Received: 14 July 2022 | Revised: 16 September 2022 | Accepted: 26 October 2022

DOI: 10.1049/cth2.12393

IET Control Theory & Applications

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

Attack detection and fault-tolerant control of interconnected cyber-physical systems against simultaneous replayed time-delay and false-data injection attacks

Salman Baroumand[1] | **Amirreza Zaman**[2] | **Lyudmila Mihaylova**[3]

[1]Department of Electrical Engineering, Faculty of Engineering, Fasa University, Fasa, Iran

[2]Control Engineering Group, Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden

[3]Department of Automatic Control and Systems Engineering, University of Sheffield, Sheffield, UK

Correspondence
Control Engineering Group, Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden.
Email: amirreza.zaman@ltu.se

Funding information
the Horizon 2020 Research Programme of the European Commission, Grant/Award Number: 956059 (ECO-Qube); the EPSRC project EP/V026747/1 (Trustworthy Autonomous Systems Node in Resilience)

Abstract

Nowadays, interconnected cyber-physical systems (CPSs) are widely used with increasing deployments of Industrial Internet of Things (IIoT) applications. Other than operating properly under system uncertainties, CPSs should be secured under unwanted adversaries. To mark such challenges, this paper proposes the solution of secure decentralized robust control for uncertain CPSs under replayed time-delay and false-data injection attacks altogether. Potentially, considered attacks can force the whole system to instability and crash. Three challenges are addressed, and solutions are presented: (1) model non-linearity and uncertainties, (2) existing simultaneous time-delay and potential false-data injection attacks with skew probability density functions, and (3) requirement to use real-time attack detection. Thus, a novel, robust control method to deal with thwart attacks on a closed-loop control system is proposed to provide the system's trustworthiness. Additionally, novel attack detection methodologies are presented to detect these advanced attacks rapidly based on statistical methods such as Spearman's correlation coefficient, Neyman–Pearson (NP) error classification, and trend analysis. Ultimately, the proposed novel attack detection and robust control protocol are verified and evaluated in real-time.

1 | INTRODUCTION

Interconnected CPSs have been widely used in distributed networks. They involve several subsystems that are coupled to each other over the wireless network. Interconnected CPSs are generally applied in different fields of industry, such as power grids, chemical processing, communication systems, and even urban traffic networks. Since interconnected CPSs are distributed over an area, the control strategies that are used for these systems are subject to decentralized control [1]. Moreover, interconnected systems are studied in various areas, for instance, stability analysis of interconnected systems is developed in [2, 3], or fault-tolerant control issue of these systems is studied in [4].

Because of implementing decentralized interconnected CPSs and technological improvements in communication networks, networked control systems (NCSs) have been developed in recent years [5]. When the number of interconnected systems increases, the former point-to-point signal transmission procedure from local controllers to each distributed subsystem is replaced by the communication network [6]. Most approaches on NCSs consider that the quality of service (QoS) of the developed communication network is suitable enough to ensure that the NCS performs in ideal conditions, such as the developed case in [6]. In recent years, the security problem of CPSs has been gained much more attention from researchers in various applications. To provide the security of CPSs against attacks, it is necessary to monitor the CPSs under different pre-defined faulty situations and develop accurately secured and mathematically proven fault detection, defence and control strategies.

Applications of CPSs can be observed in autonomous vehicles, smart grids, chemical processes and intelligent transportation networks [7–9]. As stated formerly, interconnected CPSs are critically vulnerable to any attacks since the communication networks among subsystems are considered wireless. Different attacks can cause various faults and even failures in each section of CPSs, such as cyber components or the physical part of the system. Generally, two major categories of

cyber-attacks are defined as deception attacks and denial-of-service (DoS) attacks. In all types of deception attacks, the goal of the attacker is to compromise the transmitted data from the sensor to lessen the integrity of the data packets [10]. Specifically, some types of deception attacks occur regularly in industrial CPSs. These common attacks include false-data injection attacks in which the generated false data (noise) from the attacker is injected into the communication network to decrease the system's data authenticity, replay attacks in which the previous time data packets are stored and sent repeatedly to prevent the subsystems from reaching the steady-state phase [10], and time-delay attacks in which a delay parameter is injected to the system to cause instability in system's operation [11, 12]. Recently, authors in [13] developed a model-free reinforcement learning algorithm to control CPSs under time-delay attacks from a robust perspective. As a novel approach in CPSs' security issues, in [14], averaging attacks targeting real-world privacy-preserving algorithms are proposed. The presented averaging attacks are designed optimally to modify the sensitive dataset's attribute by injecting zero-mean bounded uniform noise to alter the dataset's histogram. Alternatively, in DoS attacks, the communication network is being blocked to prevent the data packet from being received in the data fusion and monitoring centre or to the actuators [15].

Deception attacks can cause severe failures in the system's performance, such as collisions. Thus, there is always an urgent need and an interest for engineers to detect these attacks as quickly as possible in their first stages of occurrence to implement defence and control protocols. Some approaches have been made considering linear systems under malicious deception attacks. In [16], the problem of state estimation is developed under deception attacks. In [17], the worst-case zero-mean Gaussian distributed deception attack strategy is presented. Following the approach in [17], the worst-case deception attack policy derivation with arbitrarily chosen mean value is proposed in [18]. Since false-data injection attacks can be complicated to detect quickly in some networks, some approaches follow the idea of analysing attacks' detection and stealthiness tradeoffs. In a recent study, in [19], the optimal false-data injection attack framework is obtained to maximize the attacker's degree of stealthiness by increasing the quadratic cost of the system's LQG controller.

In implementing CPSs in industrial environments, increasing the number of subsystems leads to more complex interconnected systems. Consequently, environmental, and operational uncertainties increase, which causes growing concerns and problems of providing attack detection, defence, and control methods in industrial control systems. Regarding this matter, in [20], various security issues of industrial control systems involving Supervisory Control and Data Acquisition (SCADA) are introduced and reviewed to provide a complete overview to lessen cyber threats and secure the control system's operation. Interestingly, improved form of the blind false-data injection attacks, mostly occurring in SCADA systems, were introduced recently in [21] in which they can remove the impacts of outliers in measured data and maximize the attack's performance to bypass fault detector's mechanism. Furthermore, simulation results were conducted to verify the proposed attack on PJM 5-bus and IEEE 14-bus test system.

Despite remarkable studies in CPSs' theory under uncertainties, it is still an interest to analyse and propose robust control methods for complex CPSs by assuming various types of uncertainties in industrial environments under different kinds of attacks. Further, ref. [22] referred to the mentioned two groups of uncertainties. Inherent stochastic features of a physical system or the environment which cause some uncertainties are defined as aleatory uncertainties. In contrast, some uncertainties are considered due to the lack of knowledge or information (such as limited experience and domain uncertainty), which are determined as epistemic uncertainties [23].

As much as it is important to design control protocols to maintain the CPSs' stability under various cyber threats, it is essential to detect the injected false data online at the attacks' occurrence. So, in addition to developing a robust fault-tolerant control strategy, designing a trust-based false-data detector unit is also a crucial matter. Recent significant approaches have been made lately to detect cyber threats and control CPSs under DoS or deception attacks. As an example, in [24], an event-based nonlinear controller is proposed to overcome control issues in non-linear CPSs which had been threatened by DoS attacks. Additionally, authors in [25] presented an event-triggered adaptive sliding mode controller to provide uncertain non-linear system's stability under false-data injection attacks. Besides, they introduced event-triggered functionality from sensor to observer (S-O) and from observer to controller (O-C) for the reason of decreasing the communication load. For multi-agent systems (MASs) under DoS attacks, in [26] and [27], distributed control protocols are designed to provide consensus policies. Besides, in [28], the leader-following consensus protocols are presented for discrete-time MASs against DoS attacks.

Several studies considered the problem of false-data detection under malicious attacks. In [10, 26], the Kullback–Leibler (K–L) divergence measure is applied to detect the false-data injection and replay attacks, respectively. The K–L measure is effective in detecting attacks with Gaussian distributions in higher-order linear/non-linear CPSs [26]. Additionally, correlation analysis is reviewed as another attack detection framework in [12] and its performance is compared with the K–L divergence criterion in real-time false-data detection scenarios. During our research on CPSs, we observed that by considering non-Gaussian signals injected into the system in the form of time delays or injected false data, the system's performance degraded significantly while the malicious signals remained stealthy. More specifically, the system became unstable even though we had applied former robust control and false-data detection methodologies, such as approaches in [26, 29]. So, we have come up with some challenges and technical difficulties that have not yet been dealt with: (1) Even if the injected random time delay into the process may not cause the plant's instability, it is also complicated to detect unpredicted d delays online. (2) Developed approaches did not assume non-normal distributions for generating random delays for the attacker, which must be considered. (3) Considering non-Gaussian false-data injection attacks is a research subject that should be studied

more since there is no necessity from the attacker's perspective to generate noises with normal distributions. At the same time, it is evident that normally generated injected faulty signals can be easily detected. Hence, we faced a new form of cyber threat, which we need to put more study on. To propose the solution, we reviewed the extensive literature regarding non-Gaussian signals' analysis and presented the current article's approach. As stated before, all the proposed false-data detection schemes assumed that the attacks involve Gaussian distributions to apply Kalman filter-based estimation methods. However, the design solution of robust control and false-data detection through compromised cyber links has not been studied in the presence of attacks with non-Gaussian distributions such as skew distributions. Assuming non-Gaussian attacks lead to making Kalman-filter-based attack detection methods vulnerable in which only Gaussian-distributed form of noise can be detected as an intruder, while non-Gaussian noise remains hidden. As a result, formerly developed detection methods cannot provide feasible performance under these circumstances. Therefore, it is required to introduce new online false-data detection frameworks to overcome malicious non-Gaussian cyber threats. This matter motivates the study of the present paper. In this article, the main purpose is to present novel defence strategies and attack detectors by integrating various types of attacks to the system simultaneously with non-Gaussian distributed noise. Proposed novel attack detectors in this paper are based on the application of signal trend analysis methods which enable us to detect malicious non-Gaussian noise existence in the system for combined cyber-attacks. Besides, a Lyapunov function-based delay-independent robust control method is proposed to maintain the system's stability against time-delay and false-data injection attacks happening altogether while reducing the computational complexity. This paper has the following main contributions: (1) it develops models for false-data injection and time-delay attacks in uncertain industrial interconnected CPSs. Compared to previous approaches devoted to defining cyber threats, we consider cyberattacks with non-Gaussian and skew-distributed behaviours, which introduces a new type of attacks that can degrade the system's performance while being malicious; (2) robust decentralized controllers are developed that deal with the skew-distributed cyber-attacks while maintaining the system's stability using Lyapunov stability conditions; (3) for the first time, explicit statistical analysis of online false-data detection under attacks is presented using correlation analysis, change-point detection trend analysis, and Neyman–Pearson signal classification methods to trigger an alarm as fast as possible. The proposed false-data detection frameworks can detect threats with non-Gaussian distributions online, which is beneficial in providing defence strategies for CPSs. (4) Finally, the proposed robust control and false-data detection strategies are evaluated numerically to validate the effectiveness of the developed methods.

The remainder of the article is organized as follows. In Section 2, we formulate the uncertain CPS under various types of non-Gaussian deception attacks. Thereafter, we propose the stability conditions of the modelled uncertain CPS under skew-distributed attacks in Section 3, which yields to presenting the closed-loop robust control strategy using the Lyapunov–Krasovskii functional approach. Then, in Section 4, various statistical methods are introduced to detect non-Gaussian cyberattacks, such as correlation analysis, change-point detection trend analysis, and Neyman–Pearson signal classification methods. Finally, the effectiveness of the proposed robust control protocol for uncertain CPSs against multiple types of non-Gaussian cyber-attacks is validated with numerical simulations in Section 5. Besides, the false-data detection performance is analysed and compared with various provided statistical signal trend detection methods. It is drawn that by introduced attack detection frameworks, non-Gaussian cyber-attacks can be detected online. The conclusions are drawn in Section 6. Also, the article's lemmas and mathematical proofs are provided in the Appendix.

2 | PROBLEM FORMULATION AND PRELIMINARIES

Consider a class of decentralized interconnected non-linear systems with the i-th subsystem is described as:

$$\begin{cases} \dot{x}_i(t) = A_i x_i(t) + f_i(x_1, x_2, \ldots, x_N) + B_i u_i(t) \\ y_i(t) = C_i x_i(t), \; i = 1, 2, \ldots, N \end{cases} \tag{1}$$

where $x_i \in R^{n_i}$, $u_i \in R^{m_i}$, and $y_i \in R^{p_i}$ are state, input and output vectors of the ith subsystem, respectively. output vectors of the ith subsystem, respectively. Besides, f_i is considered as a non-linear function for the ith subsystem non-linearity and ith subsystem interactions with other subsystem. In the above equation, N is the number of operating subsystems, A_i, B_i and the output matrix C_i are known constant real matrices of appropriate dimensions, in ith subsystem.

2.1 | Mathematical modelling of uncertainties

Uncertainties are usually caused by unknown inputs and parameters' inaccuracies in modelling. In this paper, for simplicity, all kinds of uncertainties can be merged as an augmented vector $W = [u_d^T \quad u_u^T \quad f_a^T]$ to the model of the system, where u_d, u_u and f_a denote input disturbance, unknown control input, and all system's fault vectors, respectively. Let define B_{w_i} as the known uncertain gain matrix for the ith subsystem. In general, by stating the term $B_{w_i}W_i$ in further equations, all types of uncertain inputs to each subsystem, such as plant non-linearities, modelling uncertainties, unmeasurable system inputs, non-linear interconnected functions and actuator faults can be considered to have better analysis of the real implemented proposed decentralized system. Depending on the type of the considered problem, some rows of the matrix $B_{w_i}W_i$ can be set to zero to obtain more specific cases. By assuming uncertainties, Equation (1) can be rewritten in a more general form for the ith

subsystem as :

$$\begin{cases} \dot{x}_i(t) = \tilde{A}_i x_i(t) + B_i u_i(t) + B_{w_i} W_i(t) \\ y_i(t) = C_i x_i(t), \; i = 1, 2, \ldots, N \end{cases} \tag{2}$$

where the term $B_{w_i} W_i(t)$ denotes the whole system's augmented uncertainties, and

$$\tilde{A}_i = A_i + \Delta A_i . \tag{3}$$

where ΔA_i represents the linear estimation of the function $f_i$regards to x_i. Additionally, W_i is a vector involving modelling uncertainty and rest of plant non-linearities are defined as $(f_i - \Delta A_i)$, where $\Delta A_i$is assumed to be the uncertainty in plant's linearization with specific norms.

Also, uncertain matrices ΔA_i , $i = 1, 2, \ldots, N$are denoted for each subsystem as

$$\Delta A_i = \bar{D}_i F_i(x_i, t) \bar{E}_i \tag{4}$$

$$F_i^T(x_i, t) F_i(x_i, t) \leq I, \tag{5}$$

where $\bar{D}_i$ and $\bar{E}_i$ are constant matrices of applicable dimensions and F_i is a time-varying matrix with a specific range. To formulate further stability derivations, uncertain matrices of all subsystems are assumed to be bounded. Therefore, we defined uncertain matrices of subsystems as in (4).

2.2 | System architecture under multiple non-Gaussian deception attacks

Attackers can threaten both sensors and actuators in CPSs. In this paper, various simultaneous attacks are modelled to analyse their effects and develop a robust decentralized control strategy against them. The proposed simultaneous attacks involve a data-integrity attack and a time-delay attack at the same time. Besides, the attack distribution is assumed to be non-normal and skewed. With this assumption, all previously developed defence strategies in CPSs have almost poor efficiency and performance against skew-distributed attacks since all of them are developed based on the assumption that all the developed attacks are with Gaussian distributions, and they cannot work properly against attacks with other types of distributions. Thus, this paper presents a fault detection solution and a robust control strategy under these new and advanced malicious attacks to overcome this issue.

Based on the false-data injection attack, the cyber intruder strives to infect the transmitted measurement data from the sensors or the input control signal to the actuators. In our case, it is assumed that the output measured data from sensors is infected by a stochastic transmitted signal $v(t)$ from the attacker with a skewed and non-normal distribution. Consequently, this type of attack can be considered as an advanced model of previously studied attacks since previous methodologies such as

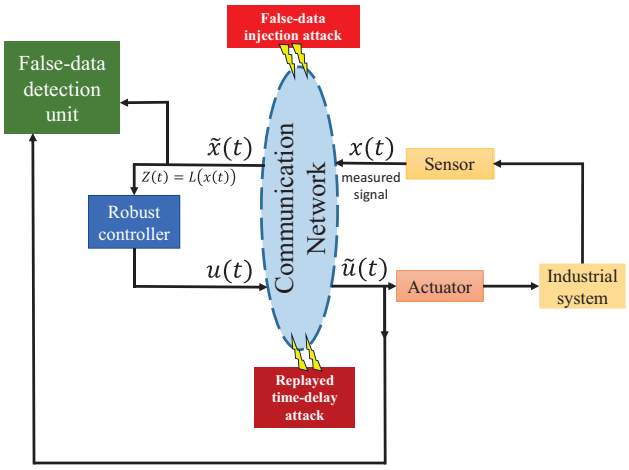

FIGURE 1 The structure of robust security control for a networked control system with false-data injection and replayed time-delay attacks

[17] just reviewed attacks with Gaussian distributions. Therefore, the proposed type of attack in the current article cannot be detected by formerly developed false-data detection protocols. So, new false-data detection and control solutions are needed to be proposed. The whole system is shown in Figure 1.

Since it is assumed that the cyber intruder has access to the communication channel and all exchanged data between subsystems, the attacker also tries to save previous data for a specific time interval and inject them as multiple delayed signals as $\Sigma_k x_i(t - \tau_{i_k})$ to the ith subsystem's control input as a time-delay attack. In addition to the introduced attack scenarios, we assume that the attacker also transmits a delayed control input to the control system as a time-delay attack with the form $\tilde{u}_i(t) = u_i(t - \tau_i)$. Consequently, the mathematical model of the ith subsystem (2) under the combined false-data injection and time-delay attacks has the following form

$$\begin{cases} \dot{x}_i(t) = \tilde{A}_i x_i(t) + B_i \tilde{u}_i(t) + \sum_{k=1}^{m_i} \tilde{H}_{i_k} x_i\left(t - \tau_{i_k}\right) + B_{w_i} W_i(t) \\ Z_i(t) = C_i x_i(t) \\ \tilde{u}_i(t) = u_i(t - \tau_i) \\ u_i(t) = K_i \tilde{x}_i(t) \\ \tilde{x}_i(t) = x_i(t) + v_i(t) \end{cases} \tag{6}$$

where for the ith subsystem, $Z_i(t)$ is the regulated output, $W_i(t)$ is an uncertain input, $v_i(t)$ is the random signal sent from attacker with a skewed and non-normal distribution, $\tilde{u}_i(t)$ is the received control signal under the time-delay attack with the specific delay interval τ_i, K_i is the feedback controller gain matrix and $\widetilde{H}_{i_k} x_i(t - \tau_{i_k})$ is considered as the model of a time-delay attack. Hence, (6) can be simplified as follows.

$$\dot{x}_i(t) = \tilde{A}_i x_i(t) + \sum_{k=0}^{m_i} \tilde{H}_{i_k} x_i\left(t - \tau_{i_k}\right) + G_i \theta_i(t) \tag{7}$$

where the above equation's variables are defined as $G_i = [B_iK_i \quad B_{w_i}]$, $\tau_{i_0} = 0$, $\theta_i = \begin{bmatrix} v_i(t) \\ W_i(t) \end{bmatrix}$, $\tilde{H}_{i_0} = B_iK_i$, $\tilde{H}_{i_k} = H_{i_k} + \Delta H_{i_k}$, $k \neq 0$, $i = 1, 2, \ldots, N$, $\Delta H_{i_k} = D_{i_k}F_i(x_i, t)E_{i_k}$. Besides, H_{i_k} $(k \neq 0)$ are specific fixed-value matrices, and D_{i_k} and E_{i_k} are matrices of applicable dimensions with specific values.

We defined the matrix $\tilde{H}_i$ for attacks' dynamics and its value can be selected by the attack provider. On the other hand, the matrix B represents the control input matrix. We can have two considerations for the matrix $\tilde{H}_i$: (1) by assuming a simpler form of attack ($\tilde{H}_i = 1$), the total attack signal is rewritten as $\sum_{k=1}^{m_i} x_i(t - \tau_{i_k})$ that decreases the attack problem's conservatism; (2) by considering attacks' dynamics, the total attack signal is reformulated as $\sum_{k=1}^{m_i} x_i(t - \tau_{i_k})$ and we can have a linear estimation of the injected delayed signal with the form $\tilde{H}_{i_k} = H_{i_k} + \Delta H_{i_k}$. Also, if there is no information about attacks' dynamics, H_{i_k} can be assumed as identity matrix and just consider estimation error obtained by the term ΔH_{i_k} while, the real value of ΔH_{i_k} is unknown and we can have an estimation of its norm value.

3 | ATTACK ANALYSIS FOR UNCERTAIN SYSTEMS

3.1 | Stability analysis of the proposed uncertain system under non-Gaussian deception attacks

According to (7), and if $Z_i(t) = C_ix_i(t)$ as the regulated output and $\theta_i(t)$ as an uncertain input of the ith subsystem, the solution of designing the robust state feedback controller with the form $u_i(t) = K_i\tilde{x}_i(t)$ can be expressed as an optimization problem of the infinite-norm of the transfer function $T_{Z\theta}$ as below.

Problem 1:

$$\min_{Kstability} \|T_{Z\theta}\|_\infty = \min_{Kstability} \sup \frac{\|Z(t)\|_2}{\|\theta(t)\|_2} = \gamma, (\gamma > 0), \quad (8)$$

where $K = diag\{K_i\}$ and $T_{Z\theta}$ is the defined transfer function from the input vector $\theta(t) = vec\{\theta_i(t)\}$ to the output vector $Z(t) = vec\{Z_i(t)\}$. By applying the L_2-norm, Equation (8) is equivalent to the following H_∞ optimization problem as the one expressed in [30]:

Problem 2:

$$\min \gamma, \text{ s.t. } J(\theta) < 0 \quad (9)$$

where $J(\theta) = \int_0^\infty [\, Z^T(s)Z(s) - \gamma\theta^T(s)\theta(s) \,]\, ds$, $\gamma > 0$.

In other words, solving (9) guarantees the system's stability by applying the worst-case uncertain signal $\theta(t)$ in formulations. Also, ref. [30] proved that the condition in (9) is fulfilled if and only if the following Hamiltonian function is obtained as the negative-definite function.

$$J_H = \frac{dV}{dt} + Z^TZ - \gamma\theta^T\theta, \quad (10)$$

where $V(x)$ is a Lyapunov function that satisfies the condition $V(x(0)) = 0$ and $V(x) \geq 0$. In further equations, the proper Lyapunov function is proposed to solve the presented H_∞ robust control problem.

3.2 | H_∞ delay-independent controller modelling

To obtain the delay-independent stability condition for the proposed system, the descriptor form for the ith subsystem (7) is stated as

$$\begin{cases} \dot{x}_i(t) = y_i(t) \\ y_i(t) = \tilde{A}_ix_i(t) + \sum_{k=0}^{m_i} \tilde{H}_{i_k}x_i\left(t - \tau_{i_k}\right) + G_i\,\theta_i(t), \end{cases} \quad (11)$$

Remark 1. Because we aim to reduce the complexity in formulating stability conditions of the system in (7), we proposed a less complicated form of (7) in a new descriptor form given in (11) with a lower order formulation by introducing an additive variable $y_i(t)$. Thus, a simpler representation of (7) is obtained by transforming (7) into (11) to reduce complexity and conservatism.

Accordingly, the above descriptor representation can be described with more details as

$$\begin{cases} \dot{x}_i(t) = y_i(t) \\ y_i(t) = \tilde{A}_ix_i(t) + \left(\sum_{k=0}^{m_i} \tilde{H}_{i_k}\right) x_i(t) \\ \quad - \sum_{k=0}^{m_i} \tilde{H}_{i_k} \int_{t-\tau_{i_k}}^{t} y_i(s)\, ds + G_i\,\theta_i(t), \end{cases} \quad (12)$$

Besides, for ith subsystem, the Lyapunov–Krasovskii functional candidate can be presented as

$$V(t) = \begin{bmatrix} x_i^T(t) & y_i^T(t) \end{bmatrix} E\,P_i \begin{bmatrix} x_i(t) \\ y_i(t) \end{bmatrix} + V_1 + V_2, \quad (13)$$

where

$$V_1 = \sum_{k=1}^{m_i} \int_{t-\tau_{i_k}}^{t} y_i^T(s)\,Q_{i_k}y_i(s)\, ds,\ Q_{i_k} > 0, \quad (14)$$

$$V_2 = \sum_{k=1}^{m_i} \int_{t-\tau_{i_k}}^{t} x_i^T(s)\,U_{i_k}x_i(s)\, ds,\ U_{i_k} > 0, \quad (15)$$

and $= \begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix}$, $P_i = \begin{bmatrix} P_1 & 0 \\ P_2 & P_3 \end{bmatrix}$, $P_1 = P_1^T > 0$. Also, P_1, Q_{i_k} and U_{i_k} are positive definite matrices, P_3 is assumed to be an

invertible matrix, and τ_{i_k} denotes the upper bound of the delay interval which is injected via time-delay attacker to the system. It is worth noting that the elements of the matrices P_i, $i = 1, 2, \ldots, n$ of each subsystem are assumed to be different from each other. Based on the proposed theorem in the following, the sufficient conditions for the closed-loop system's stability under the assumed attacks can be concluded.

Theorem 1. *Consider the proposed uncertain decentralized interconnected system under the presented cyber-attack model in (6). For a given γ and all non-zero $\theta \in L_2^q[0, \infty)$, $J(\theta) < 0$ satisfies for the closed-loop system with the proposed decentralized robust control strategy $U(t) = Kx(t)$ where $U(t)$ is the set of control inputs to all of the subsystem's actuators, and $K = diag\{K_i\}$ maintains the whole system's inner stability if for any implemented subsystem i, there exist positive symmetrical matrices Q_{i_k} and U_{i_k} ($k = 1, \ldots, m_i$), and $\bar{R}_{i_k}$ ($k = 1, \ldots, m_i$), $X_i = \begin{bmatrix} X_1 & 0 \\ X_2 & X_3 \end{bmatrix}$ and $X_1 = X_1^T$ such that the following LMI satisfies for each subsystem i ($i = 1, \ldots, N$):*

$$W_{i_1} = \begin{bmatrix} \bar{\bar{\Psi}} & 0 & 0 & \begin{bmatrix} 0 \\ G_i \end{bmatrix} & \bar{\theta}_3 & X_i \begin{bmatrix} I \\ 0 \end{bmatrix} & X_i \begin{bmatrix} 0 \\ I \end{bmatrix} \\ * & \bar{\theta}_1 & 0 & 0 & 0 & 0 & 0 \\ * & * & \bar{\theta}_2 & 0 & 0 & 0 & 0 \\ * & * & * & -\gamma^2 I & 0 & 0 & 0 \\ * & * & * & * & \bar{\theta}_4 & 0 & 0 \\ * & * & * & * & * & \bar{\theta}_5 & 0 \\ * & * & * & * & * & * & \bar{\theta}_6 \end{bmatrix} < 0,$$

$$W_{i_2} = \left(\xi_{i_k} I - \begin{bmatrix} 0 \\ E_{i_k} \end{bmatrix} \bar{R}_{i_k} \begin{bmatrix} 0 & E_{i_k}^T \end{bmatrix} \right) > 0. \tag{16}$$

where

$$\begin{aligned} \bar{\bar{\Psi}} = & \begin{bmatrix} 0 & 0 \\ A_i X_1 + B_i Y_i & 0 \end{bmatrix} + \begin{bmatrix} 0 & (A_i X_1)^T + (B_i Y_i)^T \\ 0 & 0 \end{bmatrix} \\ & + \begin{bmatrix} 0 & I \\ \sum_{k=1}^{m_i} H_{i_k} & -I \end{bmatrix} X_i + X_i^T \begin{bmatrix} 0 & \sum_{k=1}^{m_i} H_{i_k}^T \\ I & -I \end{bmatrix} \\ & + X_i^T \begin{bmatrix} C_i C_i^T & 0 \\ 0 & 0 \end{bmatrix} X_i \\ & + \begin{bmatrix} 0 & 0 \\ 0 & \xi_i^{-1} \bar{D}_i \bar{D}_i^T + \sum_{k=0}^{m_i} \xi_{i_k}^{-1} D_{i_k} D_{i_k}^T \end{bmatrix} X_i \\ & + X_i^T \begin{bmatrix} \xi_i \bar{E}_i \bar{E}_i^T + \sum_{k=0}^{m_i} \xi_{i_k} E_{i_k} E_{i_k}^T & 0 \\ 0 & 0 \end{bmatrix} X_i \\ & + \begin{bmatrix} 0 & 0 \\ 0 & \sum_{k=0}^{m_i} \tau_{i_k} \xi_{i_k} D_{i_k} D_{i_k}^T \end{bmatrix} \end{aligned} \tag{17}$$

and the rest of the variables are defined as

$\bar{\theta}_1 = -diag\{\bar{Q}_{i_k}^{-1}\}, \bar{\theta}_2 = -diag\{\bar{U}_{i_k}^{-1}\}, \bar{\theta}_5 = -diag\{\bar{U}_{i_k}\}, \bar{\theta}_6 = -diag\{\bar{Q}_{i_k}\}, \bar{Q}_{i_k} = Q_{i_k}^{-1}, \bar{U}_{i_k} = U_{i_k}^{-1}, k = 1, \ldots, m_i$

Also, we have

$$\bar{\theta}_3 = vec \left\{ \tau_{i_k} \begin{bmatrix} 0 \\ H_{i_k} \end{bmatrix} \bar{R}_{i_k} \begin{bmatrix} 0 & H_{i_k}^T \end{bmatrix} \right\},$$

$$\bar{\theta}_4 = -diag \left\{ \tau_{i_k} \left(\xi_{i_k} I - \begin{bmatrix} 0 \\ E_{i_k} \end{bmatrix} \bar{R}_{i_k} \begin{bmatrix} 0 & E_{i_k}^T \end{bmatrix} \right) \right\},$$

$k = 0, \ldots, m_i$.

Thereupon, the optimal gain of the state-feedback controller for each subsystem i is achieved by calculating $K_i = Y_i X_i^{-1}$ where $X_i = \begin{bmatrix} X_1 & 0 \\ X_2 & X_3 \end{bmatrix}$, $i = 1, \ldots, n$.

For proof of Theorem 1, see the Appendix.

The obtained LMIs in Theorem 1, guarantee the condition $J(\theta) < 0$ and provide closed-loop asymptotic stability. In other words, the inequality in (16) satisfies the Hamiltonian function in (10) which results in having $J(\theta)$ as a negative definite function. Therefore, we can conclude that the closed-loop system is L_2-stable with the L_2 gain smaller than γ. Additionally, by removing the corresponding rows and columns of θ in the obtained LMI (for $G_i = 0$) to form a new LMI, $\dot{V} < 0$ also satisfies which yields to asymptotic stability of the unforced closed-loop system (for the case of $\theta = 0$).

Remark 2. To simplify the calculations and knowing the fact that B_{w_i} is unknown, it can be inferred that $G_i \theta_i = \tilde{\theta}_i(t)$, where $\tilde{\theta}_i(t)$ implies the vector of uncertainties in the signal measurements or model of uncertainties in the system. In this case, to propose a straightforward control strategy, G_i will be replaced by Identity matrices in the calculations. However, considering this assumption may lead to a more conservative LMI condition for robust stability.

Remark 3. Theorem 1 provides internal stability of the closed-loop system and satisfies the condition $J(\theta) < 0$. Accordingly, to obtain the robust H_∞ controller with the form $K_i = Y_i X_i^{-1}$ that has the minimum value of the disturbance attenuation γ, the following optimization algorithm is required to be solved for each subsystem:

$$\min \gamma, \text{ s.t.} \tag{18}$$

for $Q_{i_k}, U_{i_k}, \bar{R}_{i_k}, X_i, Y_i$

The next section shows how real-time attacks can be detected when the system is subject to multiple and non-Gaussian deceptions.

4 | REAL-TIME ATTACK DETECTION UNDER NON-GAUSSIAN MULTIPLE DECEPTIONS

Following the presented robust control approach in the previous section, the system's stability is concluded under the non-Gaussian distributed attacks. Thus, the system's tolerance is significantly increased, which in this case, residual-based attack detection frameworks are not applicable here since system states are assumed to remain in a bounded range after implementing the robust approach. To overcome this matter and detect non-Gaussian distributed noise in the communication network, trend analysis methods are introduced to structure non-Gaussian attack detection strategies in CPSs. The existence of non-Gaussian distributed noise in the communication network leads to causing challenges in attack detection scenarios with Gaussian signals' estimation-based methodologies. Although formerly developed attack detection protocols such as the K–L divergence method require the system's inputs and outputs simultaneously, it is not necessary to provide input and output data altogether with trend analysis methods. Only using one of the system's signals is sufficient to detect false trends. In the following, standard signal trend analysis methods are reviewed. Additionally, the efficacy of the presented attack detection framework is evaluated by the provided example in the performance evaluation section.

4.1 | Correlation coefficient test

The correlation coefficient is a numerical measurement index without any units, and it is defined based on the covariance's definition. The correlation coefficient is used to calculate the degree of dependence between the two variables. In this article, the ability of standard correlation coefficient methods such as Pearson's correlation coefficient and Spearman's correlation coefficient to detect the mentioned attacks is shown in numerical simulations.

4.1.1 | Pearson's correlation coefficient test

Pearson's correlation coefficient is applied to obtain the degree, type, and direction of the coefficient value between the two variables. It is worth noting that this correlation coefficient with zero value only represents the lack of a linear relationship between two variables. However, the independence of two variables with zero value of the correlation coefficient cannot be concluded. On the other hand, this type of correlation does not necessarily show a causal relationship between system variables. The zero value of the Pearson correlation coefficient means that the variables are independent of each other if and only if the distribution of variables is normal. Thus, using Pearson's correlation coefficient in detecting attacks is powerless when the non-linear behaviour of the system increases or the injected noise from the attacker is considered as a non-normal noise.

4.1.2 | Spearman's correlation coefficient

Spearman's correlation coefficient shows the tendency of one variable to follow another variable. Unlike Pearson's correlation coefficient, finding the non-linear relationship between the two variables is developed using Spearman's correlation coefficient. Moreover, the degree of correlation of variables in non-linear systems can be obtained via Spearman's correlation coefficient. Last but not least, unlike Pearson's correlation, there is no need for normality in Spearman's correlation, and hence the Spearman's correlation is defined as a non-parametric statistical analysis. In Spearman's correlation analysis, instead of calculating the mean and variance values of variables, the correlation value is obtained using data rankings. Consequently, Spearman's correlation is not affected by outlier data. In the present paper, we expect Spearman's correlation analysis to be more effective than Pearson's since the injected noise signals by the attacker are non-normal with the skew distribution. Spearman's correlation coefficient alterations between input and output data of the system are demonstrated in numerical simulations.

4.2 | Change-point detection test

Various parametric and non-parametric statistical methods were developed to detect if a set of data follows a specific distribution or a trend. However, trend assessment analysis methods mostly refer to the analytic techniques to extract fundamental patterns from a partially or fully noisy signal's behaviour. So, the change-point detection method is a vital approach to detect periods with significant alterations in a signal or any time series. Accordingly, it is necessary to identify and analyse injected signals' trends to detect the time of attacks' occurrence and prevent the control systems from destructive failures in the system as quickly as possible.

In this article, statistical methods such as signals' trend assessment and change-point detection methods are applied to analyse the output measured signal of the system during the time horizon. Common change-point detection approaches in statistics include Pettitt's test [31], von Neumann ratio test [32], Buishand range test [33], and standard normal homogeneity (SNH) test [34]. Pettitt's test is a non-parametric test that is highly sensitive to sudden interruptions in the signals among the mentioned change-point methods. Therefore, Pettitt's test can precisely detect meaningful changes in the observed signal's mean value at any time.

In calculating Pettitt's test of a signal, let denote $x_1, x_2, \ldots, x_n$ as measured set of data. Consider a sudden change that occurs at the time index t_0. If the sequence $x_1, x_2, \ldots, x_{t0}$ has the probability distribution function $F_1(x)$ and the sequence $x_{t0+1}, x_{t0}+2, \ldots, xn$ has an altered probability distribution function

$F_2(x)$, then the non-parametric statistical hypothesis testing U_t for Pettitt's measure is given as

$$U_t = \sum_{i=1}^{t} \sum_{j=t+1}^{n} sgn\left(x_i - x_j\right), \tag{19}$$

where $sgn(\cdot)$ represents the sign function. Additionally, the statistical hypothesis $\mathbb{k}$ and the associated confidence level coefficient ρ for n data are defined as follows.

$$\mathbb{k} = max\left(|U_t|\right),$$

$$\rho = exp\left(\frac{-\mathbb{k}}{n^2 + n^3}\right), \tag{20}$$

where the approximate significance probability (P) for a changepoint test is defined as $P = 1 - \rho$.

It is evident to conclude that when some alterations in a signal exist, corresponding data series around that altered point is categorized into two subsections: before and after that altered point. Additionally, the statistical hypothesis k can be compared with different statistical confidence levels (such as 1% and 5%) to detect change points. The calculated Pettitt's hypothesis on the system's output signal under the defined multiple attacks is also illustrated in numerical simulations.

4.3 | Neyman–Pearson error classification

Data classification total error calculation is the most common performance analysis criterion in binary-based classification methods. However, asymmetrical classification errors cannot be obtained using this feature. As a solution, NP binary classification methods are proposed to deal with asymmetrical classification errors [35]. Based on the NP classification algorithm, the goal is to minimize the type II error (false negative) while maintaining the type I error (false positive) lower than the chosen error threshold (e.g. 5%). It is worth noting that in detecting cyber-attacks with NP algorithms, false-positive and false-negative rates need to be defined properly according to our goals. In this article, the "false-positive rate" is assumed to be the possibility of incorrectly classified "Class 1" observations into "Class 0", in which "Class 0 " is defined as the set of corrupted data and "Class 1 "is defined as the set of uncorrupted data.

Various NP algorithms have been developed based on different classification error grading approaches, such as logistic regression (LR), random forests (RF), support vector machines (SVM), linear discriminant analysis (LDA), naive bayes (NB), ada-boost (AB), and classification trees (CT). However, it is worth noting that there are few studies devoted to applying NP methods to detect attacks in CPSs [36, 37], or providing fault detection and isolation methods. In this paper, we first investigate if we could use NP classification methods to detect cyber-attacks. Second, we will compare obtained results from various developed NP methods in detecting the proposed cyber-attack.

5 | PERFORMANCE EVALUATION

In the current section, to evaluate the proposed method's trustworthiness, numerical examples are provided.

Example 1. Consider the following uncertain CPS, which has two subsystems ($i = 1, 2$) under the time-delay and non-Gaussian false data injection attacks as

$$\begin{cases} \dot{x}_1 = (A_1 + \Delta A_1)\, x_1(t) + A_{12} x_2(t) + B_1 \tilde{u}_1(t) \\ \qquad\quad + (H_1 + \Delta H_1)\, x_1(t - d(t)), \\ \dot{x}_2 = (A_2 + \Delta A_2)\, x_2(t) + A_{21} x_1(t) + B_2 \tilde{u}_2(t) \\ \qquad\quad + (H_2 + \Delta H_2)\, x_2(t - d(t)), \end{cases}$$

where

$$A_1 = \begin{bmatrix} -1.2 & 0.5 \\ -1.6 & -0.5 \end{bmatrix}, \Delta A_1 = \begin{bmatrix} -0.1 & 0.1 \\ 0 & 0.1 \end{bmatrix},$$

$$A_{12} = \begin{bmatrix} -0.1 & 0.1 & 0.2 \\ -0.3 & 0 & 0 \end{bmatrix},$$

$$B_1 = \begin{bmatrix} -0.5 \\ 0.5 \end{bmatrix}, A_2 = \begin{bmatrix} -1.5 & -0.1 & 1 \\ 0 & -1.3 & 0.5 \\ 1 & 0 & -1 \end{bmatrix},$$

$$\Delta A_2 = \begin{bmatrix} -0.1 & 0 & 0.1 \\ 0 & 0.1 & -0.1 \\ 0.1 & 0 & 0.1 \end{bmatrix},$$

$$A_{21} = \begin{bmatrix} -0.1 & 0 \\ 0 & 0 \\ 0 & 0.3 \end{bmatrix}, B_2 = \begin{bmatrix} -1 \\ 1 \\ 0.2 \end{bmatrix}, H_1 = \begin{bmatrix} -0.5 & 0 \\ 0 & 0.5 \end{bmatrix},$$

$$H_2 = \begin{bmatrix} -1 & 0.1 & 0 \\ 0 & 0.2 & 0 \\ 0 & -1 & 0.2 \end{bmatrix}, \Delta H_1 = \begin{bmatrix} 0.1 & 0.1 \\ 0 & -0.2 \end{bmatrix},$$

$$\Delta H_2 = \begin{bmatrix} 0.01 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -0.02 \end{bmatrix}$$

Besides, $d(t)$ represents the injected time delay to the system state feedback signals as a chirp signal with the frequency ranges from 0 to 100 Hz as a complex form of time-delay attack in which the time-delay attack $d(t)$ is consistently being replayed continuously in a time-varying form. Also, the injected false data

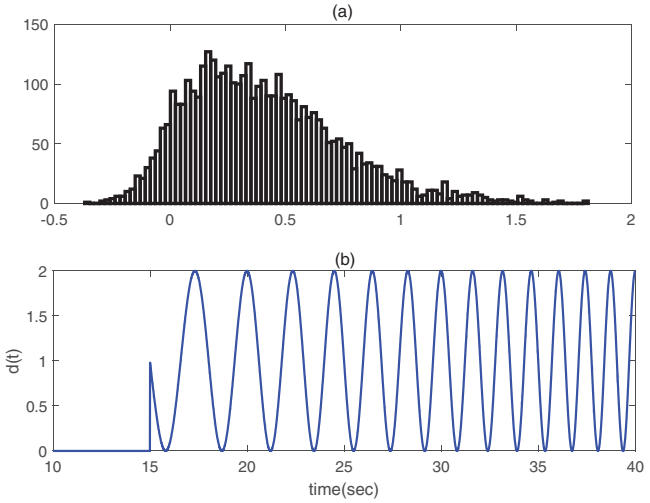

FIGURE 2 (a) Example of data integrity attack histogram chart with skewed distribution and (b) time-delay attack's delay trajectory

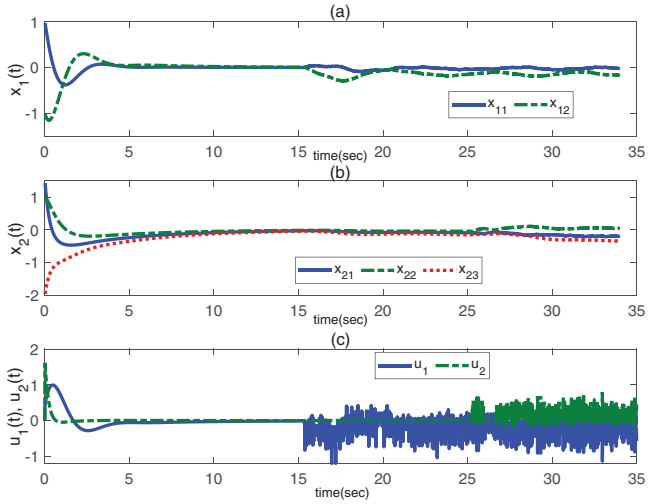

FIGURE 3 (a) states' trajectories of the 1st subsystem, (b) states' trajectories of the 2nd subsystem and (c) control input trajectories under the combined skew-distributed false-data and time-delay attacks with the article's presented robust controller

$v(t)$ is assumed to be a stochastic skew-distributed signal with a mean value of 0.4 and a variance value of 0.1. In Figure 2, the histogram chart of the signal $v(t)$ and the delay trajectory $d(t)$ are illustrated. The sampling time is 0.01 s.

It is considered that the first and second subsystems are under the combined time-delay and false-data injection attacks starting from the 15th and 25th time steps, respectively. In this case, the state and newly proposed control input trajectories are obtained in Figure 3. According to Figure 3, by occurring attacks, the system states deviate from their ideal equilibrium trajectory, but with the presented robust control strategy, they remain bounded close to the perfect trajectories. As a result, by implementing the developed control protocol, the whole system remains stable even under various non-Gaussian malicious cyber-attacks.

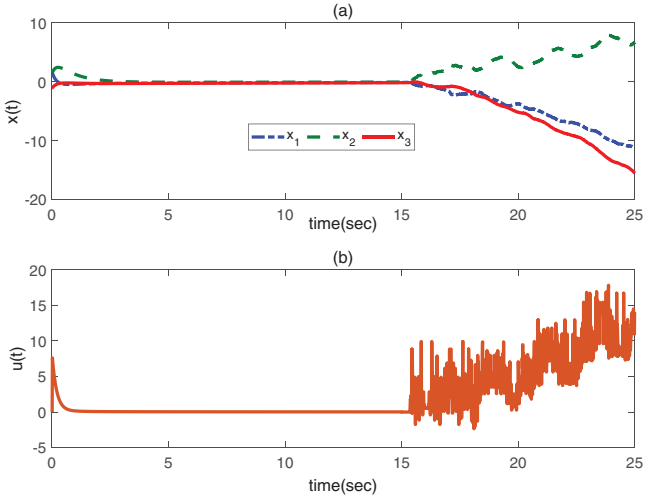

FIGURE 4 (a) Uncertain system states' trajectory and (b) control input trajectory with skew-distributed data integrity or time-delay attacks by implementing conventional robust controller [29]

The simulations of the current example were done using an operating system with Intel(R) Core(TM) i5 CPU (3.20 GHz) and 4 GB of installed memory (RAM) using MATLAB Software R2020b. The elapsed time to solve the LMI in this example is approximately 0.44 s.

Example 2. In order to analyse the effectiveness of the reviewed false-data detection methods, the second subsystem under the defined attacks is assumed with different initial conditions and attack features, as stated in the previous example. So, the dynamics of the 2nd subsystem are given as the following form

$$\dot{x} = (A + \Delta A)\, x(t) + B\tilde{u}(t) + (H + \Delta H)\, x(t - d(t)),$$

$$\tilde{u}(t) = u(t - d(t)),\ u(t) = k\tilde{x}(t),$$

$$\tilde{x}(t) = x(t) + \begin{bmatrix} 1 & 0.1 & -1.2 \end{bmatrix}^T v(t),$$

where the uncertain matrices $\Delta A(t)$ and $\Delta H(t)$ satisfy the conditions $\Delta A \leq 0.3$ and $\Delta H \leq 0.1$. Also, $\bar{D} = D = I$, $\bar{E} = 0.2I$ and $E_1 = 0.1I$. Moreover, the term $\begin{bmatrix} 1 & 0.1 & -1.2 \end{bmatrix}^T v(t)$ denotes the injected false-data attack with a non-normal distribution.

As we discussed earlier, since the combined attacks' distributions are non-Gaussian, previous conventional robust controllers like the one studied in [29] are unsuccessful in controlling the system's states under uncertainties with skew-distributed attacks. This matter is depicted in Figure 4. According to Figure 4, after the attacks' occurrence, under the conventional robust controller, the system states will not remain bounded over time.

Alternatively, the performance of the proposed robust control solution for the 2nd subsystem under the defined attacks is

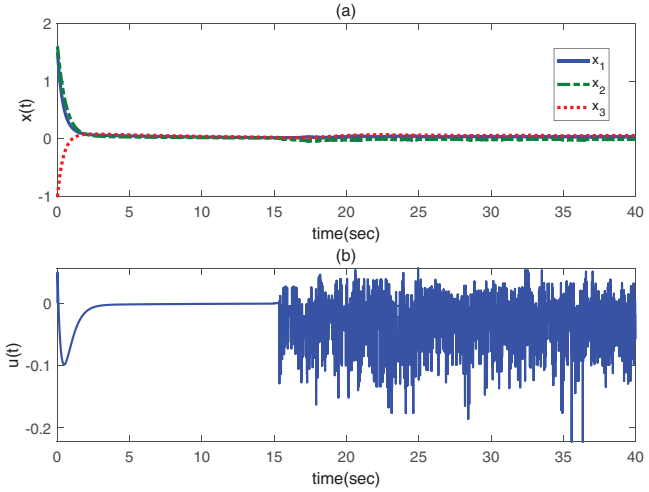

FIGURE 5 (a) System states convergence and (b) control input trajectory with the proposed robust control solution under simultaneous non-Gaussian skew-distributed data integrity and time-delay attacks

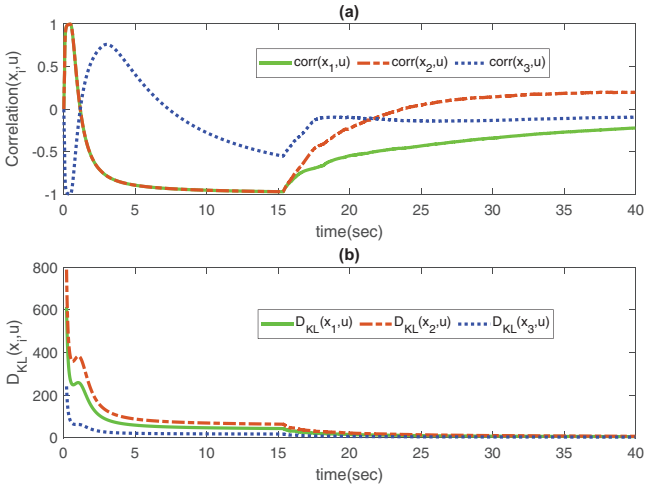

FIGURE 6 (a) Spearman's correlation coefficient and (b) the K–L divergence alterations between all the three output states and the control input $u(t)$ under the time-delay and data integrity attack. In order to evaluate the capability of NP classification methods in attack-detection scenarios, given tables are provided to represent the test results of various NP classification techniques on the simulation data.

demonstrated in Figure 5. Based on Figure 5, even by existing multiple non-Gaussian skew-distributed deception attacks, the designed robust controller performs appropriately, and the control input remains bounded, which provides the system's stability and bounded states from the time of attacks' occurrence (in the 15th second) and overtime. Finally, the system's trustworthiness is guaranteed under multiple skew-distributed non-normal deception attacks.

In the following, Spearman's correlation coefficient and Pettitt's tests are applied to detect the attack's occurrence rapidly. In Figure 6, the Spearman's correlation coefficient and the K–L divergence (Kullback–Leibler divergence) alterations between all the three output states and the control input $\tilde{u}(t)$ are demonstrated. Unlike using the K–L divergence criterion, Spearman's correlation coefficient between the transient states and sudden changes due to the attacks significantly differs in detecting faults. The occurrence of the attack and reduction of the linear association between the input and output of the system decreases the size of the correlation coefficient with a fast convergence to zero in the K–L divergence method and therefore, these kinds of attacks can degrade the system's performance stealthily under the supervision of the K–L divergence fault detection method.

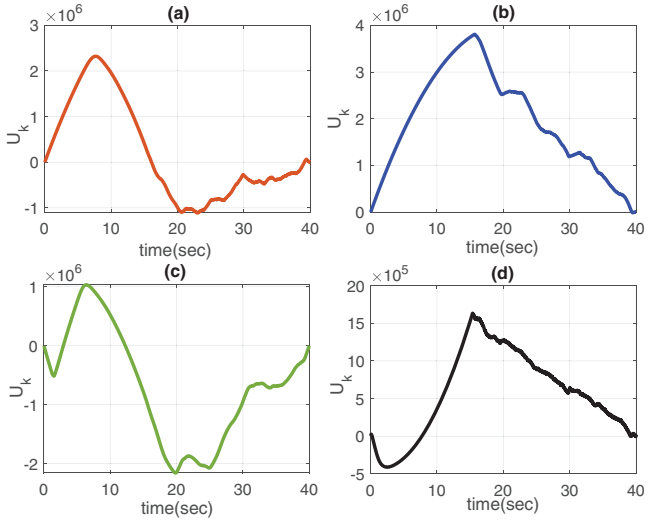

FIGURE 7 The proposed Pettitt's test evaluation to find point changes in the process of available system data, including (a) Pettitt's test of the system state x_1, (b) Pettitt's test of the system state x_2, (c) Pettitt's test of the system state x_3, and (d) Pettitt's test of the system's control input $u(t)$

In Figure 7, Pettitt's test is proposed to find point changes in the process of available system data, including system states x_1, x_2, x_3 and the system control input $\tilde{u}(t)$. Unlike the correlation-based methods, it is not required to simultaneously use both input and output data to obtain Pettitt's test value. Therefore, this test can be implemented separately on each input or output data set. From Figure 7, we can observe that Pettitt's test between $x_3(t)$ data set and the control input $\tilde{u}(t)$ correctly detects the exact point of signal trend changes and the maximum value of $|U_t|$ under the $p$value ≤ 0.05 with high accuracy. However, a change in the trend of the signal $x_3(t)$ is detected with a delay.

Observed from the figures and given the fact that the control input signal $\tilde{u}(t)$ through the applied feedback is a linear combination of system states, we expect that one alternative is to use Pettitt's test to detect faults very quickly when deception non-Gaussian attacks occur and alarm the operator to develop defence and control strategies as soon as possible and prevent the whole system to enter the failure phase. Alternatively, Spearman's correlation analysis is not affected by outlier data since Spearman's correlation analysis is also practical to develop false-data detection frameworks because the injected noise signals by the attacker are non-normal with the skew distribution. Therefore, the real-time fault detection approach

TABLE 1 Performance results of the different NP algorithms for false positive rate $\alpha = 0.01$

NP methods	Type I error ($\alpha = 0.01$)	Overall accuracy ($\alpha = 0.01$)
LR	0	0.360
RF	0.002	0.750
SVM	0.004	0.740
LDA	0.005	0.410
NB	0.005	0.570
AB	0.002	0.750
CT	0	0.690

TABLE 2 Performance results of the different NP algorithms for false positive rate $\alpha = 0.05$

NP methods	Type I error ($\alpha = 0.05$)	Overall accuracy ($\alpha = 0.05$)
LR	0.012	0.745
RF	0.022	0.757
SVM	0.035	0.740
LDA	0.041	0.737
NB	0.035	0.732
AB	0.007	0.747
CT	0	0.691

TABLE 3 Performance results of the different NP algorithms for false positive rate $\alpha = 0.1$

NP methods	Type I error ($\alpha = 0.1$)	Overall accuracy ($\alpha = 0.1$)
LR	0.012	0.745
RF	0.036	0.756
SVM	0.083	0.735
LDA	0.086	0.736
NB	0.075	0.717
AB	0.007	0.747
CT	0	0.691

against skew-distributed non-Gaussian deception attacks can be achieved by implementing Spearman's correlation analysis and Pettitt's change-point detection test. In obtaining simulation results, 1530 data samples are considered as uncorrupted data (Class 1 dataset), while 1400 data samples are assumed to be corrupted (Class 0 dataset). As a result, values obtained in Tables 1–3 verify the fact that developed NP-based classifiers have type I errors less than the pre-defined error threshold α. Besides, according to these tables, the false-positive error can easily be kept close to 0. Therefore, by applying NP classification algorithms are feasible in detecting false data or reducing the attacks' non-detection (false-positive) errors.

Since various computational and control processes are combined to form an IoT-based network structure in industry these days, it is always interesting to guarantee the network's functionality. This matter can only be achieved through analysing input/output signals from each operating device online for the goal of tracking the network's behaviour. Our proposed fault detection algorithm based on statistical analysis can be applied to such networks where multiple subsystems with various types of probability distributions of their inputs and outputs with/without time delays exist and being altered simultaneously. Additionally, with the proposed attack detection protocol, malicious signals can be distinguished quickly by applying signals' trend analysis methods introduced in the current paper to enhance the network's efficiency from technical and operational perspectives under non-divergent and non-residue faulty signals.

The simulations of the current example were done using an operating system with Intel(R) Core(TM) i5 CPU (3.20 GHz) and 4 GB of installed memory (RAM) using MATLAB Software R2020b. The elapsed time to solve the LMI in this example is ≈0.03 s. Moreover, the statistical analysis in the current article has been performed using the R software (version 4.0.4).

6 | CONCLUSION AND FUTURE WORK

In the present article, attack detection solutions and robust control in interconnected uncertain CPSs in the presence of replayed time-varying delays and non-normal skew-distributed deception attacks have been proposed. Under these circumstances, various novel false-data detection methods are provided to alarm the attacks' existence very quickly by implementing statistical and trend analysis methods, such as Spearman's correlation analysis and Pettitt's test change-point detection criterion. Furthermore, the effectiveness of the proposed Spearman and Pettitt tests is evaluated via numerical results compared to the commonly studied K–L divergence false-data detection method. Additionally, a novel robust fault-tolerant controller has been proposed that can guarantee stability of a system under various combined attacks, such as time-delay and false-data injection attacks. Finally, numerical results demonstrate the trustworthiness of the presented robust control approach under non-Gaussian cyber intruders. Future work will apply the presented robust control and fault detection framework to power management networks, smart data centres, intelligent transportation systems or mobile networks to maintain their secure performance. Moreover, resilient, adaptive control and defence strategies will be conducted in the future.

AUTHOR CONTRIBUTIONS

Salman Baroumand: Conceptualization; Data curation; Formal analysis; Investigation; Methodology; Project administration; Resources; Software; Supervision; Validation; Visualization; Writing – original draft; Writing – review & editing. Amirreza Zaman: Conceptualization; Data curation; Formal analysis; Funding acquisition; Investigation; Methodology; Project administration; Resources; Validation; Visualization; Writing – original draft; Writing – review & editing. Lyudmila Mihaylova: Formal analysis; Investigation; Methodology; Validation; Writing – review & editing

ACKNOWLEDGEMENTS

A. Zaman acknowledges the funding support by the Horizon 2020 Research Programme of the European Comission under the grant number 956059 (ECO-Qube). L. Mihaylova acknowledges the funding support by the EPSRC Project EP/V026747/1 (Trustworthy Autonomous Systems Node in Resilience). For the purpose of open access, the author has applied a Creative Commons Attribution (CC BY) licence to any Author Accepted Manuscript version arising.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

DATA AVAILABILITY STATEMENT

Data availability is not applicable to this paper.

REFERENCES

1. Gu, Z., Park, J.H., Yue, D., Wu, Z., Xie, X.: Event-triggered security output feedback control for networked interconnected systems subject to cyber-attacks. IEEE Trans. Syst., Man, Cybern.: Syst. (1), 1–10 (2020)
2. Gao, R., Zhai, D., Cheng, J.: Decentralized static output feedback sliding mode control for interconnected descriptor systems via linear sliding variable. Appl. Math. Comput. 357, 185–198 (2019)
3. Li, J., Zhang, Q.: Fuzzy reduced-order compensator-based stabilization for interconnected descriptor systems via integral sliding modes. IEEE Trans. Syst., Man, Cybern.: Syst. 49(4), 752–765 (2019)
4. Zhai, D., Liu, X., Liu, Y.: Adaptive decentralized controller design for a class of switched interconnected nonlinear systems. IEEE Trans. Cybern. 50(4), 1644–1654 (2020)
5. Liang, H., Zhang, Y., Huang, T., Ma, H.: Prescribed performance cooperative control for multiagent systems with input quantization. IEEE Trans. Cybern. 50(5), 1810–1819 (2020)
6. Peng, C., Han, Q., Yue, D.: Communication-delay-distribution-dependent decentralized control for large-scale systems with ip-based communication networks. IEEE Trans. Control Syst. Technol. 21(3), 820–830 (2013)
7. Li, Y.G., Yang, G.H.: Worst-case ∈-stealthy false data injection attacks in cyberphysical systems. Inf. Sci. 515, 352–364 (2020)
8. Ge, X., Han, Q.L., Zhong, M., Zhang, X.M.: Distributed krein space-based attack detection over sensor networks under deception attacks. Automatica 109, 108557 (2019)
9. Yan, H., Hu, C., Zhang, H., Karimi, H.R., Jiang, X., Liu, M.: h_∞ output tracking control for networked systems with adaptively adjusted event-triggered scheme. IEEE Trans. Syst., Man, Cybern.: Syst. 49(10), 2050–2058 (2019)
10. Zaman, A., Safarinejadian, B., Birk, W.: Security analysis and fault detection against stealthy replay attacks. Int. J. Control. 95, 1–22 (2020)
11. Sargolzaei, A., Yen, K.K., Abdelghani, M.N., Sargolzaei, S., Carbunar, B.: Resilient design of networked control systems under time delay switch attacks, application in smart grid. IEEE Access 5, 15901–15912 (2017)
12. Baroumand, S., Zaman, A., Mihaylova, L.: Trust-based fault detection and robust fault-tolerant control of uncertain cyber-physical systems against timedelay injection attacks. Heliyon 7(6), e07294 (2021). https://www.sciencedirect.com/science/article/pii/S2405844021013979
13. Jin, D., Hu, M., Chen, B., Yu, L.: Secure h_∞ control against time-delay attacks in cyber-physical systems. J. Control Decis 9. 1–11 (2021)
14. Asghar, H.J., Kaafar, D.: Averaging attacks on bounded noise-based disclosure control algorithms. Proc. Privacy Enhancing Technol. 2020(2), 358–378 (2020)
15. Hu, S., Yue, D., Chen, X., Cheng, Z., Xie, X.: Resilient h_∞ filtering for event-triggered networked systems under nonperiodic dos jamming attacks. IEEE Trans. Syst., Man, Cybern.: Syst. 51, 1392–1403 (2019)
16. Xie, C.H., Yang, G.H.: Secure estimation for cyber-physical systems with adversarial attacks and unknown inputs: An l_2-gain method. Int. J. Robust Nonlinear Control 28(6), 2131–2143 (2018)
17. Guo, Z., Shi, D., Johansson, K.H., Shi, L.: Worst-case stealthy innovation-based linear attack on remote state estimation. Automatica 89, 117–124 (2018)
18. Li, Y.G., Yang, G.H.: Optimal stealthy false data injection attacks in cyberphysical systems. Inf. Sci. 481, 474–490 (2019)
19. Zhang, R., Venkitasubramaniam, P.: Stealthy control signal attacks in linear quadratic gaussian control systems: Detectability reward tradeoff. IEEE Trans. Inf. Forensics Secur. 12(7), 1555–1570 (2017)
20. Colbert, E.J., Kott, A.: Cyber-security of scada and other industrial control systems. Springer, 66, (2016)
21. Ma, X.J., Wang, H.: Blind false data injection attacks in smart grids subject to measurement outliers. J. Control Decis. 9(4), 1–10 (2022)
22. Der Kiureghian, A., Ditlevsen, O.: Aleatory or epistemic? does it matter? Struct. Saf. 31(2), 105–112 (2009)
23. Tao, X., Lu, J., Chen, D., Törngren, M.: Probabilistic inference of fault condition of cyber-physical systems under uncertainty. IEEE Syst. J. 14, 3256–3266 (2020)
24. De Persis, C., Tesi, P.: Networked control of nonlinear systems under denial-ofservice. Syst. Control Lett. 96, 124–131 (2016)
25. Zhang, H., Hu, J., Liu, G.P., Yu, X.: Event-triggered secure control of discrete systems under cyber-attacks using an observer-based sliding mode strategy. Inf. Sci. 587, 587–606 (2022)
26. Xu, W., Hu, G., Ho, D.W., Feng, Z.: Distributed secure cooperative control under denial-of-service attacks from multiple adversaries. IEEE Trans. Cybern. 50, 3458–3467 (2019)
27. Feng, Z., Hu, G.: Secure cooperative event-triggered control of linear multiagent systems under dos attacks. IEEE Trans. Control Syst. Technol. 28(3), 741–752 (2019)
28. Zhang, D., Feng, G.: A new switched system approach to leader-follower consensus of heterogeneous linear multiagent systems with dos attack. IEEE Trans. Syst., Man, Cybern.: Syst. 51, 1258–1266 (2019)
29. Li, Z., Zhao, X., Yu, J.: On robust control of continuous-time systems with state-dependent uncertainties and its application to mechanical systems. ISA Trans. 60, 12–20 (2016)
30. Van Der Schaft, A.J.: L_2-gain analysis of nonlinear systems and nonlinear state feedback h_∞ control. IEEE Trans. Autom. Control 37(6), 770–784 (1992)
31. Pettitt, A.: A non-parametric approach to the change-point problem. J. R. Stat. Soc. Ser. C 28(2), 126–135 (1979)
32. Bartels, R.: The rank version of von neumann's ratio test for randomness. J. Am. Statist. Assoc. 77(377), 40–46 (1982)
33. Buishand, T.A.: Some methods for testing the homogeneity of rainfall records. J. Hydrol. 58(1-2), 11–27 (1982)
34. Alexandersson, H.: A homogeneity test applied to precipitation data. J. Climatol. 6(6), 661–675 (1986)
35. Tong, X., Feng, Y., Li, J.J.: Neyman-pearson classification algorithms and np receiver operating characteristics. Sci. Adv. 4(2), 2623–2640 (2018). https://advances.sciencemag.org/content/4/2/eaao1659
36. Zhao, A., Feng, Y., Wang, L., Tong, X.: Neyman-pearson classification under high-dimensional settings. J. Mach. Learn. Res. 17(1), 7469–7507 (2016)
37. Kumar, P.A.R., Selvakumar, S.: Distributed denial of service attack detection using an ensemble of neural classifier. Comput. Commun. 34(11), 1328–1341 (2011)
38. Boyd, S., El Ghaoui, L., Feron, E., Balakrishnan, V.: Linear matrix inequalities in system and control theory. Studies in Applied Mathematics. vol. 15. SIAM, Philadelphia, PA (1994)
39. de Souza, C.E., Li, X.: Delay-dependent robust h_∞ control of uncertain linear state-delayed systems. Automatica 35(7), 1313–1321 (1999)

How to cite this article: Baroumand, S., Zaman, A., Mihaylova, L.: Attack detection and fault-tolerant control of interconnected cyber-physical systems against simultaneous replayed time-delay and false-data injection attacks. IET Control Theory Appl. 1–15 (2022). https://doi.org/10.1049/cth2.12393

APPENDIX A

This section includes lemmas and the proof of theorem stated in previous sections.

Lemmas

Lemma 1. *[38, 39]: For any* $z,\ y \in R^n$ *and any positive definite matrix* $X \in R^{n\times n}$, *we have*

$$-2z^T y \le z^T X^{-1} z + y^T X y$$

Lemma 2. *[38, 39]: Let* A, D, E, *and* F *be real matrices of appropriate dimensions with* $F \le I$. *Accordingly, it can be concluded that*

For any scalar $\epsilon > 0$,

$$DFE + E^T F^T D^T \le \varepsilon^{-1} DD^T + \varepsilon E^T E$$

Furthermore, for any matrix $H > 0$ and scalar $\varepsilon > 0$, which applies to the inequality $\varepsilon I - EHET > 0$, we have

$$(A + DFE)\, H (A + DFE)^T \le AHA^T + \varepsilon DD^T + \Delta,$$

where $\Delta = AHE^T (\varepsilon I - EHET)^{-1} EHA^T$. Alternatively, for any matrix $H > 0$ and scalar $\varepsilon > 0$, which applies to the inequality

$H - \varepsilon DD^T > 0$, it is drawn that

$$(A + DFE)^T H^{-1} (A + DFE) \le A^T \left(H - \varepsilon DD^T\right)^{-1} A + \Delta$$

where $\Delta = \varepsilon^{-1} E^T E$

Proof of Theorem 1

From (12) to (15), the below derivative is obtained:

$$\frac{d}{dt}\left(\begin{bmatrix} x_i^T(t) & y_i^T(t) \end{bmatrix} E\, P_i \begin{bmatrix} x_i(t) \\ y_i(t) \end{bmatrix} \right) = 2\lambda, \tag{A1}$$

where $\lambda = [x_i^T(t) \quad y_i^T(t)] P_i^T \begin{bmatrix} y_i(t) \\ \Theta_i(t) \end{bmatrix}$ and $\Theta_i(t) = -y_i(t) + \tilde{A}_i x_i(t) + \left(\sum_{k=0}^{m_i} \tilde{H}_{i_k}\right) x_i(t) - \sum_{k=0}^{m_i} \tilde{H}_{i_k} \int_{t-\tau_{i_k}}^{t} y_i(s)\, ds + G_i\, \theta_i(t)$.

Thus, the derivatives of the assumed Lyapunov functions are as

$$\frac{dV_1}{dt} = \sum_{k=1}^{m_i} y_i^T(t)\, Q_{i_k} y_i(t) - \sum_{k=1}^{m_i} y_i^T\left(t-\tau_{i_k}\right) Q_{i_k} y_i\left(t-\tau_{i_k}\right), \tag{A2}$$

$$\frac{dV_2}{dt} = \sum_{k=1}^{m_i} x_i^T(t)\, U_{i_k} x_i(t) - \sum_{k=1}^{m_i} x_i^T\left(t-\tau_{i_k}\right) U_{i_k} x_i\left(t-\tau_{i_k}\right), \tag{A3}$$

Consequently, $\frac{dV}{dt}$ equals to

$$\begin{aligned}
\frac{dV}{dt} &= \mu \begin{bmatrix} 0 & I \\ 0 & -I \end{bmatrix} \begin{bmatrix} x_i(t) \\ y_i(t) \end{bmatrix} \\
&+ \mu \begin{bmatrix} 0 & 0 \\ \tilde{A}_i + \sum_{k=0}^{m_i} \tilde{H}_{i_k} & 0 \end{bmatrix} \begin{bmatrix} x_i(t) \\ y_i(t) \end{bmatrix} \\
&- \mu \begin{bmatrix} 0 \\ \sum_{k=0}^{m_i} \tilde{H}_{i_k} \int_{t-\tau_{i_k}}^{t} y_i(s)\, ds \end{bmatrix} + \mu \begin{bmatrix} 0 \\ G_i \end{bmatrix} \theta_i(t) \\
&+ \sum_{k=1}^{m_i} y_i^T(t)\, Q_{i_k} y_i(t) \\
&- \sum_{k=1}^{m_i} y_i^T\left(t-\tau_{i_k}\right) Q_{i_k} y_i\left(t-\tau_{i_k}\right) \\
&+ \sum_{k=1}^{m_i} x_i^T(t)\, U_{i_k} x_i(t) - \sum_{k=1}^{m_i} x_i^T\left(t-\tau_{i_k}\right) U_{i_k} x_i\left(t-\tau_{i_k}\right),
\end{aligned}$$

where $\mu = 2[x_i^T(t) \quad y_i^T(t)] P_i^T$. Hence, the Hamiltonian function (10) can be rewritten as

$$J_H = \xi_i \begin{bmatrix} \tilde{\Psi} & 0 & 0 & 0 & 0 & 0 & 0 & \mathrm{P_i^T} \begin{bmatrix} 0 \\ \mathrm{G_i} \end{bmatrix} \\ * & -\mathrm{Q_1} & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & \ddots & 0 & 0 & 0 & 0 & 0 \\ * & * & * & -\mathrm{Q_{m_i}} & 0 & 0 & 0 & 0 \\ * & * & * & * & \mathrm{U_1} & 0 & 0 & 0 \\ * & * & * & * & * & \ddots & 0 & 0 \\ * & * & * & * & * & * & \mathrm{U_{m_i}} & 0 \\ * & * & * & * & * & * & * & -\gamma^2 \mathrm{I} \end{bmatrix}$$

$$\xi_i^T + \sum_{k=0}^{m_i} \tilde{\eta}_{i_k} + Z_i^T Z_i, \tag{A4}$$

where

$$\begin{aligned}
\xi_i = \big[& x_i^T(t) \quad y_i^T(t) \quad y_i^T\left(t-\tau_{i_1}\right) \quad \ldots \quad y_i^T\left(t-\tau_{i\,m_i}\right) \\
& x_i^T\left(t-\tau_{i_1}\right) \quad \ldots \quad y_i^T\left(t-\tau_{i\,m_i}\right) \quad \theta_i^T(t) \big],
\end{aligned} \tag{A5}$$

and

$$\begin{aligned}
\tilde{\Psi} = P_i^T & \begin{bmatrix} 0 & I \\ \tilde{A}_i + \sum_{k=0}^{m_i} \tilde{H}_{i_k} & -I \end{bmatrix} + \begin{bmatrix} 0 & \tilde{A}_i^T + \sum_{k=0}^{m_i} \tilde{H}_{i_k}^T \\ I & -I \end{bmatrix} P_i \\
& + \begin{bmatrix} \sum_{k=1}^{m_i} U_{i_k} + C_i C_i^T & 0 \\ 0 & \sum_{k=1}^{m_i} Q_{i_k} \end{bmatrix},
\end{aligned} \tag{A6}$$

and

$$\tilde{\eta}_{i_k} = -2\int_{t-\tau_{i_k}}^{t} \begin{bmatrix} x_i^T(t) & y_i^T(t) \end{bmatrix} P_i^T \begin{bmatrix} 0 \\ \tilde{H}_{i_k} \end{bmatrix} y_i(s)\, ds\,. \tag{A7}$$

Using Lemmas 1 and 2, we can observe that

$$\tilde{\eta}_{i_k} \le \tau_{i_k} \begin{bmatrix} x_i^T(t) & y_i^T(t) \end{bmatrix} P_i^T \begin{bmatrix} 0 \\ \tilde{H}_{i_k} \end{bmatrix} R_{i_k}^{-1} \begin{bmatrix} 0 & \tilde{H}_{i_k} \end{bmatrix} \times P_i \begin{bmatrix} x_i(t) \\ y_i(t) \end{bmatrix} + \int_{t-\tau_{i_k}}^{t} y_i^T(s) R_{i_k} y(s)\, ds \le \eta_{i_k},$$

with η_{i_k} defined as

$$\begin{aligned} \eta_{i_k} = {} & \begin{bmatrix} x_i^T(t) & y_i^T(t) \end{bmatrix} \tau_{i_k} P_i^T \left(\begin{bmatrix} 0 \\ H_{i_k} \end{bmatrix} R_{i_k}^{-1} \begin{bmatrix} 0 & H_{i_k}^T \end{bmatrix} \right. \\ & + \begin{bmatrix} 0 \\ H_{i_k} \end{bmatrix} R_{i_k}^{-1} \begin{bmatrix} 0 & E_{i_k}^T \end{bmatrix} \\ & \left(\xi_{i_k} I - \begin{bmatrix} 0 \\ E_{i_k} \end{bmatrix} R_{i_k}^{-1} \begin{bmatrix} 0 & E_{i_k}^T \end{bmatrix} \right)^{-1} \begin{bmatrix} 0 \\ E_{i_k} \end{bmatrix} \\ & \left. R_{i_k}^{-1} \begin{bmatrix} 0 & H_{i_k}^T \end{bmatrix} \right) \\ & P_i \begin{bmatrix} x_i(t) \\ y_i(t) \end{bmatrix} + \tau_{i_k} \begin{bmatrix} x_i^T(t) & y_i^T(t) \end{bmatrix} \\ & P_i^T \xi_{i_k} \begin{bmatrix} 0 & 0 \\ 0 & D_{i_k} D_{i_k}^T \end{bmatrix} P_i \begin{bmatrix} x_i(t) \\ y_i(t) \end{bmatrix}, \end{aligned} \tag{A8}$$

And for the positive value of ξ_{i_k}, the term $\xi_{i_k} I - \begin{bmatrix} 0 \\ E_{i_k} \end{bmatrix} R_{i_k}^{-1} \begin{bmatrix} 0 & E_{i_k}^T \end{bmatrix}$ is a positive value for $k = 0, \ldots, m_i$.

Furthermore, the following inequality can be derived for $\tilde{\Psi}$.

$$\begin{aligned} \tilde{\Psi} \le \Psi = {} & P_i^T \begin{bmatrix} 0 & I \\ A_i + \sum_{k=0}^{m_i} H_{i_k} & -I \end{bmatrix} \\ & + \begin{bmatrix} 0 & A_i + \sum_{k=0}^{m_i} H_{i_k} \\ I & -I \end{bmatrix} P_i + \begin{bmatrix} \sum_{k=1}^{m_i} U_{i_k} + C_i C_i^T & 0 \\ 0 & \sum_{k=1}^{m_i} Q_{i_k} \end{bmatrix} \\ & + P_i^T \begin{bmatrix} 0 & 0 \\ 0 & \sum_{k=0}^{m_i} \xi_{i_k}^{-1} D_{i_k} D_{i_k}^T \end{bmatrix} P_i + \begin{bmatrix} \sum_{k=0}^{m_i} \xi_{i_k} E_{i_k} E_{i_k}^T & 0 \\ 0 & 0 \end{bmatrix} \\ & + P_i^T \begin{bmatrix} 0 & 0 \\ 0 & \xi_i^{-1} \bar{D}_i \bar{D}_i^T \end{bmatrix} P_i + \begin{bmatrix} \xi_i \bar{E}_i \bar{E}_i^T & 0 \\ 0 & 0 \end{bmatrix}, \end{aligned}$$

where $\xi_i > 0$, $\xi_{i_k} > 0$, $k = 1, \ldots, m_i$. Thus, based on (24) to (29), the below inequality can be concluded

$$J_H \le \xi_i \begin{bmatrix} \Psi & 0 & 0 & 0 & 0 & 0 & 0 & \mathrm{P}^{\mathrm{T}} \begin{bmatrix} 0 \\ \mathrm{G_i} \end{bmatrix} \\ * & -\mathrm{Q}_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & \ddots & 0 & 0 & 0 & 0 & 0 \\ * & * & * & -\mathrm{Q}_{\mathrm{m_i}} & 0 & 0 & 0 & 0 \\ * & * & * & * & \mathrm{U}_1 & 0 & 0 & 0 \\ * & * & * & * & * & \ddots & 0 & 0 \\ * & * & * & * & * & * & \mathrm{U}_{\mathrm{m_i}} & 0 \\ * & * & * & * & * & * & * & -\gamma^2 \mathrm{I} \end{bmatrix} \times \xi_i^T + \textstyle\sum_{k=0}^{m_i} \eta_{i_k} + Z_i^T Z_i. \tag{A10}$$

According to (30) and applying Schur complement in deriving further equations, we can conclude that $J_H \le 0$ if the below LMI holds:

$$\mathrm{W}_1 = \begin{bmatrix} \bar{\Psi} & 0 & 0 & \mathrm{P_i^T} \begin{bmatrix} 0 \\ \mathrm{G_i} \end{bmatrix} & \theta_3 & \begin{bmatrix} \mathrm{vec\{I\}} \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ \mathrm{vec\{I\}} \end{bmatrix} \\ 0 & \theta_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \theta_2 & 0 & 0 & 0 & 0 \\ * & 0 & 0 & -\gamma^2 \mathrm{I} & 0 & 0 & 0 \\ * & * & * & * & \theta_4 & 0 & 0 \\ * & * & * & * & * & \theta_5 & 0 \\ * & * & * & * & * & * & \theta_6 \end{bmatrix} < 0$$

$$\mathrm{W}_2 = \left(\xi_{i_k} I - \begin{bmatrix} 0 \\ E_{i_k} \end{bmatrix} R_{i_k}^{-1} \begin{bmatrix} 0 & E_{i_k}^T \end{bmatrix} \right) > 0, k = 0, \ldots, m_i, \tag{A11}$$

where

$$\begin{aligned} \bar{\Psi} = {} & P_i^T \begin{bmatrix} 0 & I \\ A_i + \sum_{k=0}^{m_i} H_{i_k} & -I \end{bmatrix} + \begin{bmatrix} 0 & A_i^T + \sum_{k=0}^{m_i} H_{i_k}^T \\ I & -I \end{bmatrix} P_i \\ & + \begin{bmatrix} C_i C_i^T & 0 \\ 0 & 0 \end{bmatrix} + P_i^T \begin{bmatrix} 0 & 0 \\ 0 & \xi_i^{-1} \bar{D}_i \bar{D}_i^T + \sum_{k=0}^{m_i} \xi_{i_k}^{-1} D_{i_k} D_{i_k}^T \end{bmatrix} \\ & + \begin{bmatrix} \xi_i \bar{E}_i \bar{E}_i^T + \sum_{k=0}^{m_i} \xi_{i_k} E_{i_k} E_{i_k}^T & 0 \\ 0 & 0 \end{bmatrix} + P_i^T \begin{bmatrix} 0 & 0 \\ 0 & \sum_{k=0}^{m_i} \tau_{i_k} \xi_{i_k} D_{i_k} D_{i_k}^T \end{bmatrix} P_i \end{aligned} \tag{A12}$$

Also, variables θ_i, $I = 1, \ldots, 6$ are defined as

$\theta_1 = -diag\{Q_{i_k}\}, \theta_2 = -diag\{U_{i_k}\}, \theta_5 = -diag\{U_{i_k}^{-1}\}, \theta_6 = -diag\{Q_{i_k}^{-1}\}, k = 1, \ldots, m_i$;

$$\theta_3 = vec\left\{\tau_{i_k} P_i^T \begin{bmatrix} 0 \\ H_{i_k} \end{bmatrix} R_{i_k}^{-1} \begin{bmatrix} 0 & H_{i_k}^T \end{bmatrix}\right\},$$

$$\theta_4 = -diag\left\{\tau_{i_k}\left(\xi_{i_k} I - \begin{bmatrix} 0 \\ E_{i_k} \end{bmatrix} R_{i_k}^{-1} \begin{bmatrix} 0 & E_{i_k}^T \end{bmatrix}\right)\right\},$$

$= 0, \ldots, m_i.$

Let us define $\Xi = diag\{X_i, I, I, I, I, I\}$, $X_i = P_i^{-1}$, and denote $X_1 K_i$ by Y_i, $\bar{Q}_{i_k} = Q_{i_k}^{-1}$ and $\bar{U}_{i_k} = U_{i_k}^{-1}$. Then, by pre and post multiplying (31) by Ξ and Ξ^T, respectively, and using Schur formula again, the inequality in (16) will be obtained.

The proof of Theorem 1 is completed.