An International Journal of Optimization and Control: Theories & Applications
ISSN: 2146-0957 eISSN: 2146-5703
Vol.16, No.2, pp.598-618 (2026)
https://doi.org/10.36922/IJOCTA025500227

RESEARCH ARTICLE

Secure control of wireless networked control systems subject to stochastic deception attacks

Mutaz M. Hamdan[1*] and Nezar M. Alyazidi[2,3]

[1]Robotics and Artificial Intelligence Engineering Department, Faculty of Engineering, Al-Ahliyya Amman University, Amman, Jordan
[2]Control and Instrumentation Engineering Department, College of Engineering and Physics, King Fahd University of Petroleum Minerals, Dhahran, Eastern Province, Saudi Arabia
[3]Interdisciplinary Research Center for Smart Mobility and Logistics, King Fahd University of Petroleum & Minerals, Dhahran, Eastern Province, Saudi Arabia
mutaz.hamdan82@gmail.com, nalyazidi@kfupm.edu.sa

ARTICLE INFO

Article History:
Received: December 10, 2025
Revised: January 19, 2026
Accepted: January 26, 2026
Published Online: March 4, 2026

Keywords:
Wireless networked control systems
Cyberattacks
Secure control
Observer-based control
Stochastic delays
Linear matrix inequalities
Interconnected power systems

ABSTRACT

Given that power systems are essential to modern life and electricity demand continues to rise, ensuring their reliable and secure operation has become a critical priority. Wireless networked control systems (WNCSs), which rely on wireless channels for communication between controllers, sensors, and actuators, are increasingly deployed in energy systems such as multi-area interconnected power systems to enhance flexibility and scalability. WNCSs are susceptible to deception attacks and time-varying communication delays that can compromise interconnection stability and deteriorate performance. This paper presents an observer-based secure control methodology that models deception via independent Bernoulli processes with unknown attack probabilities, while explicitly considering actuation and measurement delays. Using a Lyapunov stability framework, we established computationally feasible linear matrix inequality conditions enabling the co-design of the controller and observer with proven stability and disturbance rejection. A two-area interconnected power-system case study validates the approach. The proposed method was tested with offline gains covering nine scenarios. Results indicate that the method sustains closed-loop performance across all nine combined attack/delay scenarios and recovers quickly even in worst-case conditions, supporting secure control of WNCSs in realistic adversarial environments.

1. Introduction

A wireless networked control system (WNCS) is a control architecture in which distributed nodes exchange signals using wireless links. Recent communication studies emphasize rapid, consistent link-to-link transmission through the channel, reducing time delay. [1] Limiting radio propagation to bounded areas strengthens security and supports interference control. [2]

In a WNCS, sensors collect data from the plant's output and transmit this sampled information to the control system through a wireless channel; subsequently, the controller generates control commands and sends them via the wireless link to the actuators to regulate the dynamics of the plant. [3]

Advances in computation, control, sensing, and wireless networking have strengthened coupling between feedback controllers, physical, and cyber processes. [4] This trend is evident in contemporary domains and applications such as the

*Corresponding Author

Internet of Things (IoT), cyber-physical systems, and the Internet that require a real-time control action. [3,5] The effects of random delays on the performance of IoT systems were discussed in earlier literature. [6] An overview of smart grid communication systems, co-simulation tools, and control has been provided, including their features, benefits, and drawbacks. [7]

The rising demand for distributed applications in manufacturing, power generation, and transportation motivates the adoption of WNCSs. In addition to the benefits of using mobile nodes in various applications, WNCSs provide flexibility in node placement, which decreases the maintenance work required for wired communication. [8] The flexibility, increased safety, and simplicity of installation and maintenance are just a few benefits of WNCSs.

Figure 1 illustrates a canonical WNCS architecture comprising a plant, a control system, sensors, actuators, and a wireless communication layer. Sensors relay measurements to the controller over a wireless link; the control system computes command inputs and returns them to the actuators over the wireless medium.

The swift expansion of technologies such as embedded and cloud computing, wireless networks, and advanced control has accelerated the development of WNCSs. Moreover, WNCSs now play a central role in Industry 4.0's. [9] Simultaneously, there have been significant advancements in the integration of modern wireless networking, computing, and control methodologies. A detailed survey of WNCS from a communications perspective is presented by Wang et al. [10] Prior research has explored various aspects, including sensing design strategies under energy and bandwidth constraints, state estimation issues over unreliable networks, control strategies to enhance WNCS performance, and appropriate WNCS architecture. By allocating network resources based on forecasts of the closed-loop efficacy and link quality at operation, Ma et al. [11] presented an optimal, dynamic transmission scheduling technique that optimizes the multiloop control performance. This strategy serves as a bridge between the closed-loop performance and the network architecture.

Industrial wireless sensor networks encounter substantial security vulnerabilities, including blackhole, wormhole, and identity replication attacks, necessitating precise attack detection. Alzubi [12] introduced an Fréchet–hyperbolic traffic-feature extraction with Dirichlet-based anomaly detection to overcome these difficulties and to enhance secure data delivery. Alzubi et al. [13] introduced an effective seeker optimization method within machine learning that optimized the model-critical parameters to improve performance robustness and detection reliability.

1.1. Related works

The resilience of WNCSs against various forms of cyberattacks, particularly in wireless control environments, has been the focus of extensive research in recent years. This subsection reviews related works that address secure control strategies and mitigation approaches. Yuan et al. [14] investigated resilient control for WNCSs under Denial-of-Service (DoS) attacks, modeling packet dropouts with a two-state Markov chain. A cross-layer approach with Nash power and optimal control strategies was used to maintain system performance. The security of WNCS was examined, taking into account system disruptions and external attacks in the study by Liu et al. [15] The genuine transmitter's power control was taken into consideration to prevent the attacker from conducting a cyberattack. Additionally, the Stackelberg game framework was suggested as a way to simulate the exchange between the broadcaster and the attacker. The control technique was designed at the physical layer by combining sliding mode control and linear quadratic regulator control. In the study by Cetinkaya et al., [16] the control input packets were sent over an unprotected wireless communication channel that is vulnerable to jamming assaults from a controller to a distant linear plant. It was demonstrated that even if the attacked system is stable without disturbance, jamming attacks can cause instability when the system experiences disruption.

Recently, the utilization of numerous alternative energy supplies has risen dramatically in electrical power facilities. Most distributed generating systems are located near consumption centers to provide electricity to local customers. Distributed generating systems encompass many methods, including microturbines, diesel-powered engines, hydrogen cells, photovoltaics, and windmills. Integrating clean energy sources introduces uncertainties that challenge the stability and reliability of multi-area interconnected power systems. [17] Due to communication limits, load fluctuations, and dynamic conditions, model-free controllers offer an effective solution for maintaining stable and dependable grid performance.

An online adaptive policy control scheme was developed to tackle the complexities of load frequency control in both single- and multi-area power grids. [18] This approach utilizes an optimal

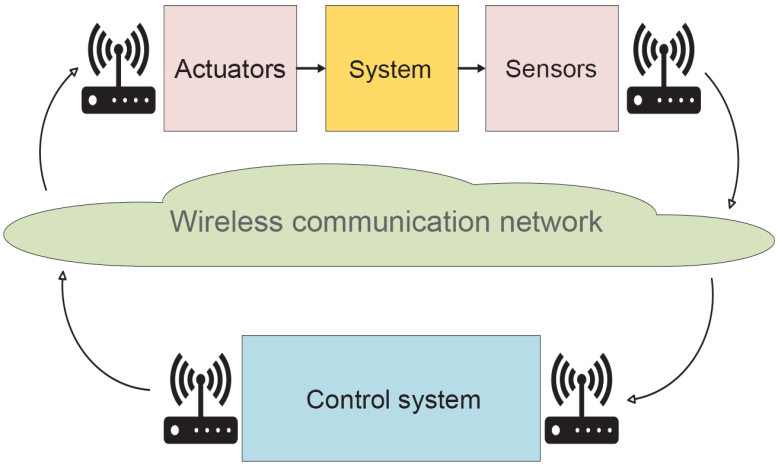

Figure 1. Model of a wireless networked control system

control framework integrating the Bellman equation and two neural networks. The first neural network estimates the value function of the proposed solution, while the second approximates the optimal control strategy.

Xu et al. [19] analyzed the resilience of switching network control systems subject to deception attacks, which were expressed as a Bernoulli process with undetermined variables. The switched controller enhanced efficiency despite specific subsystems destabilizing by unknown deception endeavours, enabling a robust way to attenuate cyber threats. Shi and Zhang [20] addressed resilient H_∞ networked control systems under packet losses and deception attacks modeled by Bernoulli distributions, using an observer-based controller. It ensures stochastic exponential stability and H_∞ performance, validated through linear matrix inequality (LMI)-based synthesis and an uninterruptible power supply simulation example. Devanathan et al. [21] presented a finite-time distributed state estimation-based control strategy for IoT-enabled microgrids under deception attacks, ensuring stability through Lyapunov analysis and linear matrix inequalities.

Dynamic event-triggered fuzzy control strategies for stabilizing direct current microgrids under false data injection attacks, network delays, and premise mismatching were proposed. [22,23] Li et al. [22] introduced a saturated fuzzy non-fragile controller that significantly reduced communication by 84.98%, while Li et al. [23] presented a discrete-time approach with a novel dynamic triggering mechanism that avoided Zeno behavior and achieved 27.5% communication savings even when 13.5% of data were being tampered with.

Meng et al. [24] focused on safe estimation for networked control systems in the presence of DoS attacks, disruptions, and noise. Abdelkader et al. [26] examined cyber threats, defense strategies, and recommendations for improving the reliability and resilience of current power systems. Huang et al. [26] reviewed reinforcement learning (RL) approaches for feedback-enabled cyber resilience, highlighting key challenges (detection, adaptability, and generalization) and outlining future research directions to strengthen resilient control systems.

The approach proposed in the current study differs from data-driven and RL-based methods by offering strong theoretical guarantees on stability and robustness under deception attacks. Unlike RL-based controllers, which require extensive training data and may lack formal safety assurances, our method is computationally efficient, reliable, and grounded in rigorous control-theoretic foundations.

Table 1 provides a summary of key previous studies, highlighting their employed methods, main findings, and inherent limitations. The comparison also clarifies how our proposed approach addresses these gaps and advances the state of the art in secure WNCSs. In summary, the established methods typically focus on single-channel vulnerabilities, such as measurement-side deception attacks, often neglecting the simultaneous impact of disturbances, system faults, and time-varying delays. Unlike these specialized tools, our approach provides a unified deception-attack framework that explicitly models stochastic interference on both sensing and actuation channels using independent Bernoulli processes. This comprehensive modeling of concurrent adversarial effects ensures system stability in realistic, worst-case environments where standard methods may fail to account for the full range of potential disruptions.

Table 1. Summary of previous studies on resilient control under cyber-physical attacks

Ref.	Attack type	Approach/Method	Main contribution	Limitations	Novelty of our proposed approach
[14]	DoS attack	Two-state Markov chain for DoS modeling; Nash equilibrium-based crosslayercontrol	Demonstrates robustness of crosslayer control under DoS conditions	Uses a simplified dropout model; scalability to complex networks not addressed	Unlike their DoS-only scheme, our approach addresses deception attacks while also considering disturbances, faults, and delays in both sensing and actuation channels.
[15]	DoS attack	Stackelberg game between transmitter and attacker	Introduces a game-theoretic design for robust communication under DoS	Relies on idealized attacker model; computational complexity increases with system size	Extends beyond DoS by developing a secure deception-resilient controller robust against disturbances and system faults.
[19]	Deception attack	Switching controllers; deception odeled as Bernoulli process	Improves resilience of networked systems under deceptioninduced instability	Does not consider disturbances and system faults	Improves upon Bernoullibased deception modeling by also considering disturbances, faults, and attacks on both measurement and actuation links.
[20]	Deception attack	Observer-based H_∞ control	Ensures stochastic exponential stability against deception attacks	Models packet losses and deception attacks separately	Provides a unified deception-attack framework that simultaneously covers both sensing and actuating attacks under faults and disturbances.
[21]	Deception attack	Finite-time distributed stateestimation based control	Provides robust control for IoT-enabled microgrids under deception	Limits attack modeling to measurement side deception	Extends measurement only modeling by addressing deception at both measurement and actuation channels, including disturbances and faults.
[22,23]	False data injection (FDI) attack	Fuzzy nonfragile controller with event-triggered scheme	Reduces communication and triggering load while maintaining stability	Focuses on FDI only; does not consider multiple concurrent attacks	Unlike their FDI-focused works, our method targets deception attacks with stochastic probabilities, variable delays, and practical disturbances/faults.

Abbreviations: DoS: Denial-of-Service; IoT: Internet of Things.

1.2. Main contributions

This subsection highlights the main contributions of our work in advancing WNCSs under deception attacks. Specifically, we present novel methodologies that enhance system resilience, ensure stability, and maintain performance despite adversarial disruptions.

This article's key contributions can be summarized as follows:

(i) Mitigation of a unified research limitation: This work presents a secure control framework that builds upon existing studies, which have primarily examined single-channel vulnerabilities or simplified dropout models. The proposed approach considers, within a unified formulation, the simultaneous presence of dual-channel deception attacks, time-varying communication delays, and external disturbances.

(ii) Improved Stochastic Attack Modeling: The developed scheme provides a more realistic illustration of adversarial behavior by explicitly modeling deception attacks on both sensing and actuation links as stochastic events. These are represented using independent Bernoulli processes with variable conditional probabilities, ensuring the system is stable even when attack frequencies are unknown a priori.

(iii) Systematic Mathematical Framework: We introduce a modeling framework that integrates combined probabilistic threats and variable delays into nine distinct,

tractable scenarios. This systematic synthesis allows for the analysis of complex concurrent disruptions within a single mathematical design, enhancing its potential for practical networked applications.

(iv) Security-Centric Performance Index: The "security nature" of our algorithm is reflected through a mean-square boundedness criterion, which ensures system's states remain within a specific scalar bound despite adversarial signals. This framework handles system faults and disturbances through robust rejection rather than explicit diagnosis, maintaining operational stability in the face of signal corruption.

(v) Rigorous Co-Design and Stability Analysis: We derive computationally feasible LMI conditions for the co-design of observer and controller gains. Using Lyapunovâ€“Krasovskii functionals, we provide a mathematically proof of mean-square stability, offering a "safety margin" against stochastic disruptions that avoids the need for ad hoc, case-by-case testing.

(vi) Practical Validation and Real-Time Feasibility: The proposed controller is validated using a realistic example of two-area interconnected power system (TAIPS). The simulation results demonstrate that while the optimization is performed offline to handle computational complexity, the resulting fixed-gain implementation ensures minimal online demand, allowing the system to recover stability even under worst-case concurrent attacks and parameter variations.

The remainder of the paper is organized in the following format: Section 2 includes the formulation of the system model, the control scheme, and the problem formulation. The main results are detailed in Section 3. Section 4 provides an illustrative example, and the conclusions are presented in Section 5.

2. Problem formulation and the control scheme

The WNCS to be considered in this article consists of a system, the attached sensors and actuators, an observer-based controller, and a wireless network system, as shown in Figure 2. As in most wireless network systems, the network has the risk of a delay in the output signal that is transmitted from the sensors to the controller and/or a delay in the actuating signal that the control system sends to the actuators. Moreover, we are considering the occurrence of a deception attack that could affect the two communication signals, *i.e.*, the output signal and the actuating signal.

The following is an expression for the system model:

$$\begin{aligned} x(k+1) =& Ax(k) + Bu_a(k) + E_d d(k) \\ &+ E_f f(k), \\ y_s(k) =& Cx(k) \end{aligned} \tag{1}$$

where $x(k) \in \Re^{n_x}$, $u_a(k) \in \Re^{n_u}$, and $y_s(k) \in \Re^{n_y}$ are the state vector of the system, the input, and the output, respectively. $d(k) \in \Re^{n_d}$ and $f(k) \in \Re^{n_f}$ are the disturbance and the faults in the system. Also, the system matrices are A, B, E_d, E_f, and C with proper dimensions.

This paper presents a controller designed in conjunction with an observer, which estimates the unknown states of the system before applying full state control. The equations for the observer and the controller are provided, considering potential delay and deception attacks on the signal due to the use of a wireless communication network. Thus, we have:

$$\begin{cases} \hat{x}(k+1) = A\hat{x}(k) + Bu_c(k) + L(y_o(k) - \hat{y}_o(k)), \\ \hat{y}_o(k) = C\hat{x}(k), \\ u_c(k) = K\hat{x}(k). \end{cases} \tag{2}$$

where $\hat{x}(k) \in \Re^{n_x}$, $y_o(k)$, and $\hat{y}_o(k) \in \Re^{n_y}$ are the states' estimation, the output signal received by the observer, and the output of the observer, respectively. Moreover, the control signal generated by the observer-based controller is denoted by $u_c(k)$. Also, the gain of the controller is $K \in \Re^{n_u \times n_x}$ and the gain of the observer is $L \in \Re^{n_x \times n_y}$.

This article does not adopt explicit fault diagnosis or fault estimation; instead, it focuses on state estimation to facilitate full-state feedback control, as shown in Equation (2). The observer is designed to estimate unknown system states ($x(k)$), while resilience to faults is achieved through the co-design of observer and controller gains (L and K) using LMI conditions. Consequently, the system is engineered to be secured by rejecting the influence of faults as part of a broader disturbance-rejection framework, rather than utilizing a dedicated module to identify or isolate the specific nature of the faults.

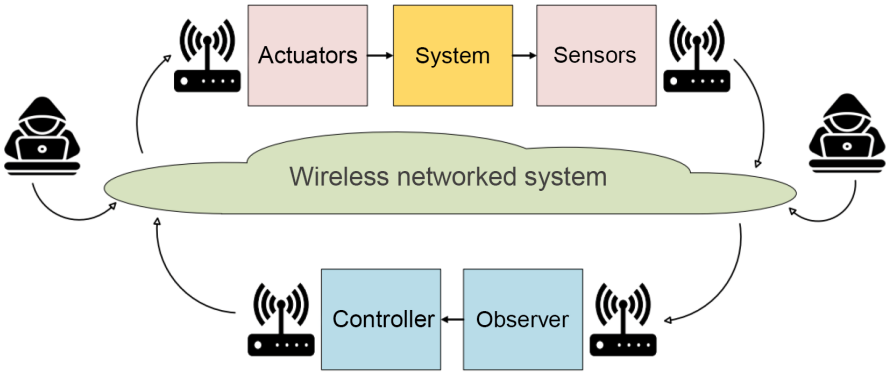

Figure 2. Model of the proposed wireless networked control

2.1. The deception attack effects

Wireless communications make the system vulnerable to cyberattacks at any node. Therefore, both the output signals and the actuating signals are affected by the deception attack. The following equation describes the output signal received by the observer:

$$\begin{aligned} y_o(k) &= \alpha_1(k)\xi_y(k) + (1-\alpha_1(k)) \\ &\big[(1-\beta_1(k))Cx(k) \\ &\quad + \beta_1(k)Cx(k-\tau_f)\big] \end{aligned} \tag{3}$$

with τ_f is the delay in the output signal and has a Bernoulli distribution white sequences $\beta_1(k)$. The deception attack's effect appears in the modified output signal $\xi_y(k)$, which has Bernoulli-distributed white sequences $\alpha_1(k)$. The attack indicator $\alpha_1(k)$ is defined as:

$$\alpha_1(k) = \begin{cases} 1, & \text{if a deception attack occurs at time } k, \\ 0, & \text{otherwise,} \end{cases}$$

with an unknown probability distribution given by $\mathbb{P}[\alpha_1(k)=1]=\rho$ and $\mathbb{P}[\alpha_1(k)=0]=1-\rho$, where $\rho \in [0,1]$ is not assumed to be known *a priori*. The proposed stability analysis and control strategy are therefore designed to ensure robustness against the uncertainty in ρ, addressing the stochastic nature of wireless communication under potential deception attacks.

The actuating signal generated by the controller is selected to be $u_c = K\hat{x}$. When this signal is transmitted from the controller to the actuator, it is affected by the time delay in the wireless control network as well as the cyber deception attack. The signal received by the actuator is described by the following equation:

$$\begin{aligned} u_a(k) &= \alpha_2(k)\xi_u(k) + (1-\alpha_2(k)) \\ &\big[(1-\beta_2(k))K\hat{x}(k) \\ &\quad + \beta_2(k)K\hat{x}(k-\tau_b)\big] \end{aligned} \tag{4}$$

where τ_b is the delay in the actuating signal and has a Bernoulli distribution white sequences $\beta_2(k)$. Also, the effect of the deception attack appears in the modified actuating signal $\xi_u(k)$, which has Bernoulli distributed white sequences $\alpha_2(k)$.

Remark 1. *Considering the purposefully designed characteristics of deception attacks, we describe the attack signal as an i.i.d. Bernoulli sequence, with the success probability defining the expected attack to occur. The signal is constrained within bounded energy limits to capture realistic behavior. This model reflects the intruder's design choices while preserving analytical tractability, as discussed in previous studies.* [27,28]

The variables τ_b and τ_f applied in this paper are considered to be varying with time and satisfy predetermined limits as follows:

$$\tau_f^{\min} \le \tau_f \le \tau_f^{\max}, \quad \tau_b^{\min} \le \tau_b \le \tau_b^{\max} \tag{5}$$

Remark 2. *In our model, we assume that when there is a deception attack, the transmitted signal will be maliciously modified and replaced with the modified version of the original signal. In the absence of cyberattacks, randomized time delay might eventually happen in the output or actuation signals, or both, due to the nature of the wireless medium. Accordingly, there are nine possible scenarios of the occurrence of the delay in the signals and the deception attacks as illustrated in Table 2; each scenario (i) has a probability ρ_i value, while $\hat{\rho}_i$ represents the expectation of it. As seen in the table, scenario 9 corresponds to the nominal situation without attacks or delays. On the other hand, scenario 1 captures the worst situation, where both the measurements and actuating signals are manipulated by attacks.*

Table 2. Scenarios of delay and deception attacks affecting the system

Scenario (i)	Attack (OS)	Delay (OS)	Attack (AS)	Delay (AS)
1	✓	-	✓	-
2	✓	-	×	✓
3	✓	-	×	×
4	×	✓	✓	-
5	×	✓	×	✓
6	×	✓	×	×
7	×	×	✓	-
8	×	×	×	✓
9	×	×	×	×

Note"-" denotes not applicable
Abbreviations: AS: Actuating signal; OS: Output signal.

2.2. Wireless networked control with deception attack

This section attempts to figure out the WNCS framework while taking into account how a deception attack might affect the transmission network. The error in estimation is calculated by defining $\epsilon(k) = x(k) - \hat{x}(k)$. Subsequently, we can articulate $x(k+1)$ and $\epsilon(k+1)$ in the following manner:

$$\begin{aligned} x(k+1) &= \big[A + (1-\alpha_2(k))(1-\beta_2(k))BK\big]x(k) \\ &- \big[(1-\alpha_2(k))(1-\beta_2(k))BK\big]\epsilon(k) + \\ &\Big[(1-\alpha_2(k))\beta_2(k)BK\Big]x(k-\tau_b) \\ &- \big[(1-\alpha_2(k))\beta_2(k)BK\big]\epsilon(k-\tau_b) + \\ &\alpha_2(k)B\xi_u(k) + E_d d(k) + E_f f(k) \end{aligned} \tag{6}$$

$$\begin{aligned} \epsilon(k+1) &= \big[(1-\alpha_2(k))(1-\beta_2(k))BK \\ &- (1-\alpha_1(k))(1-\beta_1(k))LC \\ &- BK + LC\big]x(k) - \big[(1-\alpha_2(k))(1-\beta_2(k))BK \\ &+ A + BK - LC\big]\epsilon(k) \\ &+ \big[\beta_2(k)(1-\alpha_2(k))BK\big]x(k-\tau_b) \\ &- \big[+\beta_2(k)(1-\alpha_2(k))BK\big]\epsilon(k-\tau_b) \\ &+ \big[-\beta_1(k)(1-\alpha_1(k))LC\big]x(k-\tau_f) \\ &+ \alpha_2 B\xi_u(k) - \alpha_1 L\xi_y(k) \\ &+ E_d d(k) + E_f f(k) \end{aligned} \tag{7}$$

Suppose that $\zeta(k) = [x^T(k) \quad \epsilon^T(k)]^T$, combining Equations (6) and (7), we deduce:

$$\begin{aligned} \zeta_j(k+1) = \mathcal{A}_j\zeta(k) + \mathcal{B}_j\zeta(k-\tau_f) \\ +\mathcal{C}_j\zeta(k-\tau_b) \\ +\mathcal{E}_j\xi_{uy}(k) + \mathcal{D}_j d(k) + \mathcal{F}_j f(k), \\ j = 1, \cdots, 9 \end{aligned} \tag{8}$$

using $\xi_{uy}(k) = [\xi_u(k) \quad \xi_y(k))]^T$, and $j = 1, \cdots, 9\}$, where j serves as an index denoting each scenario within the system, with the subsequent contents:

$$\mathcal{A}_j = \begin{cases} \begin{bmatrix} A & 0 \\ LC - BK & A + BK - LC \end{bmatrix} & \text{for } j = 1, 2, 4, 5 \\ \begin{bmatrix} A + BK & -BK \\ LC & A - LC \end{bmatrix} & \text{for } j = 3, 6 \\ \begin{bmatrix} A & 0 \\ -BK & A + BK - LC \end{bmatrix} & \text{for } j = 7, 8 \\ \begin{bmatrix} A + BK & BK \\ 0 & A - LC \end{bmatrix} & \text{for } j = 9 \end{cases}$$

$$\mathcal{B}_j = \begin{cases} \begin{bmatrix} 0 & 0 \\ -LC & 0 \end{bmatrix} & \text{for } j = 4, 5, 6 \\ \mathbf{0} & \text{for others} \end{cases},$$

$$\mathcal{C}_j = \begin{cases} \begin{bmatrix} BK & -BK \\ BK & -BK \end{bmatrix} & \text{for } j = 2, 5, 8 \\ \mathbf{0} & \text{for others} \end{cases}$$

$$\mathcal{E}_j = \begin{cases} \begin{bmatrix} B & 0 \\ B & -L \end{bmatrix} & \text{for } j = 1 \\ \begin{bmatrix} 0 & 0 \\ 0 & -L \end{bmatrix} & \text{for } j = 2, 3 \\ \begin{bmatrix} B & 0 \\ B & 0 \end{bmatrix} & \text{for } j = 4, 7 \\ \mathbf{0} & \text{for others} \end{cases},$$

$$\mathcal{D}_j = \begin{bmatrix} E_d \\ E_d \end{bmatrix}; \qquad \mathcal{F}_j = \begin{bmatrix} E_f \\ E_f \end{bmatrix}$$

Remark 3. *The left-hand side of Equation (8), $\zeta_j(k+1)$, describes the dynamic update of the system state under one of the nine potential cases. Each case relates to a specific set of coefficient matrices associated with delays and deception attacks, as outlined in Table 2. Conversely, the right-hand side $\zeta(k)$ indicates the extended model state representation, expressed as $[x^T(k); \epsilon^T(k)]^T$, which incorporates both the plant states and the estimation error.*

Remark 4. *The false information injected by the attacker is assumed to be state-independent arbitrary bounded energy signals and to satisfy the*

following condition: [27,28]

$$\xi_{uy}^T \xi_{uy} < \varrho_2^2 \tag{9}$$

This assumption prevents arbitrarily fast variations in the injected signal and ensures that the attack behavior remains physically plausible within the communication network.

Also, a restriction is imposed on the frequency of deception attacks to guarantee that the system retains sufficient attack-free intervals for corrective control actions. This restriction is consistent with existing studies on secure control of networked systems and is necessary for establishing stability in the presence of stochastic or adversarial events.

Definition 1. *System (8) is defined as* $\varrho_1, \varrho_2, \varrho_3, \varrho_4, \varrho_5$, *secure for known scalars* $\varrho_1, \varrho_2, \varrho_3 > 0, \varrho_4 > 0, \varrho_5 > 0$; *if* $\epsilon^T(k)\epsilon(k) \leq \varrho_1^2$, $\xi_{uy}^T \xi_{uy} < \varrho_2^2$, $d^T(k)d(k) < \varrho_3^2$, *and* $f^T(k)f(k) < \varrho_4^2$, *the evolution of the considered system's dynamics is bounded by* $\mathbb{E}\|\zeta(k)\|^2 \leq \varrho_5^2, \forall k$ *in the mean square's sense.*

The security nature of the proposed scheme is fundamentally reflected in its performance index through a mean-square boundedness criteria, as formally established in Definition 1. Rather than utilizing a traditional cost function focused solely on error minimization, the algorithm defines "security" as the ability to maintain the system's state ($\mathbb{E}\|\zeta(k)\|^2$) within a specific scalar bound. This bound must hold even in the presence of defined levels of measurement error, stochastic deception signals, disturbances, and faults, effectively making the performance index a measure of stochastic resilience across nine different adversarial scenarios.

In summary, the system's dynamics are modeled as linear time-invariant and subject to bounded disturbances. Time delays and deception attacks occurring in wireless networks are represented as independent Bernoulli processes with established probability distributions within practical operational ranges. To reflect realistic scenarios, the attack's dwell time and inter-arrival time are constrained within defined intervals to represent actual responses. Furthermore, it is assumed that the observer has complete knowledge of system dynamics and is capable of estimating unidentified states.

The proposed controller is designed to maintain stability under varying network conditions, as demonstrated in this section. While this study focuses on deception attacks in a fixed topology, the theoretical framework can be extended to mobile nodes and dynamic topologies. Future work will explicitly address scenarios including unmanned aerial vehicle networks and mobile WNCSs to validate resilience under mobility and time-varying connectivity.

3. Results

We aim to develop a controller formulated in Equation (2) ensuring the networked process Equation (8), operating under wireless network communication, is maintained secure concerning $\varrho_1, \varrho_2, \varrho_3, \varrho_4, \varrho_5$, as stated in Definition 1. We used ρ_j and $\mathbb{E}[\rho_j]$ for denoting each probability and its expected value, respectively, with $j = 1, \cdots, 9$.

The Lyapunov function presented below was utilized for establishing the main theorems:

$$V(\zeta(k)) = \sum_{i=1}^{5} V_i(\zeta(k)) \tag{10}$$

with

$$V_1(\zeta(k)) = \sum_{j=1}^{9} \zeta^T(k) P \zeta(k),\ P > 0 \tag{11}$$

$$V_2(\zeta(k)) = \sum_{j=1}^{9} \sum_{i=k-d_f}^{k-1} \zeta^T(i) Q_j \zeta(i),\ Q_j = Q_j^T > 0$$

$$V_3(\zeta(k)) = \sum_{j=1}^{9} \sum_{i=k-d_b}^{k-1} \zeta^T(i) Q_j \zeta(i)$$

$$V_4(\zeta(k)) = \sum_{j=1}^{9} \sum_{l=-d_f^{\max}+2}^{-d_f^{\min}+1} \sum_{i=k+l-1}^{k-1} \zeta^T(i) Q_j \zeta(i) \tag{12}$$

$$V_5(\zeta(k)) = \sum_{j=1}^{9} \sum_{l=-d_b^{\max}+2}^{-d_b^{\min}+1} \sum_{i=k+l-1}^{k-1} \zeta^T(i) Q_j \zeta(i) \tag{13}$$

The presented controller synthesis utilizes the expected values of attack probabilities. This approach remains robustly significant within the proposed mean-square stability framework. By designing the controller based on expected values ($\hat{\rho}_j$), we established a mathematically rigorous foundation for ensuring stochastic security despite the random nature of Bernoulli-distributed deception attacks. Furthermore, the implementation of the Lyapunov functional approach provides a necessary safety margin, allowing the system to maintain stability even when the actual operational attack frequency deviates from the estimated expectations used during the design phase.

Remark 5. *The chosen Lyapunov function Equation (10) provides rigorous stability guarantees under deception attacks that stochastic characteristics within the framework, offering a unified and adaptable tool for analyzing WNCSs subject to uncertainties. Also, the Lyapunov methods allow the treatment of cyberattacks in a single mathematical framework, avoiding the need for case-by-case ad hoc stability tests. However, this approach may involve significant computational complexity and potential conservatism in stability conditions, which is left for future work.*

Theorem 1. *For the scalars $\varrho_1, \varrho_2, \varrho_3, \varrho_4, \varrho_5 > 0$ and for a given observer-based controller as formulated in Equation (2) and has gains K and L for the controller and observer, respectively, the system Equation (8) is $\varrho_1, \varrho_2, \varrho_3, \varrho_4, \varrho_5$ secure if there are matrices P, $R_j^T = Q_j$, $S_j^T = S_j > 0$, $j = 1, \cdots, 9$ and scalars $\varsigma_1 > 0$ and $\varsigma_2 > 0$ that satisfys the LMI given below:*

$$\begin{cases} \Upsilon_j < 0 \\ \frac{\theta^2 q_0^2}{eig_{min}(P)(q_0-1)} \leq \varrho_3^2 \end{cases} \tag{14}$$

where

$$\begin{aligned}
\Upsilon_j &= \begin{bmatrix} \Upsilon_{11j} & \Upsilon_{12j} & \Upsilon_{13j} & \Upsilon_{14j} & \Upsilon_{15j} & \Upsilon_{16j} \\ \bullet & \Upsilon_{22j} & \Upsilon_{23j} & \Upsilon_{24j} & \Upsilon_{25j} & \Upsilon_{26j} \\ \bullet & \bullet & \Upsilon_{33j} & \Upsilon_{34j} & \Upsilon_{35j} & \Upsilon_{36j} \\ \bullet & \bullet & \bullet & \Upsilon_{44j} & \Upsilon_{45j} & \Upsilon_{46j} \\ \bullet & \bullet & \bullet & \bullet & \Upsilon_{55j} & \Upsilon_{56j} \\ \bullet & \bullet & \bullet & \bullet & \bullet & \Upsilon_{66j} \end{bmatrix} \\
\Upsilon_{11j} &= \hat{\rho}_j \left[\mathcal{A}_j^T P \mathcal{A}_j - P + 2Q_j + (\Delta\tau_f + \Delta\tau_b) Q_j\right], \ \Upsilon_{12j} = \mathcal{A}_j^T \hat{\rho}_j P \mathcal{B}_j, \\
\Upsilon_{13j} &= \mathcal{A}_j^T \hat{\rho}_j P \mathcal{C}_j, \ \Upsilon_{14j} = \mathcal{A}_j^T \hat{\rho}_j P \mathcal{E}_j, \ \Upsilon_{15j} = \mathcal{A}_j^T \hat{\rho}_j P \mathcal{D}_j, \\
\Upsilon_{16j} &= \mathcal{A}_j^T \hat{\rho}_j P \mathcal{F}_j, \ \Upsilon_{22j} = \mathcal{B}_j^T \hat{\rho}_j P \mathcal{B}_j - \hat{\rho}_j Q_j, \ \Upsilon_{23j} = \mathcal{B}_j^T \hat{\rho}_j P \mathcal{C}_j \\
\Upsilon_{24j} &= \mathcal{B}_j^T \hat{\rho}_j P \mathcal{E}_j, \ \Upsilon_{25j} = \mathcal{B}_j^T \hat{\rho}_j P \mathcal{D}_j, \ \Upsilon_{26j} = \mathcal{B}_j^T \hat{\rho}_j P \mathcal{F}_j, \\
\Upsilon_{33j} &= \mathcal{C}_j^T \hat{\rho}_j P \mathcal{C}_j - \hat{\rho}_j Q_j \ \ \Upsilon_{34j} = \mathcal{C}_j^T \hat{\rho}_j P \mathcal{E}_j, \ \Upsilon_{35j} = \mathcal{C}_j^T \hat{\rho}_j P \mathcal{D}_j, \\
\Upsilon_{36j} &= \mathcal{C}_j^T \hat{\rho}_j P \mathcal{F}_j, \ \Upsilon_{44j} = \mathcal{E}_j^T \hat{\rho}_j P \mathcal{E}_j - \varsigma_1 I, \ \Upsilon_{45j} = \mathcal{E}_j^T \hat{\rho}_j P \mathcal{D}_j, \\
\Upsilon_{46j} &= \mathcal{E}_j^T \hat{\rho}_j P \mathcal{F}_j, \ \Upsilon_{55j} = \mathcal{D}_j^T \hat{\rho}_j P \mathcal{D}_j - \varsigma_2 I, \ \Upsilon_{56j} = \mathcal{D}_j^T \hat{\rho}_j P \mathcal{F}_j, \\
\Upsilon_{66j} &= \mathcal{F}_j^T \hat{\rho}_j P \mathcal{F}_j - \varsigma_3 I,
\end{aligned} \tag{15}$$

with $\theta^2 = \varsigma_1 \varrho_1^2 + \varsigma_2 \varrho_2^2 + \varsigma_3 \varrho_3^2$

See Appendix A1 for the detailed proof of Theorem 1.

Remark 6. *The transmitted signal through a wireless network communication changes with a certain boundary as a result of the deception attacks. The scalars $\hat{\rho}_j, j = 1, \cdots, 9$ in Theorems 1 are computed by selecting related numbers by calling random generators. Then, they are used to calculate the states and the error trajectories. [29] Other methods in the literature do not have this feature for securing WNCSs.*

Theorem 2. *For the provided scalars $\varrho_1, \varrho_2, \varrho_3, \varrho_4, \varrho_5 > 0$, a delay bounds $\tau_f^{\max}$, $\tau_f^{\min}$, $\tau_b^{\max}$, $\tau_b^{\min}$ and $\hat{\rho}_j$, $j = 1, .., 9$, matrices X, $\mathcal{Y}$, $\mathcal{Z}$, $\zeta > 0$, $j = 1, .., 9$, and scalars $\varsigma_1, \varsigma_2, \varsigma_3 > 0$. The overall system Equation (8) is $\varrho_1, \varrho_2, \varrho_3, \varrho_4, \varrho_5$ secure if there exist a controller with gain K and observer with gain L together have a control scheme as Equation (2) and satisfy the LMI given by:*

$$\left\{ \Omega \leq 0 \quad and \ \frac{\theta^2 q_0^2}{eig_{min}(P)(q_0-1)} \leq \varrho_3^2 \right. \tag{16}$$

where:

$$\Omega = \begin{bmatrix} \hat{\rho}_j \hat{X} + \hat{\phi}_j & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \\ \bullet & -\hat{\rho}_j Q_j & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \\ \bullet & \bullet & -\hat{\rho}_j Q_j & \mathbf{0} & \mathbf{0} & \mathbf{0} & \hat{\Theta}_j \\ \bullet & \bullet & \bullet & \varsigma_1 I & \mathbf{0} & \mathbf{0} & \\ \bullet & \bullet & \bullet & \bullet & -\varsigma_2 I & \mathbf{0} & \\ \bullet & \bullet & \bullet & \bullet & \bullet & -\varsigma_3 I & \\ & & & \bullet & & & -\hat{\rho}_j \hat{X} \end{bmatrix} \tag{17}$$

with

$$\widehat{X} = \begin{bmatrix} X & 0 \\ 0 & X \end{bmatrix}, \tag{18}$$

$$\hat{\phi}_j = 2\hat{\rho}_j \mathcal{M}_j + \hat{\rho}_j(\Delta\tau_b + \Delta\tau_f)\mathcal{M}_j \tag{19}$$

$$\hat{\Theta}_j = \begin{bmatrix} \hat{\mathcal{A}}_j^T & \mathcal{B}_j^T & \mathcal{C}_j^T & \mathcal{E}_j^T & \mathcal{D}_j^T & \mathcal{F}_j^T \end{bmatrix}^T \tag{20}$$

$$\hat{\mathcal{A}}_j^T = \begin{cases} \begin{bmatrix} XA^T & 0 \\ Z^T - Y^T B^T & XA^T + YB^T - Z^T \end{bmatrix}, & j = 1,2,4,5 \\ \begin{bmatrix} XA^T + Y^T B^T & -Y^T B^T \\ Z^T & XA^T - Z^T \end{bmatrix}, & j = 3,6 \\ \begin{bmatrix} XA^T & 0 \\ Y^T B^T & XA^T + Y^T B^T - Z^T \end{bmatrix}, & j = 7,8 \\ \begin{bmatrix} XA^T + Y^T B^T & Y^T B^T \\ 0 & XA^T - Z^T \end{bmatrix}, & j = 9 \end{cases}$$

Moreover, gain $K = YX^{-1}$ *and gain* $L = ZX^{-1}C^{\dagger}$.

Proof. Select Θ_j to be:

$$\Theta_j = \begin{bmatrix} \mathcal{A}_j & \mathcal{B}_j & \mathcal{C}_j & \mathcal{E}_j & \mathcal{D}_j & \mathcal{F}_j \end{bmatrix}^T$$

In this case, Equation (15) is rewritten in the following expressions:

$$\Upsilon_j = \widetilde{\Upsilon}_j + \hat{\rho}_j \Theta_j P \Theta_j^T < 0 \tag{21}$$

$$\widetilde{\Upsilon}_j = \text{diag}\{-\hat{\rho}_j P + \phi_1, -\hat{\rho}_j Q_j, -\hat{\rho}_j Q_j, -\varsigma_1 I, -\varsigma_2 I, -\varsigma_3 I\} \tag{22}$$

where $\phi_1 = 2\hat{\rho}_j Q_j + \hat{\rho}_j(\Delta_f + \Delta_b)Q_j$. Now, define P^{-1} as $\hat{X}$ and by applying Schur complements, Υ_j in Equation (21) is rewritten in the following form:

$$\begin{bmatrix} \widetilde{\Upsilon}_j & \Theta_j \\ \bullet & -\hat{\rho}_j \hat{X} \end{bmatrix} < 0 \tag{23}$$

Multiply matrix inequality Equation (22) by $diag[\hat{X}, I, I, I, I, I, I]$ from right and left and by implementing Equation (18) $\mathcal{M}_j = \hat{X} Q_j \hat{X}$, and matrix inequality Equation (17) subject Equation (20) is obtained.

The proposed framework provides rigorous theoretical guarantees and is particularly effective for offline control design. Nevertheless, its practical implementation may be constrained by substantial computational demands and difficulties in integrating with existing communication and control infrastructures.

Remark 7. *Theorem 2 outlines the methodology to design a* $\varrho_1, \varrho_2, \varrho_3, \varrho_4, \varrho_5$ *secure observer-based controller Equation (2) that has gained* K *and* L *for a discrete-time WNCS Equation (1) that has an overall description in Equation (8) while considering the occurrences of deception attacks on both measurements and actuating signals.*

The proposed controller in this article functions as a regulatory framework designed to guarantee mean-square stability across a comprehensive spectrum of adversarial conditions. Rather than being validated against a single, static interference type, the system is engineered using a mathematical foundation that accounts for nine distinct scenarios involving concurrent delays and deception attacks. This ensures that the networked system maintains operational security and performance even when the specific timing and frequency of stochastic disruptions remain unpredictable.

Remark 8. *The previous discussion highlights that this paper primarily focuses on linear plants in the simplified form of Equation (1). Nevertheless, the proposed approach is not limited to linear systems. It can also be applied to nonlinear systems that are linearized into this form, thereby covering*

a wide range of practical applications, including a TAIPS, as detailed in ***Section 4****. Furthermore, all theorems and stability conditions derived in this paper remain valid for nonlinear systems that are expressed in this form.*

$$f(x(k)) = Ax(k) + Bu(k) + N(x,u) \tag{24}$$

where $N(x,u)$ *is a nonlinear function satisfying a specific boundary condition. The extension of this method to other forms of nonlinear systems is left for future research.*

4. Illustrative example: Two-area interconnected power system

The observer-based control scheme is comparatively straightforward to implement with conventional state feedback and estimation methods, thereby minimizing the computing burden. The methodology is extremely flexible, capable of addressing stochastic deception threats and fluctuating delays in parallel, making it appropriate for practical WNCSs. The research example investigating a TAIPS illustrates that the technique efficiently maintains stability against extreme attack scenarios with minimal adjustment, showing resilience and practical utility.

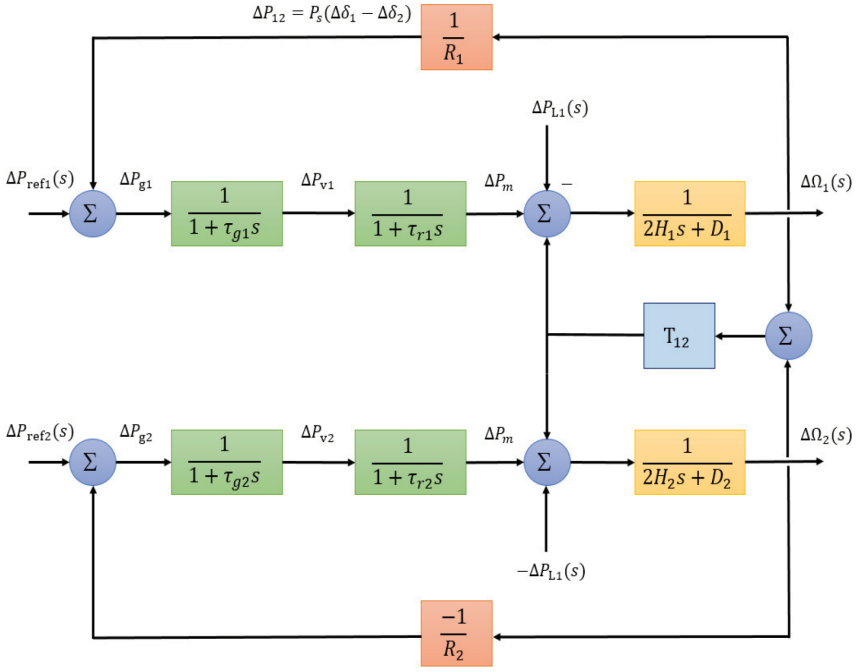

Figure 3. A block model of a two-area interconnected power system

A demonstration of TAIPS is implemented in this section to verify the usefulness of the presented control scheme, as illustrated in Figure 3.

In a TAIPS, frequency control is achieved through primary and supplementary speed control. [29] Primary speed control provides an initial coarse frequency adjustment, enabling generators within a control area to respond to load variations and share them proportionally to the capacity of each one. The response speed is primarily bounded by the inherent delays of time in both the system and the turbine, typically ranging from 2 to 20 seconds, depending on the turbine type. Once the primary control stabilizes the system, supplementary speed control refines the frequency adjustment by eliminating any remaining frequency error through integral action. The supplementary control operates at a slower pace, engaging only after the primary control has taken effect, with response times typically around one minute. [29]

An unregulated, a TAIPS is depicted in Figure 3. Here, f represents the frequency of the system (Hz), R_i denotes the regulation coefficient (Hz/pu), T_g, T_t, and T_p are the time constants of the governor, the turbine, and the power system, respectively. The depicted system could be formulated

in the form of Equation (1) and has the following states and input matrices:

$$\begin{aligned} x &= \left[\Delta p_{tie}(t); \Delta f_1(t); \Delta p_{g1}(t); \Delta x_{v1}(t); \Delta f_2(t); \Delta p_{g2}(t); \Delta x_{v2}(t)\right]; \\ U &= \left[\Delta p_{c1}(t); \Delta p_{c2}(t)\right] \end{aligned} \tag{25}$$

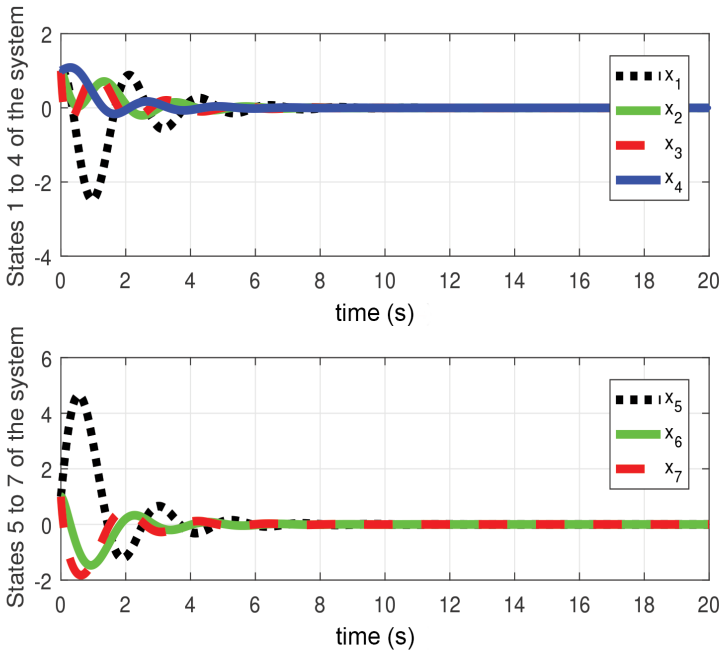

Figure 4. States of the two-area interconnected power system without any attack

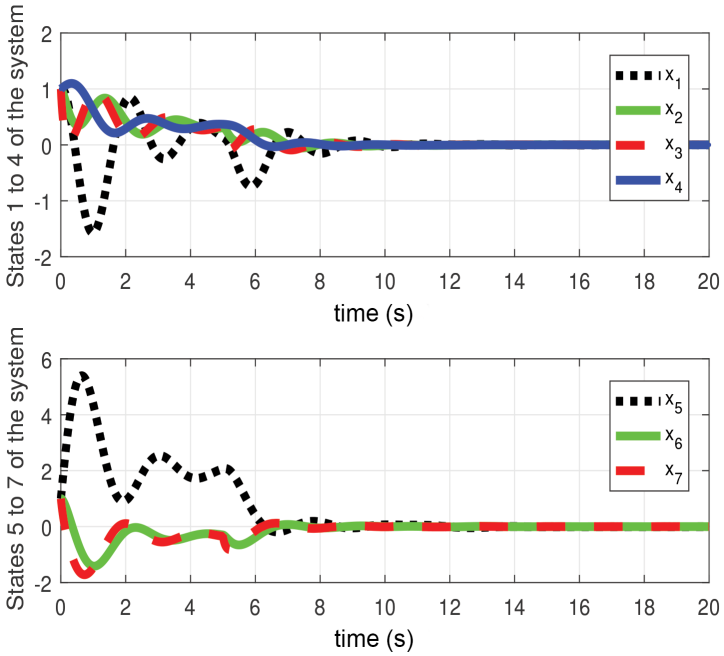

Figure 5. States of the two-area interconnected power system affected by deception attacks in the forward path

Now, by utilizing the parameters, one can get the system matrices shown in Equation (26): [25]

$$
\begin{aligned}
A &= \begin{bmatrix}
1.0003 & 0.0590 & 0.0009 & -0.0600 & 0 & 0 & 0 \\
-0.0008 & 0.9672 & 0.0308 & 0 & -0.0001 & 0 & \\
-0.0490 & -0.0015 & 0.8825 & 0.0013 & -0.0051 & -0.0002 & 0 \\
0.0055 & 0.0002 & 0 & 0.9998 & -0.0005 & 0 & 0 \\
0.0002 & 0 & 0 & 0.06 & 0.9995 & 0.0590 & 0.0009 \\
0 & 0 & 0 & 0 & -0.0008 & 0.9672 & 0.0308 \\
0 & 0 & 0 & -0.0015 & -0.0489 & -0.0015 & 0.8825
\end{bmatrix}; \\
B &= \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0.0020 & 0.1175 \\
0 & 0.0020 & 0.1175 & 0 & 0 & 0 & 0
\end{bmatrix}^T; \\
C &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}
\end{aligned} \tag{26}
$$

An observer-based controller, as in Equation (3) is implemented to achieve the stability of the system that is running on a remote station. A wireless network communication system is used for sending and receiving signals among system items. The deception attacks could affect the measurement and actuating signals, as shown in Figure 2. The observer and controller gains were determined using MATLAB (MathWorks, Inc., United States) and YALMIP based on the implementation of Theorem 2, and were obtained as follows:

$$
K = \begin{bmatrix}
-0.0068 & -0.0157 \\
-0.0035 & -0.0233 \\
0.0001 & -0.0379 \\
-0.0531 & 0.0248 \\
-0.0148 & -0.0005 \\
-0.0234 & -0.0017 \\
-0.0382 & -0.0003
\end{bmatrix}^T \qquad L = \begin{bmatrix}
0.0128 \\
-0.0027 \\
-0.0125 \\
-0.0057 \\
-0.0109 \\
0.0174 \\
0.4562
\end{bmatrix} \tag{27}
$$

It is worth mentioning that the computational cost of the method primarily depends on the size of the system matrices and the number of switching modes considered. Specifically, the computational complexity of LMI-based synthesis scales. For the TAIPS case study considered, the complete optimization process required 12.96 hours of computation time on a standard workstation (Intel Core i7, 1.3 GHz, 8 GB RAM), indicating that the method is computationally feasible for the design of the offline controller.

While we acknowledge that the offline optimization for the TAIPS case study required 12.96 hours on a standard workstation, it is critical to distinguish between design-time and run-time complexity. Because the proposed controller and observer use fixed gains (K and L) derived once during the design phase, the online computational demand remains minimal, ensuring the system can provide real-time control actions even on resource-constrained wireless nodes. This trade-off is often acceptable in critical infrastructures like power systems, where the priority is rigorous stability guarantees against concurrent attacks rather than rapid re-design cycles

Since the proposed controller is designed offline and implemented in real-time with fixed gains, the online computational demand remains minimal. Future work will investigate scalable formulations and distributed optimization techniques to further enhance computational efficiency and applicability to large interconnected systems.

The simulations are carried out on a discrete-time linear WNCS model with specified parameter values and controller gains satisfying the Lyapunov-based stability conditions. Attack scenarios include bounded deception signals injected into communication channels. Randomness is introduced through random realizations based on the specified distributions of attack sequences.

The simulation environment was implemented in MATLAB/Simulink, where the attack processes were modeled through the switching variables $\alpha_1(k)$, $\alpha_2(k)$, $\beta_1(k)$, and $\beta_2(k)$, each generated as Bernoulli-distributed sequences with probabilities specified in Table 2. To capture a comprehensive range of conditions in WNCSs, four representative attack scenarios were considered, and the corresponding system state responses were obtained through MATLAB/Simulink simulations.

Figure 4 illustrates the system's performance in the absence of deception attacks, demonstrating stable operation with well-regulated frequency and power deviations. The system maintained its dynamic response within acceptable limits, ensuring effective coordination among interconnected areas. This scenario serves as a benchmark for evaluating the impact of deception attacks on system stability.

Figure 5 shows the effect of a deception attack targeting measurement signals, where incorrect data were fed into the control system, leading

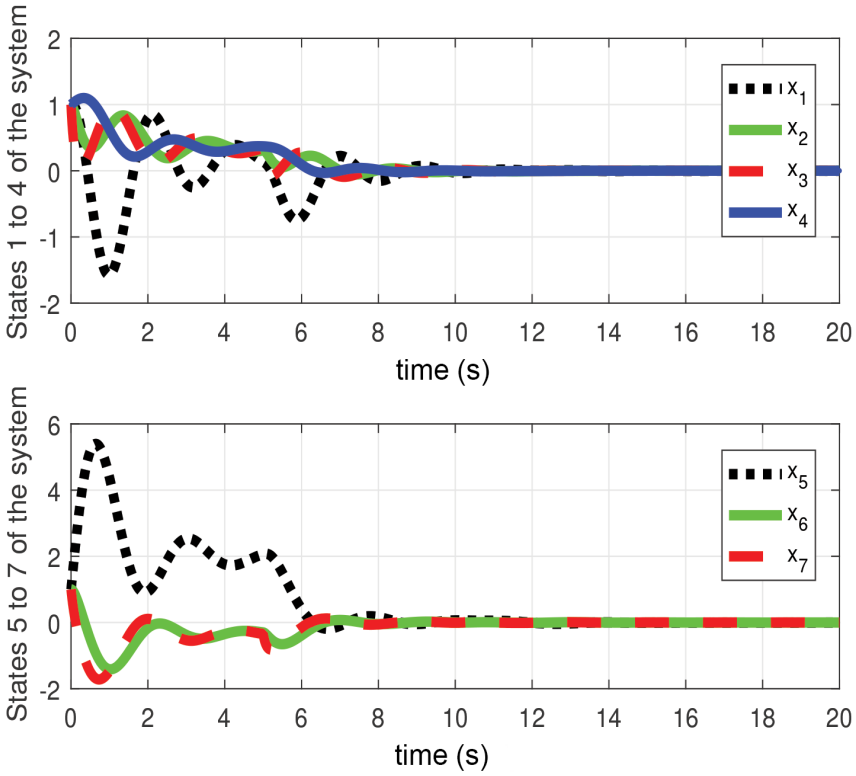

Figure 6. States of the two-area interconnected power system with the actuating signals subjected to deception attacks

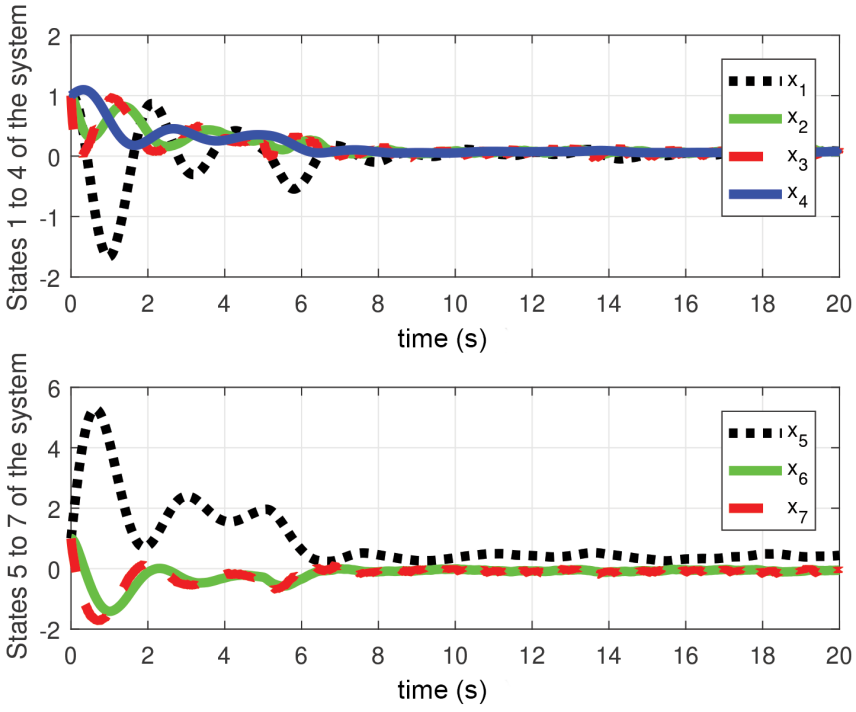

Figure 7. States of the two-area interconnected power system affected by deception attacks in both signals

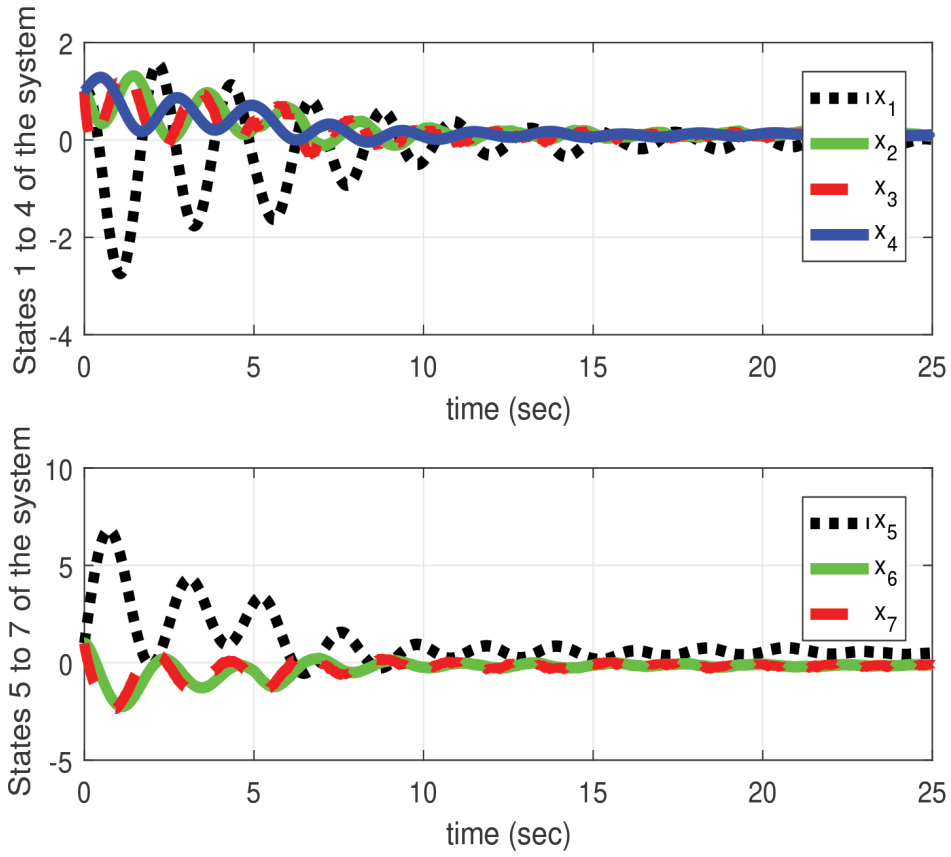

Figure 8. Two-area interconnected power system states with deception attacks in both signals with variations in matrix A

to deviations in frequency and power. The response was degraded, exhibiting oscillations and delayed settling times due to the corrupted measurements influencing the control actions. However, the system maintained stability within a reasonable time.

Figure 6 presents the system's behavior under a deception attack affecting actuating signals, where control commands sent to actuators were manipulated. This resulted in a more pronounced disturbance compared to Figure 4, as incorrect actuation disrupts the system's ability to regulate power flow effectively.

Figure 7 shows the worst-case scenario, where deception attacks compromised both measurement and actuating signals. The system exhibited large frequency oscillations and poor damping characteristics. But even in this worst-case scenario, the designed observer-based controller succeeded in bringing the system back to stability.

Finally, the worse-case scenario was repeated with a 0.5% modification applied to the system matrix A. As illustrated in Figure 8, the system still achieved stability, though with a longer settling time. It is also important to note that a promising future direction is to investigate the system's robustness under different variations and to refine the controller design accordingly.

Remark 9. *Although we demonstrate the framework using a power system example, it is directly applicable to a wide variety of WNCSs that either have a linear form or can be transformed into the form in Equation (1), such as intelligent transportation systems, smart grids, and IoT-enabled healthcare systems. Its foundation on state-space modeling and stability analysis makes it adaptable to different domains where stochastic deception attacks compromise communication. Nonetheless, the expansion of this methodology to nonlinear dynamics and the assurance of scalability in extensive networks are critical avenues for future investigation. Future reserach can could focus on extending the approach through hierarchical or distributed control strategies to ensure feasibility in industrial IoT and smart grid applications.*

As demonstrated in this section, the proposed method was validated on a TAIPS under various attack scenarios. Unlike previous studies, the proposed approach successfully addresses all possible

cases of delays and deception attacks. Furthermore, it demonstrates the controller's capability to restore system stability even under worst-case conditions.

While the proposed method demonstrates strong performance, it is limited by its focus on linear system models. The computational complexity of the proposed approach may also hinder its use in large-scale or real-time systems. Future work will aim to extend the method to nonlinear and time-varying systems. Extending the approach to nonlinear systems through nonlinear input-to-state stability Lyapunov functions, sum-of-squares or dissipativity methods, or hybrid Lyapunov techniques may enhance its robustness. Moreover, incorporating nonlinear observers, adaptive learning layers, and distributed verification can improve scalability and enable broader use in real-world nonlinear WNCSs.

5. Conclusions

A WNCS is a feedback control architecture that exchanges signals among distributed nodes via wireless channels. Stated differently, the WNCS's controller interacts with sensors and actuators wirelessly. This paper examined the risk of cyber-attacks on WNCSs, potentially resulting in instability and system failure. We proposed a control method for a class of WNCS subject to deception attacks, where deception attacks were modeled as stochastic processes with variable conditional probabilities and affect both the measurement and actuating signals. Consequently, the presented control mechanism is better suited for real-world applications that may involve multiple methods from concurrent adversaries. This formulation incorporates a comprehensive set of deception-attack scenarios, such as the time delays, disturbances, and faults that occur in the signals. The proposed control scheme is developed to tackle different deception-attack scenarios that could affect the system, especially wireless delay, and disturbance. Finally, a case study of a TAIPS was used to assess the effectiveness of the new controller. A realistic model was used to consider the simple and worst scenarios of the deception attack and prove the presented scheme's validity. The proposed method successfully preserved the stability of the selected system in the nominal situation and in the case of cyber deception attacks.

The present study concentrates on deception attacks in order to develop a rigorous theoretical basis and to validate the effectiveness of the proposed approach. Future research will aim to examine the robustness of the framework in the presence of hybrid and adaptive attack scenarios, as well as to extend the controller design to enhance resilience against multiple concurrent threats, particularly under resource-constrained operating conditions.

Acknowledgments

None.

Funding

None.

Conflict of interest

The authors declare they have no competing interests.

Author contributions

Conceptualization: Mutaz M. Hamdan
Formal analysis: Nezar M. Alyazidi
Investigation: Nezar M. Alyazidi
Methodology: Mutaz M. Hamdan
Writing–original draft: Mutaz M. Hamdan
Writing–review & editing: Nezar M. Alyazidi

Availability of data

Not applicable.

AI tools statement

All authors confirm that no AI tools were used in the preparation of this manuscript.

References

1. Aljubouri MA, Iskandarani MZ. Comparative analysis of coding schemes for effective wireless communication. *Indones J Electr Eng Comput Sci.* 2024;34(2):926–940. https://doi.org/10.11591/ijeecs.v34.i2.pp926-940
2. Qasem N. Measurement and simulation for improving indoor wireless communication system performance at 2.4 ghz by modifying the environment. *IEEE Access.* 2024. https://doi.org/10.1109/ACCESS.2024.3426490
3. Hamdan MM, Mahmoud MM. Analysis and challenges in wireless networked control system: A survey. *Int J Robot Control Syst.* 2022;2(3):492–522. https://doi.org/10.31763/ijrcs.v2i3.731
4. Park P, Ergen SC, Fischione C, Lu C, Johansson KH. Wireless network design for control systems: A survey. *IEEE Commun Surv Tutor.* 2017;20(2):978–1013. https://doi.org/10.1109/COMST.2017.2780114
5. Bello O, Zeadally S. Intelligent device-to-device communication in the internet of things. *IEEE Syst J.* 2014;10(3):1172–1182. https://doi.org/10.1109/JSYST.2014.2298837

6. Lu X, Li J. Improving stability and performance in iot-driven networked control systems. *Comput Electr Eng.* 2024;119:109537. https://doi.org/10.1016/j.compeleceng.2024.109537
7. Aslam MM, Li W, Liu W, Qi Y, Saleem U, Riaz S. A review of integrated modeling and simulation of control and communication systems in smart grid. *Comput Electr Eng.* 2024;119:109553. https://doi.org/10.1016/j.compeleceng.2024.109553
8. Al-Dabbagh AW. Design of a wireless control system with unreliable nodes and communication links. *IEEE Trans Cybern.* 2017;49(1):315–327. https://doi.org/10.1109/TCYB.2017.2772869.25
9. Majid M, Habib S, Javed AR, Rizwan M, Srivastava G, Gadekallu TR, Lin JC-W. Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. *Sensors.* 2022;22(6):2087. https://doi.org/10.3390/s22062087
10. Wang Y, Wu S, Lei C, Jiao J, Zhang Q. A review on wireless networked control system: The communication perspective. *IEEE Internet Things J.* 2023. https://doi.org/10.1109/JIOT.2023.3342032
11. Ma Y, Guo J, Wang Y, Chakrabarty A, Ahn H, Orlik P, Guan X, Lu C. Optimal dynamic transmission scheduling for wireless networked control systems. *IEEE Trans Control Syst Technol.* 2022;30(6):2360–2376. https://doi.org/10.1109/TCST.2022.3141581
12. Alzubi OA. A deep learning-based frechet and dirichlet model for intrusion detection in iwsn. *J Intell Fuzzy Syst.* 2022;42(2):873–883. https://doi.org/10.3233/JIFS-189756
13. Alzubi OA, Alzubi JA, Alazab M, Alrabea A, Awajan A, Qiqieh I. Optimized machine learning-based intrusion detection system for fog and edge computing environment. *Electronics.* 2022;11(19):3007. https://doi.org/10.3390/electronics11193007
14. Yuan Y, Yuan H, Ho DW, Guo L. Resilient control of wireless networked control system under denial-of-service attacks: A cross-layer design approach. *IEEE Trans Cybern.* 2018;50(1):48–60. https://doi.org/10.1109/TCYB.2018.2863689
15. Liu Z, Li Y, Li L, Ma K, Yang Y. On the security and stability for wireless networked control systems with external attack and disturbances. *Int J Robust Nonlinear Control.* 2022. https://doi.org/10.1002/rnc.6260
16. Cetinkaya A, Ishii H, Hayakawa T. Effects of jamming attacks on wireless networked control systems under disturbance. *IEEE Trans Autom Control.* 2022;68(2):1223–1230. https://doi.org/10.1109/TAC.2022.3153275
17. Alyazidi NM, Mahmoud MS. L1 adaptive networked controller for islanded distributed generation systems in a microgrid. *Int J Syst Sci.* 2018;49(12):2507–2524. https://doi.org/10.1080/00207721.2018.1487093
18. Al-Yazidi NM, Al-Wajih YA, Mahmoud MS. Iterative learning control for load frequency in cyber-attacked multi-area power systems. *IEEE Access.* 2023. https://doi.org/10.1109/ACCESS.2023.3309150.26
19. Xu Z, Yang X, Li X, Lu J. Input-to-state stability of switched network control systems under unknown deception attacks. *IEEE Trans Cybern* 2024. https://doi.org/10.1109/TCYB.2024.3376695
20. Shi H, Zhang Y. hinfty control for networked control systems with packet loss and deception attack. in: *2024 39th Youth Academic Annual Conference of Chinese Association of Automation (YAC)*, IEEE, 2024, pp. 579–584. https://doi.org/10.1109/YAC63405.2024.10598802
21. Devanathan B, Selvaraj P, Suyampulingam A. Finite-time control for iot-enabled microgrids using distributed state estimation under deception attack. in: *2024 IEEE 21st India Council International Conference (INDICON)*, 2024, pp. 1–5. https://doi.org/10.1109/INDICON63790.2024.10958434
22. Li F, Li K, Peng C, Gao L. Dynamic event-triggered fuzzy control of dc microgrids under fdi attacks and imperfect premise matching. *Int J Electr Power Energy Syst.* 2023;147:108890. https://doi.org/10.1016/j.ijepes.2022.108890
23. Li F, Li K, Peng C, Gao L. Dynamic event-triggered fuzzy non-fragile control of dc microgrids. *ISA Trans.* 2023;142:83–97. https://doi.org/10.1016/j.isatra.2023.07.012
24. Meng Q, Kasis A, Yang H, Polycarpou MM. Secure state estimation of networked switched systems under denial-of-service attacks. *Eur J Control.* 2024:101037. https://doi.org/10.1016/j.ejcon.2024.101037
25. Abdelkader S, Amissah J, Kinga S, Mugerwa G, Emmanuel E, Mansour D-EA, Bajaj M, Blazek V, Prokop L. Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. *Results Eng.* 2024:102647. https://doi.org/10.1016/j.rineng.2024.102647
26. Huang Y, Huang L, Zhu Q. Reinforcement learning for feedback-enabled cyber resilience. *Annu Rev Control.* 2022;53:273–295. https://doi.org/10.1016/j.arcontrol.2022.01.001
27. Ding D, Wang Z, Q.-Han L, Wei G. Security control for discrete-time stochastic nonlinear systems subject to deception attacks. *IEEE Trans Syst Man Cybern Syst.* 2016;48(5):779–789. https://doi.org/10.1109/TSMC.2016.2616544
28. Hamdan MM, Mahmoud MS, Baroudi UA. Event-triggering control scheme for discrete time cyberphysical systems in the presence of simultaneous hybrid stochastic attacks. *ISA Trans.* 2022;122:1–12. https://doi.org/10.1016/j.isatra.2021.04.027.27

29. Mahmoud M, Selim S, Shi P, Baig M. New results on networked control systems with non-stationary packet dropouts. *IET Control Theory Appl.* 2012;6(15):2442–2452. https://doi.org/10.1049/iet-cta.2012.0487
30. Mahmoud MS, Khalid HM, Hamdan MM. *Cyberphysical infrastructures in power systems: architectures and vulnerabilities.*. Academic Press, 2021. https://doi.org/10.31763/ijrcs.v2i3.731

Mutaz M. Hamdan *is an Assistant Professor in the Faculty of Engineering at Al-Ahliyya Amman University, Jordan, where he has been serving since 2023. He earned his B.Sc. degree from Palestine Polytechnic University, Hebron, Palestine, in 2006. He received his M.Sc. and Ph.D. degrees in Systems and Control Engineering in 2012 and 2019, respectively, from the Systems Engineering Department at King Fahd University for Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia. Dr. Hamdan completed a Postdoctoral Fellowship with the Systems Engineering Department at KFUPM (2020–2021). He subsequently served as an Assistant Professor in the Mechanical Engineering Department at the National University College of Technology, Amman, Jordan (2022–2023). His research interests include secure control of cyber-physical systems, distributed control systems, and intelligent control systems. Dr. Hamdan has over ten years of academic and research experience. He has co-authored a book published by Elsevier, authored more than 19 peer-reviewed journal articles, and holds three U.S. patents. He also serves as a reviewer for several high-impact journals in the field of systems and control engineering.*
https://orcid.org/0000-0002-4516-571X

Nezar M. Alyazidi *graduated from Hadramout University of Science and Technology (HUST), Hadramout, Yemen (2006). He received his M.Sc. and Ph.D. degrees in systems and control engineering (2012, 2017) respectively from the Systems Engineering Department at King Fahd University for Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia. He worked as a Lecture-B with Systems Engineering Department at KFUPM (2013–2017). In 2013, he joined the distributed control research group at KFUPM, as a Research Fellow from 2013 to present. He worked a Postdoctoral Fellow with the Systems Engineering Department at KFUPM (2017-2018). He is currently Assistant Professor at KFUPM with Control and Instrumentation Engineering Department. He is currently Research Scholar Fellow of acting Director Interdisciplinary Research Center, Smart Mobility Logistics, KFUPM. His research interests are focused on optimal control, adaptive control, reinforcement learning, machine learning, intelligent and Optimization algorithms, distributed generation units, time delay systems, wireless communication networks and secure control systems.*
https://orcid.org/0000-0001-8977-9302

Appendix

A1. Proof of Theorem 1

The difference of $V_1(\zeta(k))$ is evaluated for the overall system equation (8) as follows:

$$\begin{aligned}
&\mathbb{E}[\Delta V_1(\zeta(k))] = \mathbb{E}[V_1(\zeta_j(k+1))] - V_1(\zeta(k)) \\
&= \sum_{j=1}^{9} \Big[\zeta^T(k) \left[\mathcal{A}_j^T \hat{\rho}_j P \mathcal{A}_j - P \right] \zeta(k) + 2\zeta^T(k) \mathcal{A}_j^T \hat{\rho}_j P \mathcal{B}_j \zeta(k-\tau_f) \\
&+ 2\zeta^T(k) \mathcal{A}_j^T \hat{\rho}_j P \mathcal{C}_j \zeta(k-\tau_b) + 2\zeta^T(k) \mathcal{A}_j^T \hat{\rho}_j P \mathcal{E}_j \xi_{uy}(k) + 2\zeta^T(k) \mathcal{A}_j^T \hat{\rho}_j P \mathcal{D}_j d(k) \\
&+ 2\zeta^T(k) \mathcal{A}_j^T \hat{\rho}_j P \mathcal{F}_j f(k) + \zeta^T(k-\tau_f)(k) \mathcal{B}_j^T \hat{\rho}_j P \mathcal{B}_j \zeta(k-\tau_f) \\
&+ 2\zeta^T(k-\tau_f)(k) \mathcal{B}_j^T \hat{\rho}_j P \mathcal{C}_j \zeta(k-\tau_b) + 2\zeta^T(k-\tau_f)(k) \mathcal{B}_j^T \hat{\rho}_j P \mathcal{E}_j \xi_{uy}(k) \\
&+ 2\zeta^T(k-\tau_f)(k) \mathcal{B}_j^T \hat{\rho}_j P \mathcal{D}_j d(k) + 2\zeta^T(k-\tau_f)(k) \mathcal{B}_j^T \hat{\rho}_j P \mathcal{F}_j f(k) \\
&+ \zeta^T(k-\tau_b)(k) \mathcal{C}_j^T \hat{\rho}_j P \mathcal{C}_j \zeta(k-\tau_b) + 2\zeta^T(k-\tau_b)(k) \mathcal{C}_j^T \hat{\rho}_j P \mathcal{E}_j \xi_{uy}(k) \\
&+ 2\zeta^T(k-\tau_b)(k) \mathcal{C}_j^T \hat{\rho}_j P \mathcal{D}_j d(k) + +2\zeta^T(k-\tau_b)(k) \mathcal{C}_j^T \hat{\rho}_j P \mathcal{F}_j f(k) \\
&+ \xi_{uy}^T(k) \mathcal{E}_j^T \hat{\rho}_j P \mathcal{E}_j \xi_{uy}(k) + 2\xi_{uy}^T(k) \mathcal{E}_j^T \hat{\rho}_j P \mathcal{D}_j d(k) + 2\xi_{uy}^T(k) \mathcal{E}_j^T \hat{\rho}_j P \mathcal{F}_j f(k) \\
&+ d^T(k) \mathcal{D}_j^T \hat{\rho}_j P \mathcal{D}_j d(k) + 2d^T(k) \mathcal{D}_j^T \hat{\rho}_j P \mathcal{F}_j f(k) + f^T(k) \mathcal{F}_j^T \hat{\rho}_j P \mathcal{F}_j f(k) \Big]
\end{aligned} \tag{A1}$$

Simple calculations for ΔV_2–ΔV_5 results in:

$$\begin{aligned}
\mathbb{E}[\Delta V_2(\zeta(k))] \leq \textstyle\sum_{j=1}^{9} \hat{\rho}_j \Big[&\zeta^T(k) Q_j \zeta(k) - \zeta^T(k-\tau_f) Q_j \zeta(k-d_k^f) \\
&+ \textstyle\sum_{i=k+1-d_f^{\max}}^{k-d_f^{\min}} \zeta^T(i) Q_j \zeta(i) \Big]
\end{aligned} \tag{A2}$$

$$\begin{aligned}
\mathbb{E}[\Delta V_3(\zeta(k))] \leq \sum_{j=1}^{9} \hat{\rho}_j \Big[&\zeta^T(k) Q_j \zeta(k) - \zeta^T(k-d_k^b) Q_j \zeta(k-\tau_b) \\
&+ \sum_{i=k+1-d_b^{\max}}^{k-d_b^{\min}} \zeta^T(i) Q_j \zeta(i) \Big]
\end{aligned} \tag{A3}$$

and

$$\begin{aligned}
\mathbb{E}[\Delta V_4(\zeta(k))] = \sum_{j=1}^{9} \hat{\rho}_j \Big[&(d_f^{\max} - d_f^{\min}) \zeta^T(k) Q_j \zeta(k) \\
&- \sum_{i=k+1-d_f^{\max}}^{k-d_f^{\min}} \zeta^T(i) Q_j \zeta(i) \Big]
\end{aligned} \tag{A4}$$

$$\begin{aligned}
\mathbb{E}[\Delta V_5(\zeta(k))] = \sum_{j=1}^{9} \hat{\rho}_j \Big[&(d_b^{\max} - d_b^{\min}) \zeta^T(k) Q_j \zeta(k) \\
&- \sum_{i=k+1-d_b^{\max}}^{k-d_b^{\min}} \zeta^T(i) Q_j \zeta(i) \Big]
\end{aligned} \tag{A5}$$

The combination of Equations (A1)-(A5) and considerations of $d^T(k)d(k) \leq \varrho_1^2$, $f^T(k)f(k) \leq \varrho_2^2$, $\zeta(k)^T(k)\zeta(k) \leq \varrho_3^2$, and $\epsilon^T(k)\epsilon(k) \leq \varrho_4^2$ will lead to:

$$\begin{aligned}
&\mathbb{E}[\Delta V(\zeta(k))] \leq \\
&\sum_{j=1}^{9} \Big[\zeta^T(k) \hat{\rho}_j \left[\mathcal{A}_j^T P \mathcal{A}_j - P + 2Q_j + (\Delta\tau_f + \Delta\tau_b) Q_j \right] \zeta(k)
\end{aligned}$$

$$
\begin{aligned}
&+ 2\zeta^T(k)\mathcal{A}_j^T\hat{\rho}_j P\mathcal{B}_j\zeta(k-\tau_f) + 2\zeta^T(k)\mathcal{A}_j^T\hat{\rho}_j P\mathcal{C}_j\zeta(k-\tau_b)\\
&+ 2\zeta^T(k)\mathcal{A}_j^T\hat{\rho}_j P\mathcal{E}_j\xi_{uy}(k) + 2\zeta^T(k)\mathcal{A}_j^T\hat{\rho}_j P\mathcal{D}_j d(k)\\
&+ 2\zeta^T(k)\mathcal{A}_j^T\hat{\rho}_j P\mathcal{F}_j f(k) + \zeta^T(k-\tau_f)(k)(\mathcal{B}_j^T\hat{\rho}_j P\mathcal{B}_j - \hat{\rho}_j Q_j)\zeta(k-\tau_f)\\
&+ 2\zeta^T(k-\tau_f)(k)\mathcal{B}_j^T\hat{\rho}_j P\mathcal{C}_j\zeta(k-\tau_b) + 2\zeta^T(k-\tau_f)(k)\mathcal{B}_j^T\hat{\rho}_j P\mathcal{E}_j\xi_{uy}(k)\\
&+ 2\zeta^T(k-\tau_f)(k)\mathcal{B}_j^T\hat{\rho}_j P\mathcal{D}_j d(k) + 2\zeta^T(k-\tau_f)(k)\mathcal{B}_j^T\hat{\rho}_j P\mathcal{F}_j f(k)\\
&+ \zeta^T(k-\tau_b)(k)(\mathcal{C}_j^T\hat{\rho}_j P\mathcal{C}_j - \hat{\rho}_j Q_j)\zeta(k-\tau_b)\\
&+ 2\zeta^T(k-\tau_b)(k)\mathcal{C}_j^T\hat{\rho}_j P\mathcal{E}_j\xi_{uy}(k) + 2\zeta^T(k-\tau_b)(k)\mathcal{C}_j^T\hat{\rho}_j P\mathcal{D}_j d(k)\\
&+ 2\zeta^T(k-\tau_b)(k)\mathcal{C}_j^T\hat{\rho}_j P\mathcal{F}_j f(k) + \xi_{uy}^T(k)(\mathcal{E}_j^T\hat{\rho}_j P\mathcal{E}_j - \varsigma_1 I)\xi_{uy}(k)\\
&+ 2\xi_{uy}^T(k)\mathcal{E}_j^T\hat{\rho}_j P\mathcal{D}_j d(k) + 2\xi_{uy}^T(k)\mathcal{E}_j^T\hat{\rho}_j P\mathcal{F}_j f(k)\\
&+ d^T(k)(\mathcal{D}_j^T\hat{\rho}_j P\mathcal{D}_j - \varsigma_2 I)d(k) + 2d^T(k)\mathcal{D}_j^T\hat{\rho}_j P\mathcal{F}_j f(k)\\
&+ f^T(k)(\mathcal{F}_j^T\hat{\rho}_j P\mathcal{F}_j - \varsigma_3 I f(k)\Big]
\end{aligned}
\tag{A6}
$$

Let:

$$
\Omega(k) = \big[\zeta^T(k); \zeta^T(k-\tau_f); \zeta^T(k-\tau_b); \xi_{uy}^T(k); d^T(k); f^T(k)\big] \tag{A7}
$$

Then, Equation (A6) is rewritten in the following form:

$$
\mathbb{E}[\Delta V(\zeta(k))] \leq \sum_{j=1}^{9}\Big[\Omega^T(k)\widetilde{\Upsilon}_j\Omega(k) + \theta^2\Big] \tag{A8}
$$

From Equation (A7), it follows:

$$
\mathbb{E}[\Delta V(k)] \leq -\mathrm{eig}_{min}(-\Omega)\mathbb{E}\big[||\zeta(k)||^2\big] + \theta^2 \tag{A9}
$$

Moreover, when the energy-like functional's concept $V(k)$ is considered, one has:

$$
V(k) \leq \mathrm{eig}_{max}(P)\mathbb{E}\big[||\zeta(k)||^2\big] \tag{A10}
$$

Let us define a scalar $q > 1$. By considering Equations (A9)-(A10) we obtain:

$$
\begin{aligned}
\mathbb{E}[q^{k+1}V(k+1)] - \mathbb{E}[q^k V(k)] &= q^{k+1}\mathbb{E}[\Delta V(k)] + q^{k+1}\mathbb{E}[V(k)] - s^k\mathbb{E}[V(k)]\\
&\leq q^{k+1}\Big[-\mathrm{eig}_{min}(-\Omega)\mathbb{E}\big[||\zeta(k)||^2\big] + \theta^2\Big] + q^k(q-1)\mathbb{E}[V(k)]\\
&\leq h(q)q^k\mathbb{E}\big[||\zeta(k)||^2\big] + q^{k+1}\theta^2
\end{aligned}
\tag{A11}
$$

with $h(q) = -\mathrm{eig}_{min}(-\Omega)q + (q-1)\mathrm{eig}_{max}(P)$.

A integer s is considered, the two sides of Equation (A11) are summed with respect to k during the period 0 to $s-1$, this leads to:

$$
\mathbb{E}[q^T V(s)] - \mathbb{E}[V(0)] \leq h(q)\sum_{k=0}^{s-1} q^k\mathbb{E}\big[||\zeta(k)||^2\big] + \frac{q(1-q^s)}{1-q}\theta^2 \tag{A12}
$$

Becuase $h(1) = -\mathrm{eig}_{min}(-\Omega) < 0$, $h(q_0) = 0$ for a scalar $q_0 > 1$, and $\lim_{q\to\infty} = +\infty$, a scalar q_0 can be obtained using the following inequality:

$$
\mathbb{E}[q_0^s V(s)] - \mathbb{E}[V(0)] \leq \frac{q_0(1-q_0^s)}{1-q_0}\theta^2 \tag{A13}
$$

Note:

$$
\begin{aligned}
\mathbb{E}[q_0^T V(s)] &\geq \mathrm{eig}_{min}(P)q_0^s\mathbb{E}\big[||\zeta(s)||^2\big]\\
&\geq \mathrm{eig}_{min}(P)q_0^s\mathbb{E}\big[||\epsilon(s)||^2\big]
\end{aligned}
\tag{A14}
$$

Therefore:

$$
\mathbb{E}\big[||\epsilon(s)||^2\big] \leq \frac{(q_0^s-1)\phi^2}{q_0^{s-1}(q_0-1)\mathrm{eig}_{min}(P)} \tag{A15}
$$

Considering Equation (A6), one can show that $\mathbb{E}\|\epsilon(s)\|^2 \leq \varrho_2^2$, and using Definition 1, one can conclude that the system is $\varrho_1, \varrho_2, \varrho_3, \varrho_4, \varrho_5$ secure, thereby completing the proof.

An International Journal of Optimization and Control: Theories & Applications
(https://accscience.com/journal/ijocta)