

Article

Observer-Based Event-Triggered Secure Control for Networked Nonlinear Systems Under Denial-of-Service Attacks

Dianhua Lu ¹, He Zhang ¹, Quanling Zhang ^{2,*} and Cuimei Bo ¹ 

¹ School of Electrical Engineering and Control Science, Nanjing Tech University, Nanjing 211816, China; ldh123@njtech.edu.cn (D.L.); zhanghe@njtech.edu.cn (H.Z.); lj_bcm@163.com (C.B.)

² Institute of Intelligent Manufacturing, Nanjing Tech University, Nanjing 210009, China

* Correspondence: zhangquanling@njtech.edu.cn

Abstract

This paper investigates an observer-based secure control method for networked non-Lipschitz nonlinear systems subject to unknown nonlinearities, external disturbances, sensor noises, and intermittent denial-of-service (DoS) attacks. Multi-layer neural networks (MNNs) are adopted to compensate for non-smooth, non-Lipschitz terms, guaranteeing bounded approximation errors. A resilient high-gain observer fused with the MNN is developed to continuously reconstruct system states. When DoS attacks block sensor channels, the observer acts as a virtual dynamic engine to substitute for lost real-time measurements, providing uninterrupted feedback to the controller. Furthermore, to optimize communication efficiency, an observer-based static event-triggered mechanism (SETM) coupled with a hold-input strategy is integrated. Employing the Lyapunov–Krasovskii functional method, sufficient conditions are derived to prove that the closed-loop system remains uniformly ultimately bounded (UUB) under the joint effects of approximation errors, disturbances, and attacks. Simulation results on a two-link manipulator demonstrate that the proposed secure control scheme effectively counters aggressive DoS attacks while achieving a 56.8% reduction in network transmissions compared with conventional periodic sampling paradigms, striking a favorable balance between tracking accuracy and resource efficiency.

Keywords: state observer; denial-of-service attacks; neural networks; nonlinear systems

1. Introduction

In practical networked control systems (NCSs), constrained by sensor costs, installation space, and harsh measurement environments, the internal states of the system are often not directly measurable. Therefore, state observers have become a core link in realizing output feedback safety control [1,2].

In practical cyber–physical systems, networked nodes and subsystems typically correspond to physical mechatronic actuators, such as servo motor drives, hydraulic valves, or robotic joints. Therefore, mitigating the effects of network degradation and cyber-attacks is not merely a theoretical communication issue, but a critical prerequisite for ensuring safe and reliable physical actuation performance in networked control systems. However, the shared communication networks in NCSs are highly vulnerable to malicious cyber threats. Denial-of-service (DoS) attacks, by injecting massive amounts of junk data to congest communication channels, lead to the intermittent loss of measurement signals [3].



Academic Editor: Ioan Ursu

Received: 28 May 2026

Revised: 16 June 2026

Accepted: 22 June 2026

Published: 3 July 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

Traditional state observers may experience performance degradation during communication interruptions, and prolonged attacks can significantly increase estimation errors, thereby affecting closed-loop stability and control performance [2,4].

To address the data interruption problem caused by DoS attacks, scholars have proposed a series of resilient state observer design methods [5,6]. Switched observers are currently the most widely used resilient observer architecture, whose core idea is to design sub-observers for normal communication and attack interruption modes respectively, and switch the observation gain in real time according to attack detection results [1,5]. Existing studies have further proposed composite observers based on attack compensators, which predict and compensate for lost output signals by introducing an attack compensation module. This solves the difficulty of state reconstruction during DoS attacks and realizes predefined-time tracking control of nonlinear systems combined with dynamic event-triggered mechanisms [5,7].

However, physical systems often exhibit complex nonlinear characteristics, which poses a significant challenge to observer design and feedback control. To deal with the unknown nonlinearities of the system, neural networks (NNs) and fuzzy logic systems have been widely introduced into resilient control [8,9]. Recent studies have also reported practical applications of fuzzy control strategies in nonlinear system regulation, such as fuzzy PD-based approaches for mechanical system stabilization [10]. For instance, Lin et al. [11] applied a data-driven RBF neural network observer to a permanent magnet synchronous motor speed regulation system, realizing high-precision compensation for non-smooth nonlinearities. Scholars have also utilized radial basis function neural networks (RBFNNs) to approximate unknown nonlinear terms, designed neural network switched observers, and realized resilient control of power system load frequency [8,12]. Despite these advancements, most existing resilient observers assume that the system nonlinearities satisfy the global Lipschitz continuity condition. In conventional observer-based designs, the Lipschitz constant is typically required to establish observer error dynamics and derive Lyapunov-based stability conditions. However, for practical nonlinear systems with polynomial growth, velocity-coupling terms, or non-smooth friction effects, obtaining a finite and sufficiently tight global Lipschitz constant is often impossible or excessively conservative. As a result, observer gains derived from Lipschitz bounds can become overly conservative, leading to state estimation peaking, heightened sensitivity to measurement noise, and diminished robustness in the presence of communication interruptions induced by denial-of-service (DoS) attacks. Specifically, many practical nonlinear systems, such as robotic manipulators and electromechanical actuator systems, contain polynomial, quadratic velocity-coupling, friction, and saturation-related nonlinearities whose derivatives may grow unboundedly with respect to the system states. Consequently, although these nonlinear functions remain continuous on compact operating regions, they generally do not satisfy the global Lipschitz condition required by conventional observer design approaches. Although the fuzzy neural extended state observer proposed by Fei et al. [13] can effectively estimate lumped disturbances, severe convergence issues remain when dealing with non-Lipschitz nonlinearities with locally unbounded rates of change, especially when the measurement channel is simultaneously blocked by DoS attacks.

Recently, significant progress has been made in composite anti-disturbance and attack-resilient control for networked systems under event-triggered communication mechanisms. For instance, an event-triggered output feedback control framework for systems subject to disturbances and actuator attacks was developed in [14], highlighting the effectiveness of integrating communication-efficient strategies with robust control design. Motivated by these developments, this paper investigates an observer-based event-triggered secure control strategy for networked non-Lipschitz nonlinear systems under DoS attacks.

Multi-layer neural networks (MNNs) are employed to approximate unknown nonlinear dynamics that do not satisfy the global Lipschitz condition. A neural-network-assisted high-gain observer is designed to continuously reconstruct unavailable state information during communication interruptions caused by DoS attacks, thereby maintaining continuous state estimation performance.

To improve communication efficiency and reduce unnecessary data transmissions, a static event-triggered mechanism (SETM) is integrated into the observer-based control framework. Meanwhile, a zero-order-hold mechanism is adopted to maintain the latest successfully transmitted control signal during attack intervals. Based on the Lyapunov–Krasovskii functional method, sufficient conditions are derived to guarantee the uniform ultimate boundedness (UUB) of the closed-loop system under the combined effects of neural network approximation errors, bounded disturbances, event-triggered transmissions, and DoS attacks.

The main contributions of this paper are summarized as follows:

- (1) A neural-network-assisted high-gain observer is developed for non-Lipschitz nonlinear systems under DoS attacks. By explicitly incorporating the multi-layer neural network (MNN) into the observer dynamics, the proposed framework provides predictive information during DoS intervals, thereby facilitating bounded state estimation without relying on strict Lipschitz assumptions.
- (2) An observer-based static event-triggered secure control strategy is proposed. This mechanism effectively reduces communication burden while maintaining closed-loop stability under intermittent DoS attacks.
- (3) A unified stability analysis framework incorporating DoS attacks and event-triggered transmission behaviors is established. Based on this framework, LMI-based sufficient conditions are derived to guarantee the uniformly ultimately bounded (UUB) stability of the closed-loop system.

2. Problem Description and Preliminaries

2.1. System Description

Consider a class of nonlinear systems described by the following state space:

$$\begin{aligned}\dot{\mathbf{x}}(t) &= \mathbf{A}\mathbf{x}(t) + \delta(\mathbf{x}, t) + \mathbf{B}\mathbf{u}(t) + \mathbf{d}(t) \\ \mathbf{y}(t) &= \mathbf{C}\mathbf{x}(t) + \boldsymbol{\omega}(t)\end{aligned}\quad (1)$$

where $\mathbf{x}(t) \in \mathbb{R}^n$ is the system state, $\mathbf{u}(t) \in \mathbb{R}^m$ is the control input, $\delta(\mathbf{x}, t)$ is the nonlinear term representing system uncertainties and control actions, $\mathbf{d}(t)$ is the external disturbance input, $\mathbf{y} \in \mathbb{R}^n$ is the system output, and $\boldsymbol{\omega}(t)$ is the measurement noise. $\mathbf{A}, \mathbf{B}, \mathbf{C}$ are known system matrices of appropriate dimensions. It is assumed that the disturbances and measurement noise are bounded.

The objective of this study is to design a state observation-based feedback control strategy under the conditions of unknown nonlinearities, external disturbances, and denial-of-service (DoS) attacks on the communication channel.

The following assumptions are introduced:

Assumption 1. The state and control input of the nonlinear system are bounded, $\mathbf{x}(t) \in X$ and $\mathbf{u}(t) \in U$, where $X \subset \mathbb{R}^n$ and $U \subset \mathbb{R}^m$ are compact sets.

Remark 1. It should be emphasized that Assumption 1 only constrains the actual system trajectories to evolve within a compact operating region and does not imply that the nonlinear function satisfies a global Lipschitz condition. In particular, practical nonlinear dynamics may contain polynomial growth terms, quadratic velocity-coupling terms, or non-smooth friction effects. Their derivatives

can become arbitrarily large outside the operating region, preventing the existence of a finite global Lipschitz constant. Therefore, the considered system belongs to the class of nonlinear systems that are continuous on compact sets but do not satisfy global Lipschitz continuity.

Moreover, although a local Lipschitz constant may exist on a compact operating region, such a constant is generally unknown and highly dependent on the operating domain. Therefore, conventional observer designs relying on explicit Lipschitz bounds may become conservative and difficult to implement in practice.

Assumption 2. There exist ideal neural network weight matrices $\mathbf{M}_1^*$ and $\mathbf{M}_2^*$ with bounded norms. Furthermore, the approximation error of the neural network satisfies $\|\epsilon(t)\| \leq \phi\|\mathbf{x}(t)\|$, where $\phi > 0$ is a known constant.

Assumption 3. The activation function satisfies the Lipschitz continuity condition; there exists a constant $L_\mu > 0$ such that $\|\mu(a) - \mu(b)\| \leq L_\mu\|a - b\|$ holds for all $a, b \in \mathbb{R}^{n_h}$.

Assumption 4. The system disturbances $\mathbf{d}(t)$ are bounded, satisfying $\|\mathbf{d}(t)\| \leq \mathbf{d}_0$.

Remark 2. Practical Applicability and Conservativeness of the Boundedness Assumptions: Assumptions 1, 2, and 4 constrain the system states, control inputs, neural network approximation errors, and external disturbances to be strictly bounded. In the context of practical networked nonlinear systems (e.g., robotic manipulators), these assumptions are not overly conservative but rather direct reflections of physical realities. For instance, control inputs are naturally bounded by actuator saturation limits (e.g., maximum motor torque), states are confined by mechanical workspaces, and ambient disturbances or sensor noises inherently possess finite energy.

However, in real-world scenarios under severe DoS conditions or extreme environmental shocks, these assumptions might only be partially satisfied (e.g., transient disturbance spikes exceeding the predefined theoretical bound $\mathbf{d}_0$). Benefiting from the uniformly ultimately bounded (UUB) property established in Theorem 1, such transient violations do not instantly trigger system instability; instead, they merely result in a proportional and temporary expansion of the ultimate residual error set. Nevertheless, if these bounded assumptions are persistently and massively violated, the MNN may be forced to operate outside its valid compact set, which would degrade the accuracy of the feedforward compensation and eventually risk system instability.

2.2. Relevant Lemmas

Lemma 1. Consider a differentiable function $\mu(t) : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ satisfying

$$\dot{\mu}(t) \leq -a_\theta \mu(t) + b_\theta \int_{t_k}^t \mu(v) dv + p_\theta(t), \quad \forall t \in [t_k, t_{k+1}) \quad (2)$$

Then, $k \in \mathbb{N}$, $t_0 \geq 0$ and $0 < h_M = t_{k+1} - t_k < +\infty$, where a_θ , b_θ and c_θ are positive real numbers. The function $p_\theta(t) : \mathbb{R}^+ \rightarrow \mathbb{R}$ is fundamentally bounded and it satisfies $c_\theta = \sup_{t \geq 0} \text{Ess } p_\theta(t)$. If $h_M < \chi_\theta = a_\theta / b_\theta$, then

$$\mu(t) \leq e^{-\tilde{\theta}(t-t_0)} \mu(t_0) + c_\theta h_M \frac{2 - e^{-\tilde{\theta} h_M}}{1 - e^{-\tilde{\theta} h_M}} \quad (3)$$

where $0 < \tilde{\theta} = a_\theta(1 - h_M/\chi_\theta)e^{-a_\theta h_M}$.

Lemma 2. Given a continuous real function $g(t) : t \in [-\sigma, +\infty) \rightarrow g(t) \in [0, +\infty)$, it satisfies the integral inequality

$$g(t) \leq s(t) + \rho \int_{t-\sigma}^t g(v) dv, t \geq 0 \quad (4)$$

where $\sigma > 0$, ρ is a positive constant, and $s(t)$ denotes a non-decreasing non-negative real function. If $\rho\sigma < 1$, we have $g(t) \leq z(t)/(1 - \rho\sigma)$; then,

$$z(t) = s(t) + \rho \int_{-\sigma}^0 g(v) dv > 0. \quad (5)$$

3. Observer-Based Event-Triggered Secure Control Design

3.1. Multi-Layer Neural Networks (MNNs)

Multi-layer neural networks (MNNs), with their powerful nonlinear fitting capabilities, can effectively handle complex nonlinear dynamics that do not satisfy Lipschitz continuity, laying a foundation for subsequent observer design. To handle the unknown nonlinear term in the system state space, Equation (1), we propose an MNN structure comprising two input layers, at least one hidden layer, and two output layers. An MNN with one hidden layer and zero-bias term can be represented in matrix–vector form as follows:

$$\delta_{nn}(\mathbf{x}, \mathbf{M}_1^*, \mathbf{M}_2^*) = \mathbf{M}_2^* \mu(\mathbf{M}_1^* \mathbf{x}(t)) \quad (6)$$

where $\delta_{nn}(\mathbf{x}, \mathbf{M}_1^*, \mathbf{M}_2^*)$ represents the output of the neural network, $\mathbf{M}_1^*$ is the weight matrix between the input layer and the hidden layer, and $\mathbf{M}_2^*$ is the weight matrix between the hidden layer and the output layer. In this work, the bipolar sigmoid function is adopted as the activation function:

$$\mu_i(s) = d \cdot \frac{1 - e^{-qs}}{1 + e^{-qs}}, \quad (7)$$

where $d > 0$ is the output range parameter and $q > 0$ is the slope parameter. This function satisfies $\mu_i(0) = 0$ and is bounded for any input s . According to the properties of MNNs, any continuous nonlinear function on a compact set can be approximated to arbitrary precision. Thus, the nonlinear term can be expressed as

$$\delta(\mathbf{x}, t) = \delta_{nn}(\mathbf{x}, \mathbf{M}_1^*, \mathbf{M}_2^*) + \varepsilon(\mathbf{x}, t) \quad (8)$$

where $\varepsilon(\mathbf{x}, t)$ is the approximation error, which satisfies Assumption 2. Consequently, the original system can be rewritten as

$$\begin{aligned} \dot{\mathbf{x}}(t) &= \mathbf{A}\mathbf{x}(t) + \mathbf{M}_2^* \mu(\mathbf{M}_1^* \mathbf{x}(t)) + \varepsilon(\mathbf{x}, t) + \mathbf{B}\mathbf{u}(t) + \mathbf{d}(t) \\ \mathbf{y}(t) &= \mathbf{C}\mathbf{x}(t) + \boldsymbol{\omega}(t) \end{aligned} \quad (9)$$

Remark 3. The existing elastic state estimation schemes [15] handle nonlinear dynamics via Lipschitz linearization to facilitate controller parameter design, which limits their applicability to strictly nonlinear systems. To address this issue, this paper re-models the nonlinear dynamics using a multi-layer neural network (MNN), effectively ensuring boundedness of approximation errors under complex operating conditions. More critically, in the event of denial-of-service (DoS) attacks that impair measurement feedback, the model-based neural network (MNN) serves as a robust auxiliary approximator of the unknown nonlinear system dynamics. During communication interruptions, it furnishes model-driven compensation signals to the observer, thereby enhancing state estimation accuracy under partial or complete measurement loss.

3.2. High-Gain Observer Design

During periods of normal communication or between attack intervals, the system employs the following MNN-based high-gain observer for state estimation:

$$\begin{aligned}\dot{\hat{\mathbf{x}}}(t) &= \mathbf{A}\hat{\mathbf{x}}(t) + \delta_{nn}(\hat{\mathbf{x}}, \mathbf{M}_1^*, \mathbf{M}_2^*) + \mathbf{B}\mathbf{u}(t) - \theta\mathbf{K}\boldsymbol{\eta}(t) \\ \dot{\boldsymbol{\eta}}(t) &= \theta\boldsymbol{\xi}(t), \boldsymbol{\eta}(0) = 0 \\ \dot{\boldsymbol{\xi}}(t) &= -\theta\boldsymbol{\Omega}_1\boldsymbol{\xi}(t) - \theta\boldsymbol{\Omega}_2\boldsymbol{\eta}(t) + \theta^2\mathbf{A}^T\boldsymbol{\eta}(t) \\ &\quad + \theta\mathbf{C}^T(\mathbf{C}\hat{\mathbf{x}}(t_k) - \mathbf{y}(t_k) + \boldsymbol{\delta}(t)) \\ \dot{\boldsymbol{\delta}}(t) &= -\theta k_1\boldsymbol{\eta}_1(t), \quad \boldsymbol{\delta}(t_k) = 0\end{aligned}\quad (10)$$

where $\hat{\mathbf{x}}(t)$ is the state estimate and $\delta_{nn}(\hat{\mathbf{x}}, \mathbf{M}_1^*, \mathbf{M}_2^*)$ is the neural network approximation. $\theta > 0$ is an adjustable high-gain parameter; increasing θ can enhance the convergence rate. The parameter $\theta > 1$ dictates the convergence speed of the observer. According to the scaled error dynamics, a larger θ forces the state estimation error to decay exponentially faster, thereby powerfully overriding bounded external disturbances and network uncertainties. However, an excessively large θ may induce the “peaking phenomenon” and amplify high-frequency measurement noise. Thus, its selection is a tradeoff between convergence rate and noise sensitivity.

The variables $\boldsymbol{\eta}(t)$, $\boldsymbol{\zeta}(t)$, and $\boldsymbol{\delta}(t)$ are auxiliary dynamic variables introduced to manage sampling errors and measurement noise, ensuring continuity and providing filtering effects. $\mathbf{K} = \text{diag}(k_1, k_2, \dots, k_n)$ is the high-gain feedback matrix, while $\boldsymbol{\Omega}_1 = \text{diag}(\sigma_1, \dots, \sigma_n)$ and $\boldsymbol{\Omega}_2 = \text{diag}(\varepsilon_1, \dots, \varepsilon_n)$ are auxiliary variable feedback gains. All signals are updated using the sample-and-hold output $\mathbf{y}(t_k)$ to maintain estimation during output channel blockages or DoS attacks. By introducing these auxiliary dynamic variables, the composite observer inherently constructs a filtering mechanism. This structure effectively attenuates the amplification of high-frequency measurement noise and alleviates peaking phenomena without compromising the rapid convergence guaranteed by the high-gain parameter, thereby striking a favorable balance between convergence speed and noise sensitivity.

3.3. Observation State Convergence Analysis

Before presenting the convergence analysis, the following lemma is introduced.

Lemma 3. Consider a matrix $\mathcal{M}$ and define

$$\mathcal{M} = \begin{bmatrix} \mathbf{A} & -\mathbf{K} & 0_n \\ 0_n & 0_n & \mathbf{I}_n \\ \mathbf{C}^T\mathbf{C} & -\boldsymbol{\Omega}_2 + \mathbf{A}^T & -\boldsymbol{\Omega}_1 \end{bmatrix}. \quad (11)$$

There exists a matrix $\mathbf{K}$, $\boldsymbol{\Omega}_1$ and $\boldsymbol{\Omega}_2$, such that $\mathcal{M}$ is Hurwitz, and there exist a symmetric positive definite matrix $\mathbf{P}$ and a constant $\gamma > 0$ satisfying

$$\mathbf{P}\mathcal{M} + \mathcal{M}^T\mathbf{P} \leq -2\gamma\mathbf{I}_{3n}. \quad (12)$$

To analyze the stability of the observation error system, we define the estimation error as $\tilde{\mathbf{x}}(t) = \hat{\mathbf{x}}(t) - \mathbf{x}(t)$. By introducing the scaled transformation and defining the augmented state vector $\bar{\boldsymbol{\zeta}}(t)$, the error dynamics can be expressed in a scaled form:

$$\begin{aligned}
\dot{\bar{\mathbf{x}}}(t) &= \theta \bar{\mathbf{A}} \bar{\mathbf{x}}(t) + \theta^{n-1} \Delta(\theta) \bar{\mathbf{M}}_2^* [\mu(\bar{\mathbf{M}}_1^* \hat{\mathbf{x}}(t)) - \mu(\bar{\mathbf{M}}_1^* \bar{\mathbf{x}}(t))] \\
&\quad - \theta^{n-1} \Delta(\theta) \bar{\boldsymbol{\varepsilon}}(\bar{\mathbf{x}}, t) - \theta \bar{\mathbf{K}} \bar{\boldsymbol{\eta}}(t) - \theta^{n-1} \Delta(\theta) \bar{\mathbf{d}}(t), \\
\dot{\bar{\boldsymbol{\eta}}}(t) &= \theta \bar{\boldsymbol{\xi}}(t), \\
\dot{\bar{\boldsymbol{\xi}}}(t) &= -\theta \bar{\boldsymbol{\Omega}}_1 \bar{\boldsymbol{\xi}}(t) - \theta \bar{\boldsymbol{\Omega}}_2 \bar{\boldsymbol{\eta}}(t) + \theta \bar{\mathbf{A}}^T \bar{\boldsymbol{\eta}}(t) \\
&\quad + \theta \bar{\mathbf{C}}^T \bar{\mathbf{C}} \bar{\mathbf{x}}(t) - \theta^{n-1} \bar{\mathbf{C}} \boldsymbol{\omega}(t_k) - \theta \bar{\mathbf{C}}^T \bar{\mathbf{z}}(t),
\end{aligned} \tag{13}$$

By constructing a Lyapunov function $V(t) = \bar{\boldsymbol{\zeta}}^T(t) \mathbf{P} \bar{\boldsymbol{\zeta}}(t)$, where $\mathbf{P}$ is a symmetric positive definite matrix satisfying the conditions in Lemma 1, we can derive the derivative of the energy function. If the conditions of the observer gains and sampling intervals are satisfied, yielding the exponential decay of the Lyapunov functional, then it follows that the observation error converges exponentially to a bounded set.

3.4. DoS Attack Model and Time-Varying Delay Representation

Denial-of-service (DoS) attacks disrupt the communication channel and prevent real-time state information from being transmitted to the controller. In this work, their effect is not modeled as a switched system. Instead, it is uniformly represented as a continuous time-varying communication delay $\tau(t)$ induced by packet loss and event-triggered transmission blocking.

The DoS attack process is characterized by the following frequency and duration constraints:

$$\begin{aligned}
N_D(t) &\leq \kappa_D + \frac{t}{\tau_D} \\
\sum_{q: h_q^e \leq t} (h_q^e - h_q^d) &\leq T_D + \eta_D t
\end{aligned}$$

These constraints define an admissible class of DoS signals with bounded long-term attack frequency and bounded attack duration ratio. Specifically, the first inequality limits the average number of attack occurrences over time, while the second inequality restricts the asymptotic fraction of time under denial-of-service conditions, where $\eta_D \in (0, 1)$.

Importantly, these constraints do not impose any deterministic minimum attack-free interval or dwell-time condition in the classical switched-system sense. Instead, they ensure a non-vanishing proportion of attack-free transmission opportunities in an average sense through the condition $\eta_D \in (0, 1)$, which guarantees sufficient communication availability for the Lyapunov–Krasovskii functional to establish stability.

In particular, back-to-back DoS attacks are fully admissible in this framework and are naturally absorbed into the continuous evolution of the time-varying delay $\tau(t)$ without introducing additional switching structures or inter-attack interval assumptions. Their cumulative effect is captured through the aggregation of successive communication blocking intervals within the delay trajectory.

Under this admissible set of DoS signals, the induced delay remains bounded as

$$\tau(t) \leq \tau_M$$

where τ_M denotes the maximum admissible delay used in the subsequent stability analysis.

During DoS intervals, the most recently transmitted control input is maintained via a zero-order-hold (ZOH) mechanism. Therefore, the closed-loop system can be equivalently transformed into a time-delay system, which unifies regular sampling, event-triggered transmission, and packet dropouts within a single analytical framework.

3.5. Static Event-Triggered Mechanism

To alleviate the communication network bandwidth constraints and reduce redundant data transmission induced by periodic sampling, a discrete event-triggered communication scheme is deployed between the observer and the controller.

Let h be the fixed sampling period; the sampling sequence is denoted as $\{s_i = s_0 + ih, i \in \mathbb{N}\}$. The event-triggered error is defined as the deviation between the current sampled state and the last successfully transmitted state:

$$\mathbf{e}_k(s_i) = \hat{\mathbf{x}}(t_k) - \hat{\mathbf{x}}(s_i) \quad (14)$$

To balance communication efficiency and steady-state performance, the following static event-triggered condition is constructed:

$$t_{k+1} = \inf \left\{ s_i > t_k \mid \mathbf{e}_k^T(s_i) \Omega \mathbf{e}_k(s_i) > \rho \hat{\mathbf{x}}^T(s_i) \Omega \hat{\mathbf{x}}(s_i) + \mu_0 \right\} \quad (15)$$

where $\Omega \in \mathbb{R}^{n \times n}$ is a symmetric positive definite weighting matrix to be designed.

$\rho \in (0, 1)$ is a given threshold parameter regulating the triggering frequency, and $\mu_0 > 0$ is a small positive constant to maintain steady-state operation and avoid Zeno behavior.

According to the triggering rule described above, during any adjacent triggering interval $[t_k, t_{k+1})$, all discrete sampling points inherently satisfy the following inequality constraint:

$$\rho \hat{\mathbf{x}}^T(s_i) \Omega \hat{\mathbf{x}}(s_i) - \mathbf{e}_k^T(s_i) \Omega \mathbf{e}_k(s_i) + \mu_0 \geq 0 \quad (16)$$

This inequality constitutes the core boundary condition of the system's communication-triggering mechanism and will be embedded as a prior constraint in the subsequent closed-loop stability proof.

3.6. Stability Analysis of Feedback Control Based on Static Event-Triggered Mechanism

This section aims to prove the uniform ultimate boundedness (UUB) and practical stability of the networked non-Lipschitz nonlinear system under the joint action of the proposed static event-triggered mechanism (SETM) and intermittent DoS attacks. This analysis accounts for MNN approximation errors, DoS attack-induced data dropouts, and communication network constraints using the Lyapunov–Krasovskii functional (LKF) method.

By adopting the feedback control law based on state observation, and considering the static event-triggered transmission rule, the actual control signal received by the actuator can be expressed as

$$\mathbf{u}(t) = \mathbf{u}(t_k) = -\mathbf{K}_p \hat{\mathbf{x}}(t_k) - \mathbf{K}_d \dot{\hat{\mathbf{x}}}(t_k), \quad t \in [t_k, t_{k+1}) \quad (17)$$

To establish a unified mathematical framework, we introduce a continuous time-varying delay function defined as $\tau(t) = t - t_k$. In the presence of intermittent DoS attacks, the growth of $\tau(t)$ is bounded by both the maximum allowable triggering interval and the physical upper bound of the attack duration T_{DoS} . Therefore, the comprehensive network-induced delay satisfies the following upper bound:

$$0 \leq \tau(t) \leq \tau_M, \quad \tau_M = (1 + L)h + T_{DoS} \quad (18)$$

By utilizing the algebraic identity $\hat{\mathbf{x}}(t_k) = \mathbf{x}(t - \tau(t)) + \tilde{\mathbf{x}}(t - \tau(t)) + \mathbf{e}_k(t)$, and substituting the control law (17) into the plant dynamics, the closed-loop comprehensive time-varying delay model is formulated as

$$\begin{aligned}\dot{\mathbf{x}}(t) = & (\mathbf{A} - \mathbf{BK}_p)\mathbf{x}(t) + \mathbf{BK}_p\zeta_1(t) - \mathbf{BK}_d\dot{\mathbf{x}}(t - \tau(t)) \\ & + \mathbf{BK}_p\mathbf{e}_k(t) + \mathbf{BK}_d\dot{\mathbf{e}}_k(t) + \boldsymbol{\omega}_t(t)\end{aligned}\quad (19)$$

where $\zeta_1(t) = \mathbf{x}(t) - \mathbf{x}(t - \tau(t))$ represents the state difference vector, and the lumped disturbance term $\boldsymbol{\omega}_t(t)$ is defined as

$$\boldsymbol{\omega}_t(t) = \boldsymbol{\delta}(\mathbf{x}, t) + \mathbf{d}(t) - \mathbf{BK}_p\tilde{\mathbf{x}}(t - \tau(t)) - \mathbf{BK}_d\dot{\tilde{\mathbf{x}}}(t - \tau(t)) \quad (20)$$

Based on the bounded property of the MNN approximation error and the exponential convergence of the observer error established in Theorem 1, the lumped disturbance is strictly bounded by $\|\boldsymbol{\omega}_t(t)\| \leq \mu_A$.

Based on the bounded property of the MNN approximation error established in Assumption 2, the bounded external disturbance from Assumption 4, and the exponential convergence of the scaled observer estimation errors verified in Section 3.3, all constituent elements of the lumped disturbance $\boldsymbol{\omega}_t(t)$ are strictly upper-bounded within the compact operating space. Consequently, by invoking the mathematical triangle inequality, the lumped disturbance vector is guaranteed to be strictly bounded by a comprehensive positive constant μ_A . This constant μ_A is fundamentally determined by the supremum bounds of the ideal neural network weights, the activation functions, the compact system states, and the steady-state observer estimation errors along with their derivatives on their respective compact domains.

The sufficient conditions for the practical stability of the closed-loop system under SETM and DoS constraints are presented in Theorem 1.

Theorem 1. For the closed-loop networked non-Lipschitz nonlinear system (19) subject to intermittent DoS attacks and event-triggered constraints, given the maximum delay bound τ_M , the desired damping decay rate $\delta > 0$, the trigger parameters $\rho \in (0, 1)$, $\mu_0 > 0$, and the tuning scalars λ, η_1, η_2 , if there exist symmetric positive definite matrices $\mathbf{P}, \mathbf{Q}_1, \mathbf{Q}_2, \mathbf{Q}_3, \boldsymbol{\Omega}, \boldsymbol{\Omega}_d \in \mathbb{R}^{n \times n}$, a free-weighting matrix $\mathbf{G} \in \mathbb{R}^{n \times n}$, an invertible matrix $\mathbf{P}_2 \in \mathbb{R}^{n \times n}$, and intermediate decision matrices $\mathbf{X}, \mathbf{Y} \in \mathbb{R}^{m \times n}$ such that the following Linear Matrix Inequality (LMI) holds:

$$\Phi = \begin{bmatrix} \Xi_{11} & \Xi_{12} & \Xi_{13} & \Xi_{14} & \Xi_{15} & \mathbf{X} & \mathbf{Y} & \mathbf{P}_2 \\ * & \Xi_{22} & \Xi_{23} & 0 & 0 & 0 & 0 & 0 \\ * & * & \Xi_{33} & 0 & 0 & 0 & 0 & 0 \\ * & * & * & \Xi_{44} & \Xi_{45} & \lambda\mathbf{X} & \lambda\mathbf{Y} & \lambda\mathbf{P}_2 \\ * & * & * & * & \Xi_{55} & 0 & 0 & 0 \\ * & * & * & * & * & -\boldsymbol{\Omega} & 0 & 0 \\ * & * & * & * & * & * & -\boldsymbol{\Omega}_d & 0 \\ * & * & * & * & * & * & * & -\eta_t\mathbf{I} \end{bmatrix} < 0 \quad (21)$$

where $\eta_t = (\eta_1^{-1} + \eta_2^{-1})^{-1}$, and the block matrix elements are defined as follows:

$$\begin{aligned}\Xi_{11} &= \text{He}\{\mathbf{P}_2\mathbf{A} - \mathbf{X}\} + 2\delta\mathbf{P} + \mathbf{Q}_2 + \tau_M\mathbf{Q}_3 - \frac{e^{-2\delta\tau_M}}{\tau_M}\mathbf{Q}_1 \\ \Xi_{12} &= \mathbf{X} + \frac{e^{-2\delta\tau_M}}{\tau_M}(\mathbf{Q}_1 - \mathbf{G}), \quad \Xi_{13} = \frac{e^{-2\delta\tau_M}}{\tau_M}\mathbf{G} \\ \Xi_{14} &= \mathbf{P} - \mathbf{P}_2 + \lambda\mathbf{A}^T\mathbf{P}_2^T - \lambda\mathbf{X}^T, \quad \Xi_{15} = -\mathbf{Y} \\ \Xi_{22} &= -\frac{e^{-2\delta\tau_M}}{\tau_M}(2\mathbf{Q}_1 - \mathbf{G} - \mathbf{G}^T) + \rho e^{-2\delta\tau_M}\boldsymbol{\Omega} \\ \Xi_{23} &= \frac{e^{-2\delta\tau_M}}{\tau_M}(\mathbf{Q}_1 - \mathbf{G}), \quad \Xi_{33} = -e^{-2\delta\tau_M}\mathbf{Q}_2 - \frac{e^{-2\delta\tau_M}}{\tau_M}\mathbf{Q}_1 \\ \Xi_{44} &= -\lambda\text{He}\{\mathbf{P}_2\} + \tau_M\mathbf{Q}_1, \quad \Xi_{45} = -\lambda\mathbf{Y}, \quad \Xi_{55} = -\epsilon_d\mathbf{I}\end{aligned}$$

then, the closed-loop system trajectories are exponentially uniformly ultimately bounded (UUB), and the system state strictly converges to the following residual set:

$$\mathcal{P} = \left\{ \mathbf{x} \in \mathbb{R}^n \mid \|\mathbf{x}\| \leq \sqrt{\frac{c_t + e^{-2\delta\tau_M}\mu_0}{2\delta\lambda_{\min}(\mathbf{P})}} \right\} \quad (22)$$

Furthermore, the controller gains can be precisely extracted by $\mathbf{K}_p = (\mathbf{P}_2\mathbf{B})^{-1}\mathbf{X}$ and $\mathbf{K}_d = (\mathbf{P}_2\mathbf{B})^{-1}\mathbf{Y}$.

Based on the time-delay representation established in Section 3.4, the closed-loop system is analyzed using a Lyapunov–Krasovskii functional (LKF). The resulting Linear Matrix Inequality (LMI) conditions are derived with respect to the maximum admissible delay bound τ_M .

These LMI conditions ensure that the closed-loop system is uniformly ultimately bounded (UUB), provided that the induced time-varying delay satisfies

$$\tau(t) \leq \tau_M$$

Unlike classical switched-system-based DoS-resilient control frameworks, the proposed approach does not require explicit dwell-time or minimum attack-free interval parameters within the LMI formulation. This is because the system dynamics are not modeled as mode switching between attack and normal operation; instead, all communication disruptions are embedded into the continuous evolution of a single delay variable $\tau(t)$.

In this framework, consecutive or back-to-back DoS attacks are fully admissible and do not introduce any additional structural complexity. They are naturally absorbed into the accumulation of communication blocking intervals, and therefore only affect the magnitude of the time-varying delay rather than the system structure.

The admissible DoS constraints introduced in Section 3.4 guarantee that the induced delay $\tau(t)$ remains within a bounded region characterized by τ_M . In particular, the frequency and duty-cycle constraints ensure that the cumulative blocking time cannot dominate the total time horizon, thereby preventing unbounded growth of $\tau(t)$.

If this bound is violated due to excessively persistent communication blocking, the sufficient LMI conditions for UUB stability are no longer satisfied, which is consistent with standard time-delay system theory.

From a control-theoretic perspective, τ_M serves as a robustness margin of the LKF-based stability condition rather than a restriction on individual attack events or an explicit dwell-time condition.

The feasibility of the LMI conditions in Theorem 1 depends on the admissible bounds of the network-induced delay, DoS duration, and the event-triggering parameter. Within these bounds, the LMI admits feasible solutions that guarantee closed-loop stability. When these parameters increase, the feasible region becomes more constrained, reflecting the intrinsic tradeoff between system robustness and communication limitations.

Proof of Theorem 1. To analyze the energy evolution of the system under both time-varying communication delays and triggering perturbations, we construct the following Lyapunov–Krasovskii functional incorporating the exponential decay rate:

$$V(t) = V_1(t) + V_2(t) + V_3(t) + V_4(t) \quad (23)$$

where the sub-components are defined as

$$\begin{aligned} V_1(t) &= \mathbf{x}^T(t)\mathbf{P}\mathbf{x}(t) \\ V_2(t) &= \int_{t-\tau_M}^t \int_{\theta}^t e^{2\delta(s-t)} \dot{\mathbf{x}}^T(s) \mathbf{Q}_1 \dot{\mathbf{x}}(s) ds d\theta \\ V_3(t) &= \int_{t-\tau_M}^t e^{2\delta(s-t)} \mathbf{x}^T(s) \mathbf{Q}_2 \mathbf{x}(s) ds \\ V_4(t) &= \int_{t-\tau_M}^t \int_{\theta}^t e^{2\delta(s-t)} \mathbf{x}^T(s) \mathbf{Q}_3 \mathbf{x}(s) ds d\theta \end{aligned} \quad (24)$$

Differentiating $V(t)$ along the trajectory of (19) and adding the term $2\delta V(t)$, we introduce the free-weighting matrices satisfying the linear proportion $\mathbf{P}_1 = \lambda \mathbf{P}_2$ to construct the following zero identity:

$$2[\mathbf{x}^T(t)\mathbf{P}_2 + \dot{\mathbf{x}}^T(t)(\lambda \mathbf{P}_2)][(\mathbf{A} - \mathbf{BK}_p)\mathbf{x}(t) + \mathbf{BK}_p\zeta_1(t) - \mathbf{BK}_d\dot{\mathbf{x}}(t - \tau(t)) + \mathbf{BK}_p\mathbf{e}_k(t) + \mathbf{BK}_d\dot{\mathbf{e}}_k(t) + \boldsymbol{\omega}_t(t) - \dot{\mathbf{x}}(t)] = 0 \quad (25)$$

By applying Young's inequality to decouple the nonlinear cross-terms containing the lumped disturbance $\boldsymbol{\omega}_t(t)$, we obtain

$$2[\mathbf{x}^T(t)\mathbf{P}_2 + \lambda \dot{\mathbf{x}}^T(t)\mathbf{P}_2]\boldsymbol{\omega}_t(t) \leq \eta_1 \mathbf{x}^T(t)\mathbf{P}_2\mathbf{P}_2^T\mathbf{x}(t) + \eta_2 \lambda^2 \dot{\mathbf{x}}^T(t)\mathbf{P}_2\mathbf{P}_2^T\dot{\mathbf{x}}(t) + c_t \quad (26)$$

where $c_t = (\eta_1^{-1} + \eta_2^{-1})\mu_A^2$ is the disturbance parameter.

To deal with the time-varying delay in the integral term of $\dot{V}_2(t)$, the integration interval is split into $[t - \tau(t), t]$ and $[t - \tau_M, t - \tau(t)]$. Utilizing Jensen's integral inequality and the reciprocally convex combination lemma with the free matrix $\mathbf{G}$, the integral term can be scaled to the quadratic form of state deviations.

According to the S-procedure technique, to confine the event-triggered errors within the established boundary conditions, the triggering constraint condition is introduced with the exponential weight

$$e^{-2\delta\tau_M}(\rho \dot{\mathbf{x}}^T(t - \tau(t))\boldsymbol{\Omega}\dot{\mathbf{x}}(t - \tau(t)) - \mathbf{e}_k^T(t)\boldsymbol{\Omega}\mathbf{e}_k(t) + \mu_0) \geq 0 \quad (27)$$

By substituting the intermediate decision variables $\mathbf{X} = \mathbf{P}_2\mathbf{BK}_p$ and $\mathbf{Y} = \mathbf{P}_2\mathbf{BK}_d$, and defining the augmented state vector $\boldsymbol{\xi}(t) = \{\mathbf{x}(t), \mathbf{x}(t - \tau(t)), \mathbf{x}(t - \tau_M), \dot{\mathbf{x}}(t), \dot{\mathbf{x}}(t - \tau(t)), \mathbf{e}_k(t), \dot{\mathbf{e}}_k(t)\}$, the Schur complement lemma is applied to handle the higher-order coupling matrices $\eta_1\mathbf{P}_2\mathbf{P}_2^T$ and $\eta_2\lambda^2\mathbf{P}_2\mathbf{P}_2^T$. Consequently, the total energy evolution rate can be bounded as

$$\dot{V}(t) + 2\delta V(t) \leq \boldsymbol{\xi}^T(t)\boldsymbol{\Xi}\boldsymbol{\xi}(t) + c_t + e^{-2\delta\tau_M}\mu_0 \quad (28)$$

When the LMI condition (21) strictly holds ($\Phi < 0$), it yields the differential inequality $\dot{V}(t) \leq -2\delta V(t) + c_t + e^{-2\delta\tau_M}\mu_0$. Integrating this inequality over the time interval ensures that the system energy satisfies the ultimate boundedness, which completes the proof.

We further discuss the conservatism and feasibility characteristics of the derived LMI conditions in the following remark. $\square$

Remark 4. It is crucial to clarify the logical chain guaranteeing the boundedness of the lumped disturbance $\boldsymbol{\omega}(t)$ to avoid circular reasoning in the presence of non-Lipschitz dynamics. To strictly guarantee that the states remain within the compact region required for the neural network approximation, the proof relies on the concept of positively invariant Lyapunov level sets.

Based on the constructed Lyapunov–Krasovskii functional $V(t)$, we define a closed sublevel set $\boldsymbol{\Omega}_V = \{\zeta \mid V(\zeta) \leq \bar{V}\}$, where $\bar{V}$ is determined by both the initial condition $V(0)$ and the ultimate bound induced by the LMI conditions. The derived LMI feasibility conditions ensure that $\dot{V}(t)$ is negative definite outside a compact neighborhood of the origin, which guarantees that all trajectories starting from admissible initial conditions remain confined within the invariant set $\boldsymbol{\Omega}_V$ for all $t \geq 0$.

Provided that the neural network operating domain Ω chosen is sufficiently large such that $\boldsymbol{\Omega}_V \subset \Omega$, the system states never escape this valid approximation region. Consequently, by the Weierstrass Extreme Value Theorem, all continuous nonlinear terms evaluated over this compact set admit finite upper bounds.

This rigorously establishes the constant bound μ_A throughout the system evolution, thereby eliminating any circular dependence in the derivation.

3.7. Exclusion of Zeno Behavior

To guarantee the physical realizability of the proposed observer-based SETM scheme in practical engineering networks, it is mathematically mandatory to prove that the time interval between any two consecutive triggering events is strictly bounded away from zero.

Based on the definition of the triggering error $\mathbf{e}_k(t) = \hat{\mathbf{x}}(t_k) - \hat{\mathbf{x}}(t)$, its derivative with respect to time during the triggering interval $t \in [t_k, t_{k+1})$ satisfies

$$\frac{d}{dt} \|\mathbf{e}_k(t)\| \leq \|\dot{\mathbf{e}}_k(t)\| = \|\dot{\hat{\mathbf{x}}}(s_i)\| \quad (29)$$

Benefiting from the UUB convergence of the closed-loop system states proved in Theorem 1 and the stability of the state observer, the first-order derivative of the reconstructed state vector is globally bounded. Thus, there exists a positive constant $\kappa > 0$ such that $\|\dot{\hat{\mathbf{x}}}(s_i)\| \leq \kappa$ holds persistently. Integrating both sides of (29) over the interval $[t_k, t]$ with the initial condition $e_k(t_k) = 0$ yields

$$\|\mathbf{e}_k(t)\| \leq \int_{t_k}^t \|\dot{\hat{\mathbf{x}}}(s_i)\| ds \leq \kappa(t - t_k) \quad (30)$$

According to the static triggering condition, when the next transmission instant t_{k+1} is activated, it must satisfy the boundary condition $\|\mathbf{e}_k(t_{k+1})\| > \sqrt{\rho} \|\hat{\mathbf{x}}(t_{k+1})\|$. Combining this boundary condition with the integration inequality (30), the minimum time execution interval can be derived as

$$t_{k+1} - t_k \geq \frac{\sqrt{\rho} \|\hat{\mathbf{x}}(t_{k+1})\|}{\kappa} \quad (31)$$

Furthermore, since the proposed discrete event-triggered communication scheme (DECS) performs the threshold evaluation exclusively at the hardware's periodic sampling points $s_i = s_0 + ih$, the hardware logic enforces an absolute physical floor on the transmission interval:

$$\inf_{k \in \mathbb{N}} (t_{k+1} - t_k) \geq h > 0 \quad (32)$$

Therefore, based on both the discrete-time event generation mechanism and the sampling-based implementation framework, an infinite number of triggering events within any finite time interval is strictly precluded. Consequently, Zeno behavior is excluded by construction, under all admissible DoS attack scenarios and in the presence of bounded state fluctuations.

4. Simulation Experiments

4.1. Simulation Environment and Physical System Parameters

To objectively verify the secure control performance of the proposed MNN-based high-gain observer under the dual constraints of DoS attacks and non-Lipschitz dynamics, a class of two-link rigid manipulators with strong nonlinear coupling characteristics is employed for numerical simulation in this section. Distinct from nonlinear systems satisfying the global Lipschitz assumption, the considered two-link rigid manipulator contains quadratic velocity-coupling terms and non-smooth friction effects. For example, the Coriolis and centrifugal dynamics include terms proportional to products of joint velocities, such as $\dot{\mathbf{q}}_1 \dot{\mathbf{q}}_2$ and $\dot{\mathbf{q}}_2^2$.

These nonlinear terms exhibit polynomial growth with respect to the system states. Consequently, the corresponding Jacobian matrix contains state-dependent components whose magnitudes increase without bound as the joint velocities increase. Therefore, no finite global Lipschitz constant exists for the overall nonlinear dynamics.

Although the system trajectories are constrained within a compact operating region according to Assumption 1, the nonlinear dynamics remain globally non-Lipschitz. Conventional observer-based methods typically require explicit knowledge of a global Lipschitz constant to derive observer error bounds and stability conditions. In practical systems with velocity-coupling nonlinearities and friction effects, obtaining such a constant is difficult and often leads to overly conservative observer gains. This motivates the use of the proposed MNN-assisted observer framework, which avoids relying on a known global Lipschitz bound.

The rotational dynamics of the two-link manipulator can be modeled by the following equation:

$$\mathbf{D}(\mathbf{q})\ddot{\mathbf{q}} + \mathbf{C}(\mathbf{q}, \dot{\mathbf{q}})\dot{\mathbf{q}} + \mathbf{G}(\mathbf{q}) + \mathbf{F}_r(\dot{\mathbf{q}}) = \boldsymbol{\tau} \quad (33)$$

where $\mathbf{q} = [q_1, q_2]^T \in \mathbb{R}^2$ and $\dot{\mathbf{q}} = [\dot{q}_1, \dot{q}_2]^T \in \mathbb{R}^2$ represent the joint angular position and angular velocity vectors, respectively. The specific physical expressions for the parameter matrices and vectors of the system are defined as follows.

The inertia matrix $\mathbf{D}(\mathbf{q}) \in \mathbb{R}^{2 \times 2}$ is a symmetric positive definite matrix, with its elements given by

$$\begin{aligned} D_{11}(q) &= (m_1 + m_2)r_1^2 + m_2r_2^2 + 2m_2r_1r_2\cos(q_2) \\ D_{12}(q) &= D_{21}(q) = m_2r_2^2 + m_2r_1r_2\cos(q_2) \\ D_{22}(q) &= m_2r_2^2 \end{aligned} \quad (34)$$

The control input torque vector is $\boldsymbol{\tau} = [\tau_1, \tau_2]^T \in \mathbb{R}^2$. In this system, it is assumed that only the joint position information can be measured in real time by sensors, meaning that the output equation is $\mathbf{y} = \mathbf{q}$. Furthermore, the physical parameters regarding the link lengths, masses, and gravitational acceleration are specifically set as: $r_1 = 1.0$ m, $r_2 = 0.8$ m; $m_1 = 1.0$ kg, $m_2 = 1.5$ kg; and $g = 9.8$ m/s². The friction coefficients are set to $f_{v1} = f_{v2} = 0.5$ and $f_{c1} = f_{c2} = 0.1$.

To further verify the feasibility of the proposed LMI conditions, numerical evaluations were conducted under different delay bounds, DoS intensities, and communication thresholds, and feasible solutions were successfully obtained within the admissible parameter region.

To implement the proposed discrete event-triggered communication scheme (DECS) and feedback control under adversarial conditions, the network and controller parameters are configured based on the theoretical constraints derived in Theorem 1.

The base hardware discrete sampling period is chosen as $h = 0.01$ s. The communication channel is subject to intermittent DoS attacks, where the maximum duration of a single attack interval is strictly bounded by $T_{DoS} = 0.2$ s. The maximum number of allowable consecutive unsent sampling steps for the SETM is set to $L = 4$. Consequently, the closed-loop system operates under a unified maximum communication delay bound of $\tau_M = (1 + 4) \times 0.01 + 0.2 = 0.25$ s.

For the SETM threshold rule, the relative threshold parameter is selected as $\rho = 0.05$, and the positive steady-state relaxation constant is set to $\mu_0 = 0.01$ to prevent unnecessary trigger chatter near the equilibrium point. The tuning parameter for the observer high gain is set to $\theta = 15$. By solving the LMI conditions presented in Theorem 1 via the YALMIP toolbox with the SeDuMi solver, the optimal triggering weighting matrix $\boldsymbol{\Omega}$ and the discrete-time state feedback PD control gains $\mathbf{K}_p, \mathbf{K}_d$ are successfully obtained.

4.2. Simulation Results and Analysis

To comprehensively verify the effectiveness of the proposed strategy in handling non-Lipschitz dynamics, minimizing communication bandwidth consumption, and defending against DoS attacks, an initial state estimation deviation is introduced in the closed-loop

simulation. A thorough comparison is conducted against the standard high-gain observer (Standard HGO) operating under conventional periodic sampling mechanisms. Figures 1–4 illustrate the closed-loop tracking and estimation behaviors under a random but bounded DoS attack sequence (represented by the gray shaded areas). Note that the proposed MNN-based high-gain observer is labeled as “EHGO” in the legends for brevity.

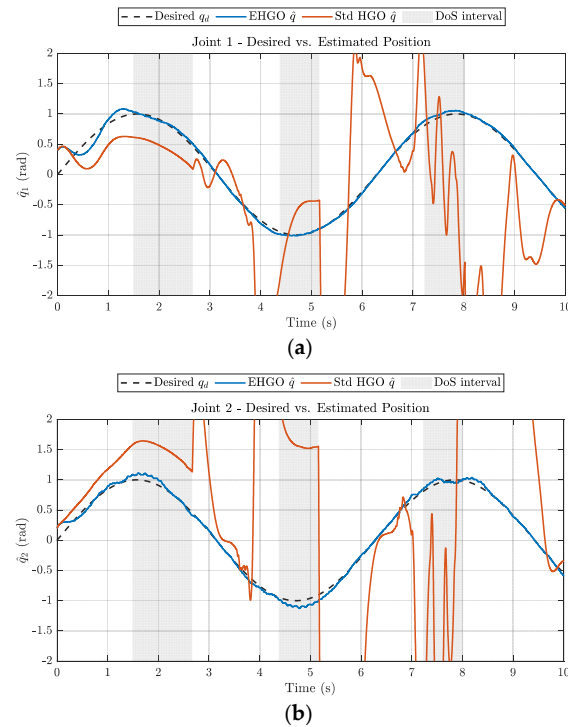


Figure 1. Trend of the system desired trajectories and the estimated positions under DoS attacks. (a) Position tracking performance of Joint 1; (b) position tracking performance of Joint 2.

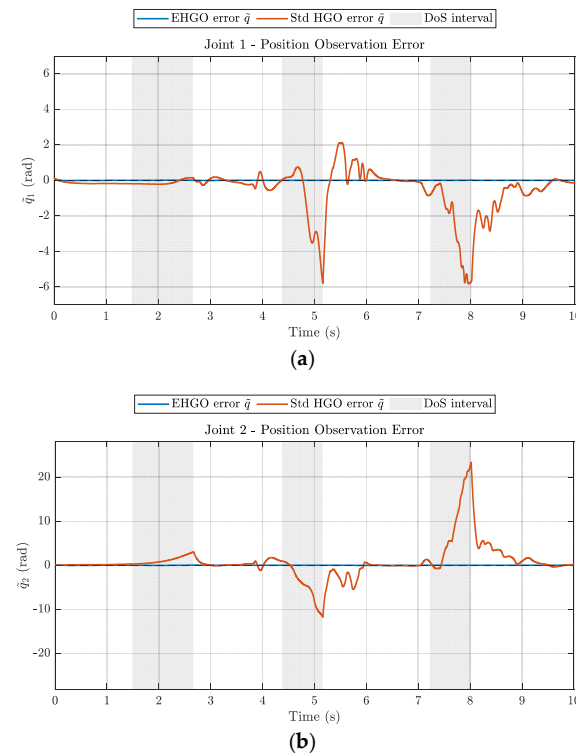


Figure 2. Evolution of the state observation errors. (a) Position observation error of Joint 1; (b) position observation error of Joint 2.

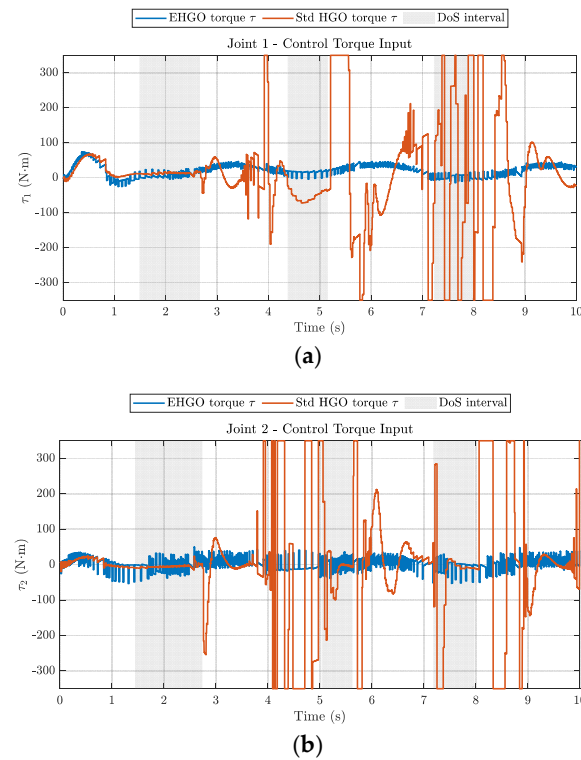


Figure 3. Control torque input of the closed-loop system. (a) Control torque applied to Joint 1; (b) control torque applied to Joint 2.

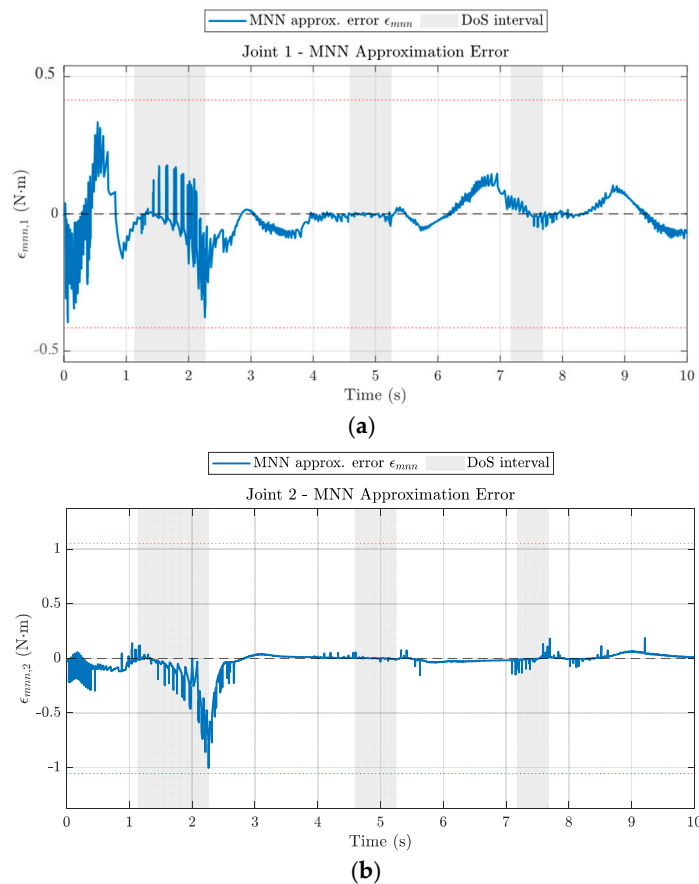


Figure 4. Approximation error of the multi-layer neural network. (a) Approximation error associated with the dynamics of Joint 1; (b) approximation error associated with the dynamics of Joint 2.

As shown in Figures 1 and 2, during the initial transient phase, both observers exhibit fluctuations due to the injected initial errors, but they rapidly achieve convergence under the high-gain injection structure. However, during the DoS attack intervals where sensor data transmission is completely severed, the Standard HGO completely loses its measurement feedback baseline. Lacking an internal compensation mechanism for the non-Lipschitz Coriolis forces and non-smooth friction, its observation errors diverge rapidly. In sharp contrast, the proposed EHGO locks the last valid states via the zero-order hold (ZOH) and utilizes the multi-layer neural network (MNN) to provide high-precision virtual feedforward dynamic compensation. Throughout the network outage blocks, its tracking errors remain strictly bounded within a minute neighborhood of zero, demonstrating strong resilience against DoS attacks.

Figure 3 illustrates the control torque input of the closed-loop system. For the system utilizing the Standard HGO, significant torque variations and noticeable high-frequency oscillations are observed at the exact instances when communication recovers (e.g., when an attack ends). This is caused by the sudden injection of huge accumulated state estimation errors into the feedback loop, which severely risks actuator saturation and physical component wear. Conversely, because the proposed EHGO effectively suppresses error divergence during disconnection periods, its control torque under the SETM framework remains smooth and stable across all switching boundaries. The distinctive step-like shape in the torque curves of the proposed method perfectly reflects the characteristics of the hold-input strategy and the event-triggered transmission, which is beneficial for practical implementation.

Figure 4 verifies the approximation performance of the MNN. The results confirm that the MNN ensures the strict boundedness of the approximation error even in scenarios with non-smooth friction and unbounded growth characteristics, functioning effectively as a local virtual dynamic engine.

To explicitly quantify the communication-saving efficiency of the proposed static event-triggered mechanism, Figures 5 and 6 depict the real-time distribution of the triggering instants and the corresponding time-varying execution intervals.

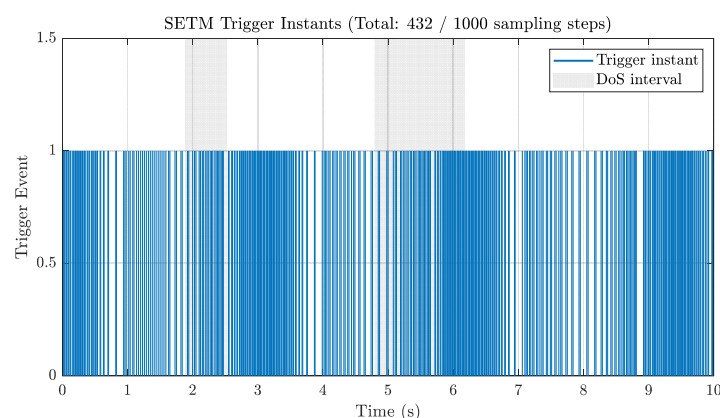


Figure 5. Distribution of the static event trigger instants over the simulation period.

It is worth noting that to ensure high-precision tracking of the fast-varying sinusoidal reference trajectories under the coupled influence of non-Lipschitz dynamics and external disturbances, the SETM maintains a necessary transmission frequency. Statistical data reveals that out of the 1000 total sampling steps within the 10 s simulation duration, the proposed mechanism actively executes exactly 432 transmissions. Although the system allocates 43.2% of the communication instances to preserve physical tracking performance against aggressive dynamic variations, it still successfully cuts down redundant network traffic by 56.8% compared to the traditional periodic time-triggered paradigm. Further-

more, the varying inter-event intervals shown in Figure 6 frequently exceed the basic hardware sampling step (reaching up to 0.11 s), validating that the proposed secure control scheme can effectively and autonomously balance network traffic congestion and physical tracking accuracy.

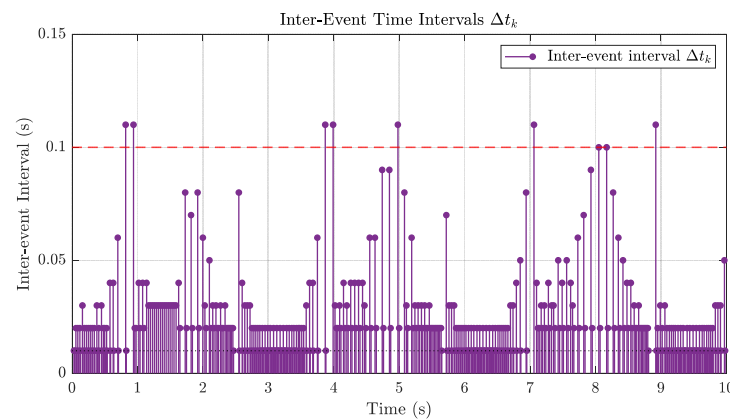


Figure 6. Evolution of the inter-event time intervals between consecutive successful transmissions.

To evaluate the tradeoff between communication efficiency and closed-loop performance, Table 1 presents a comparison between the proposed SETM-based method and a standard periodic sampling scheme under DoS attacks, where the Integral of Time-weighted Absolute Error (ITAE) is used as the performance metric. The results show that, compared with periodic sampling (1000 transmissions, average interval 10.0 ms, ITAE 60.9988), the proposed method with $\rho = 0.10$ reduces the number of transmissions to 423 and increases the average inter-event interval to 23.6 ms, while significantly lowering the ITAE to 2.8613. As the triggering threshold ρ increases, a slight degradation in tracking performance is observed, with ITAE gradually increasing from 2.8393 to 3.1670, while the communication statistics remain relatively stable. Overall, the results indicate that the proposed SETM provides an effective and tunable mechanism to balance communication load and tracking performance under DoS conditions.

Table 1. Generating quantitative tradeoff table data (periodic vs. SETM).

Threshold	Total Transmissions	Avg Interval (ms)	ITAE
Periodic (Std)	1000	10.0	60.9988
SETM $\rho = 0.05$	423	23.6	2.8393
SETM $\rho = 0.10$ (B)	423	23.6	2.8613
SETM $\rho = 0.15$	428	23.4	3.0033
SETM $\rho = 0.20$	429	23.3	3.1670

While the simulation study specifically utilizes a two-link rigid manipulator to illustrate the proposed method, the theoretical stability conditions established in Theorem 1 are fundamentally independent of this specific physical model. Consequently, the proposed LMI-based resilient observer and event-triggered control framework can be extended to a broader class of non-Lipschitz nonlinear systems, provided that the system trajectories remain confined within a compact operating region where the multi-layer neural network (MNN) approximation is valid.

However, it is worth noting that the practical effectiveness of the proposed framework may be influenced by certain system characteristics. For high-dimensional systems,

the computational complexity of the neural network increases accordingly, which may introduce additional computational burden and affect real-time implementation of the event-triggered mechanism. In addition, the validity of the MNN approximation relies on the assumption that system states remain within a predefined compact set. If the system is subjected to severe or unmodeled disturbances that drive the states outside this region, the approximation accuracy may degrade, which may lead to performance deterioration of the observer and control scheme.

5. Conclusions

In this paper, a secure observer-based feedback control framework has been developed for networked nonlinear systems subject to non-Lipschitz dynamics and intermittent DoS attacks. By utilizing multi-layer neural networks (MNNs), the proposed high-gain observer (EHGO) achieves robust state estimation in the presence of unknown nonlinearities and measurement loss. A static event-triggered mechanism (SETM) with a hold-input strategy is further introduced to improve communication efficiency.

Stability analysis based on the Lyapunov–Krasovskii functional approach shows that the closed-loop system is uniformly ultimately bounded (UUB) under the derived LMI-based sufficient conditions, explicitly accounting for non-Lipschitz nonlinearities, sampling effects, and DoS-induced disruptions.

Simulation results on a two-link rigid manipulator indicate that the proposed framework achieves satisfactory tracking performance under various DoS attack intensities, while reducing communication load by 56.8% compared with periodic sampling. These results verify the effectiveness and robustness of the proposed framework in resource-constrained cyber–physical systems.

Future work will focus on adaptive event-triggered mechanisms and the extension of the proposed framework to multi-agent systems. In addition, comparisons with advanced resilient estimation and control strategies, including adaptive observers, neural-network-based observers, and dynamic event-triggered or DoS-resilient observer designs, will be further investigated.

Author Contributions: Conceptualization, Q.Z. and H.Z.; methodology, Q.Z., D.L. and H.Z.; software, D.L.; validation, D.L., H.Z. and C.B.; formal analysis, D.L. and H.Z.; writing—original draft preparation, D.L.; writing—review and editing, H.Z. and C.B.; supervision, Q.Z.; funding acquisition, Q.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China, grant numbers 62333010 and 62203214.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Ren, H.; Liu, Z.; Liang, H.; Li, H. Pinning-Based Neural Control for Multiagent Systems with Self-Regulation Intermediate Event-Triggered Method. *IEEE Trans. Neural Netw. Learn. Syst.* **2025**, *36*, 7252–7262. [PubMed]
2. Cheng, Y.; Niu, B.; Zhao, X.; Zong, G.; Ahmad, A.M. Event-triggered adaptive decentralised control of interconnected nonlinear systems with Bouc-Wen hysteresis input. *Int. J. Syst. Sci.* **2023**, *54*, 1275–1288.
3. Gao, Z.; Zhao, N.; Zhao, X.; Niu, B.; Xu, N. Event-triggered prescribed performance adaptive secure control for nonlinear cyber physical systems under denial-of-service attacks. *Commun. Nonlinear Sci. Numer. Simul.* **2024**, *131*, 107793.
4. Tong, S.; Zhou, H.; Li, Y. Neural Network Event-Triggered Formation Fault-Tolerant Control for Nonlinear Multiagent Systems with Actuator Faults. *IEEE Trans. Syst. Man Cybern.-Syst.* **2023**, *53*, 7571–7582. [CrossRef]

5. Wang, X.; Xu, R.; Huang, T.; Kurths, J. Event-Triggered Adaptive Containment Control for Heterogeneous Stochastic Nonlinear Multiagent Systems. *IEEE Trans. Neural Netw. Learn. Syst.* **2024**, *35*, 8524–8534. [[CrossRef](#)] [[PubMed](#)]
6. Liu, Y.; Zhu, Q.; Wen, G. Adaptive Tracking Control for Perturbed Strict-Feedback Nonlinear Systems Based on Optimized Backstepping Technique. *IEEE Trans. Neural Netw. Learn. Syst.* **2022**, *33*, 853–865. [[CrossRef](#)] [[PubMed](#)]
7. Ullah, K.; Guzinski, J.; Mirza, A.F. Critical Review on Robust Speed Control Techniques for Permanent Magnet Synchronous Motor (PMSM) Speed Regulation. *Energies* **2022**, *15*, 1235. [[CrossRef](#)]
8. Hu, L.-X.; Li, Y.-X. Dynamic Event-Triggered Prescribed Performance Optimal Secure Control for Nonlinear Systems Under DoS Attacks. *Int. J. Robust Nonlinear Control* **2026**, *36*, 5044–5060. [[CrossRef](#)]
9. Cao, L.; Yao, D.; Li, H.; Meng, W.; Lu, R. Fuzzy-based dynamic event triggering formation control for nonstrict-feedback nonlinear MASs. *Fuzzy Sets Syst.* **2023**, *452*, 1–22. [[CrossRef](#)]
10. Jose, J.T.; Wratt, G.; Mishra, S.K.; Ranjan, P.; Das, J. Fuzzy PD-Based Control for Excavator Boom Stabilization Using Work Port Pressure Feedback. *Actuators* **2025**, *14*, 336. [[CrossRef](#)]
11. Lin, X.; Xu, R.; Yao, W.; Gao, Y.; Sun, G.; Liu, J.; Peretti, L.; Wu, L. Observer-Based Prescribed Performance Speed Control for PMSMs: A Data-Driven RBF Neural Network Approach. *IEEE Trans. Ind. Inform.* **2024**, *20*, 7502–7512. [[CrossRef](#)]
12. Song, X.; Sun, P.; Song, S.; Stojanovic, V. Finite-time adaptive neural resilient DSC for fractional-order nonlinear large-scale systems against sensor-actuator faults. *Nonlinear Dyn.* **2023**, *111*, 12181–12196.
13. Fei, J.; Liu, L. Fuzzy Neural Super-Twisting Sliding-Mode Control of Active Power Filter Using Nonlinear Extended State Observer. *IEEE Trans. Syst. Man Cybern.-Syst.* **2024**, *54*, 457–470. [[CrossRef](#)]
14. Zhao, N.; Lun, D.; Zhang, H.; Zhao, X.; Rudas, I.J. Composite Anti-Disturbance Control for Networked Systems with Disturbances and Actuator Attacks via Event-Triggered Output Feedback. *IEEE Trans. Cybern.* **2026**, *56*, 393–403. [[PubMed](#)]
15. Ma, S.; Li, K.; Li, Y.; Ning, J. Dynamic Event-Triggered Distributed Formation Control for Harbor Unmanned Container Transporter Platoon Under Dos Attacks. *Int. J. Robust Nonlinear Control* **2026**, *36*, 1413–1429.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.