A Survey, International Journal of Engineering Trends and Technology. 28(1) (2015) 15–20.

[28] K. Bouzoubaa, Y. Taher, and B. Nsiri, DOS-DDOS Attacks Predicting: Performance Comparison of the Main Feature Selection Strategies, International Journal of Engineering Trends and Technology. 70(1) (2022) 299–312.

[29] H. Lin, H. Su, P. Shi, R. Lu, and Z. G. Wu, Estimation and LQG Control over Unreliable Network with Acknowledgment Randomly Lost, IEEE Transactions on Cybernetics. 47(12) (2017) 4074–4085.

[30] M. Palmisano, M. Steinberger, and M. Horn, Optimal Finite-Horizon Control for Networked Control Systems in the Presence of Random Delays and Packet Losses, IEEE Control Systems Letters. 5(1) (2021) 271–276.

[31] D. Satoh, K. Kobayashi, and Y. Yamashita, Stochastic Model Predictive Control of Multi-Hop Control Networks with Packet Dropouts, 56th Annual Conference of the Society of Instrument and Control Engineers of Japan, SICE. (2017) 164–167.
[32] Y. Uchiyama, T. Zanma, S. Fujisawa, K. Koiwa, and K. Z. Liu, Optimal Self-triggered Control in Networked Control Systems, Proceedings - 12th France-Japan and 10th Europe-Asia Congress on Mechatronics, Mechatronics. (2018) 170–173.
[33] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, Coding Schemes for Securing Cyber-Physical Systems against Stealthy Data Injection Attacks, IEEE Transactions on Control of Network Systems. 4(1) (2017) 106–117.
[34] Y. Pan and G. H. Yang, Event-Triggered Fuzzy Control for Nonlinear Networked Control Systems, Fuzzy Sets, and Systems. 329(8) (2017) 91–107.
[35] Z. Pang, C. Lin, G. Liu, and C. Han, Data-Driven Networked Predictive Control of a Class of Nonlinear Systems with Random Packet Dropouts, Chinese Control Conference, CCC. (2017) 7956–7961.
[36] M. Ren, J. Zhang, M. Jiang, M. Yu, and J. Xu, Minimum = (h,φ)-Entropy Control for Non-Gaussian Stochastic Networked Control Systems and its Application to a Networked DC Motor Control System, IEEE Transactions on Control Systems Technology. 23(1) (2015) 406–411.
[37] W. Ren and J. Xiong, Tracking Control of Nonlinear Networked and Quantized Control Systems with Communication Delays, ArXiv. 65(8) (2019) 3685–3692.
[38] M. Razeghi-Jahromi and A. Seyedi, Stabilization of Networked Control Systems with Sparse Observer-Controller Networks, IEEE Transactions on Automatic Control. 60(6) (2015) 1686–1691.
[39] C. Tan, L. Li, and H. Zhang, Stabilization of Discrete-Time Networked Control Systems with Packet Dropout and Network-Induced Delay, Chinese Control Conference, CCC. (2015) 6557–6561.
[40] B. S. Solanki, R. Kumawat, and S. Srinivasan Averting and Mitigating the Effects of Uncertainties with Optimal Control in Industrial Networked Control System. (2022) 316–318. https://doi.org/10.1109/ises52644.2021.00080
[41] X. Tang, T. Li, S. Cong, and W. Qian, Event-Triggered Adaptive Control for Networked Control Systems Under Two Stochastic Cyber-Attacks, Proceedings of the 31st Chinese Control and Decision Conference, CCDC. (2019) 170–175.
[42] J. Sun and J. Chen, Networked Predictive Control for Linear Systems with Communication Delay in the Feedback Channel, Stability, Control and Application of Time-Delay Systems. (2019) 315–331.
[43] X. M. Tang, S. Yang, J. M. Yu, and H. C. Qu, Guaranteed Cost Control of Networked Control Systems With Bounded Packet Loss Based on Quantization Dependent Lyapunov Function, Zidonghua Xuebao/Acta Automatica Sinica. 44(8) (2018) 1381–1390.
[44] J. Wang and C. Liu, Stability Analysis for a Class of Nonlinear Networked Control Systems, Chinese Control Conference, CCC. (3) (2018) 1287–1290.
[45] P. Wang and W. Che, Quantized H∞ Control for Networked Control Systems with Random Packet Losses, Proceedings of the 27th Chinese Control and Decision Conference, CCDC. (2015) 6557–6562.
[46] D. Wang, D. Liu, H. Li, B. Luo, and H. Ma, An Approximate Optimal Control Approach for Robust Stabilization of a Class of Discrete-Time Nonlinear Systems with Uncertainties, IEEE Transactions on Systems, Man, and Cybernetics: Systems. 46(5) (2016) 713–717.
[47] T. Wang, H. Gao, and J. Qiu, A Combined Adaptive Neural Network and Nonlinear Model Predictive Control for Multirate Networked Industrial Process Control, IEEE Transactions on Neural Networks and Learning Systems. 27(2) (2016) 416–425.
[48] K. Xu, J. Zhou, F. Liu, and G. Gu, LQG Control for Networked Control Systems in Data Packet Drops, Chinese Control Conference, CCC. (2016) 7428–7433.
[49] Y. F. Guo and S. Y. Li, Transmission Probability Condition for Stabilizability of Networked Control Systems, IET Control Theory, and Applications. 4(4) (2010) 672–682.
[50] F. L. Qu, Z. H. Guan, T. Li, and F. S. Yuan, Stabilisation of Wireless Networked Control Systems with Packet Loss, IET Control Theory and Applications. 6(15) (2012) 2362–2366.
[51] M. Steinberger and M. Horn, A Stability Criterion for Networked Control Systems with Packetized Transmissions, IEEE Control Systems Letters. 5(3) (2021) 911–916.
[52] Z. H. Pang, W. C. Luo, G. P. Liu, and Q. L. Han, Observer-Based Incremental Predictive Control of Networked Multi-Agent Systems with Random Delays and Packet Dropouts, IEEE Transactions on Circuits and Systems II: Express Briefs. 68(1) (2021) 426–430.
[53] M. Li, Y. Chen, X. Bin Zhang, and Y. P. Xian, A Predictive Control Method for Networked Control Systems with Random Delay and Packet Dropouts, Chinese Control Conference, CCC. (2016) 4372–4377.
[54] T. Li, W. A. Zhang, and L. Yu, Improved Switched System Approach to Networked Control Systems with Time-Varying Delays, IEEE Transactions on Control Systems Technology. 27(6) (2019) 2711–2717.
[55] H. C. Cho and M. S. Fadali, Nonlinear Network-Induced Time-Delay Systems with Stochastic Learning, IEEE Transactions on Control Systems Technology. 19(4) (2011) 843–851.
[56] B. S. Solanki, R. Kumawat, and S. Srinivasan, Synthesize the Effect of Intrusion and Imperfection on Networked-Connected Control System with Optimal Control Strategy, 10th International Conference on Information and Automation for Sustainability, ICIAfS. (2021) 105–110.
[57] S. Bi and M. Zawodniok, PDF-based Tuning of Stochastic Optimal Controller Design for Cyber-Physical Systems with Uncertain Delay Dynamics, IET Cyber-Physical Systems: Theory & Applications. 2(1) (2017) 1–9.
[58] S. W. Gao and G. Y. Tang, Output Feedback Stabilization of Networked Control Systems with Random Delays, IFAC Proceedings. 44(1) (2011) 3250–3255.
[59] Z. Gao, L. Yang, H. Wang, and X. Li, Active Fault-Tolerant Control of Electric Power Steering System with Sensor Fault, Chinese Control Conference, CCC. (2017) 9630–9636.

[60] J. Li, H. Yu, W. Liang, P. Zeng, and M. Yuan, A Survey of Packet Disordering Existing in Networked Control Systems, IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, IEEE-CYBER. (2015) 1797–1801.
[61] Z. Pang, G. Liu, D. Zhou, and D. Sun, Data-Based Predictive Control for Networked Nonlinear Systems with Packet Dropout and Measurement Noise, Journal of Systems Science and Complexity. 30(5) (2017) 1072–1083.
[62] Y. Sun, Finite-Time Bounded and Boundedness of Networked Control Systems with Random Time Delay and Packet Dropout, Chinese Control Conference, CCC. (2) (2017) 7611–7615.
[63] A. O. De Sa, L. F. R. D. C. Carmo, and R. C. S. Machado, Use of Switching Controllers for Mitigation of Active Identification Attacks in Networked Control Systems, Proceedings - IEEE 15th International Conference on Dependable, Autonomic and Secure Computing, IEEE 15th International Conference on Pervasive Intelligence and Computing, IEEE 3rd International Conference on Big Data Intelligence and Compu. (2018) 257–262.
[64] A. W. Al-Dabbagh, Y. Li, and T. Chen, An Intrusion Detection System for Cyberattacks in Wireless Networked Control Systems, IEEE Transactions on Circuits and Systems II: Express Briefs. 65(8) (2018) 1049–1053.
[65] J. Hu, C. Liu, and Y. Song Switching Control for a Networked Control System with Denial-of-Service Attacks, Chinese Control Conference, CCC. (2017) 7667–7672.
[66] X. Huang and J. Dong, Reliable Control Policy of Cyber-Physical Systems against a Class of Frequency-Constrained Sensor and Actuator Attacks, IEEE Transactions on Cybernetics. 48(12) (2018) 3432–3439.
[67] S. Hu, Y. Zhou, X. Chen, and Y. Ma, H ∞ controller Design of Event-Triggered Networked Control Systems under Quantization and Denial-of-Service Attacks, Chinese Control Conference, CCC. (2018) 6338–6343.
[68] Z. H. Pang and G. P. Liu, Design and Implementation of Secure Networked Predictive Control Systems under Deception Attacks, IEEE Transactions on Control Systems Technology. 20(5) (2012) 1334–1342.
[69] C. Schellenberger and P. Zhang, Detection of Covert Attacks on Cyber-Physical Systems by Extending the System Dynamics with an Auxiliary System, IEEE 56th Annual Conference on Decision and Control, CDC. (2018) 1374–1379.
[70] J. Zhang, C. Peng, S. Masroor, H. Sun, and L. Chai, Stability Analysis of Networked Control Systems with Denial-of-Service Attacks, UKACC International Conference on Control, UKACC Control. (2016). https://doi.org/10.1109/CONTROL.2016.7737622.
[71] Q. Zhang and F. Qu, Stabilization of Networked Control Systems via Switching and Impulsive Controllers, Proceedings of the 31st Chinese Control and Decision Conference, CCDC. (2019) 1852–1856.
[72] X. M. Zhang et al., Networked Control Systems: A Survey of Trends and Techniques, IEEE/CAA Journal of Automatica Sinica. 7(1) (2020) 1–17.
[73] M. Tahboush, M. Agoyi, and A. Esaid, Multistage Security Detection in the Mobile Ad-Hoc Network (MANET), International Journal of Engineering Trends and Technology. 68(11) (2020) 97–104.
[74] B. S. Solanki, K. Renu, and S. Srinivasan, Stability and Security Analysis with Identification of Attack on Industrial Networked Control System: An Overview, Internetworking Indonesia Journal. 11(2) (2019) 3–8.
[75] C. Huang, Y. Bai, and Y. Zhu, PID Controller Design for a Class of Networked Cascade Control Systems, Proceedings - 2nd IEEE International Conference on Advanced Computer Control, ICACC. 1 (2010) 43–47.
[76] N. Noroozi, R. Geiselhart, S. H. Mousavi, R. Postoyan, and F. R. Wirth, Integral Input-To-State Stability of Networked Control Systems, IEEE Transactions on Automatic Control. 65(3) (2020) 1203–1210.
[77] Y. Zhou, J. Cao, C. Ma, and Q. Zang, A Stochastic Stability Controller Design for Networked Control Systems with Random Time Delays, Proceedings of the 27th Chinese Control and Decision Conference, CCDC. (2015) 2200–2204.
[78] C. Zhu and F. Chai, Triggered Networked Control System with a Random Delay, Proceedings of IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference, ITNEC 2019. (2019) 1145–1149.
[79] W. Lu, X. Yin, Y. Fu, and Z. Gao, Observer-Based Event-Triggered Predictive Control for Networked Control Systems Under Dos Attacks, Sensors (Switzerland). 20(23) (2020) 1–21.
[80] H. Xu, S. Jagannathan, and F. L. Lewis, Stochastic Optimal Design for Unknown Linear Discrete-Time System Zero-Sum Games in the Input-Output form Under Communication Constraints, Asian Journal of Control. 16(5) (2014) 1263–1276.
[81] K. Glover, A Loop Shaping Design Procedure using HA Synthesis, IEEE Transactions on Automatic Control. 37(6) (1992) 759–769.
[82] K. Glover and D. Mcfarlane, Robust Stabilization of Normalized Coprime Factor Plant Descriptions with H∞-Bounded Uncertainty, IEEE Transactions on Automatic Control. 34(8) (1989) 821–830.
[83] V. M. Hern, DC / DC Buck Power Converter as a Smooth Starter for a DC Motor Based on a Hierarchical Control. 30(2) (2015) 1076–1084.