mathematics

MDPI

Article

Estimate-Based Dynamic Memory-Event-Triggered Control for Nonlinear Networked Control Systems Subject to Hybrid Attacks

Bo Zhang [1], Tao Zhang [1], Zesheng Xi [1], Yunfan Wang [1] and Meng Yang [2,3,*]

[1] State Grid Laboratory of Power Cyber-Security Protection and Monitoring Technology, China Electric Power Research Institute, Nanjing 210003, China; zhangbo6@epri.sgcc.com.cn (B.Z.); zhangtao@epri.sgcc.com.cn (T.Z.); xizesheng@njust.edu.cn (Z.X.); 230240007@seu.edu.cn (Y.W.)
[2] College of Command Control Engineering, Army Engineering University of PLA, Nanjing 210007, China
[3] School of Automation, Southeast University, Nanjing 210096, China
* Correspondence: mengyang9505@163.com

Abstract

Within the framework of a dynamic memory-event-triggered mechanism (DMETM), this paper proposes an estimate-based secure control algorithm for nonlinear networked control systems (NNCSs) that suffer from hybrid attacks. Firstly, a sampled-data observer is employed utilizing the output signals to estimate the states. Secondly, due to the limitation of data transmission capacity in NNCSs, a novel DMETM with auxiliary variable is proposed, which effectively leverages the benefits of historical sampled data. In the process of network data transmission, a hybrid attack model that simultaneously considers the impact of both deception and denial of service (DoS) attacks is introduced, which can undermine signal integrity and disrupt data transmission. Then, a memory-event-triggered controller is developed, and the mean square stability of the NNCSs can be ensured by selecting some appropriate values. Finally, a numerical simulation and a practical example are given to illustrate the meaning of the designed dynamic memory-event-triggered control (DMETC) algorithm.

Keywords: nonlinear networked control systems; event-triggered control; hybrid attacks; observer; secure control

MSC: 34H05

check for updates

Academic Editor: Huaizhong Zhao

Received: 16 July 2025
Revised: 15 August 2025
Accepted: 19 August 2025
Published: 2 September 2025

Citation: Zhang, B.; Zhang, T.; Xi, Z.; Wang, Y.; Yang, M. Estimate-Based Dynamic Memory-Event-Triggered Control for Nonlinear Networked Control Systems Subject to Hybrid Attacks. *Mathematics* **2025**, *13*, 2829. https://doi.org/10.3390/math13172829

Copyright: © 2025 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) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

It is well known that nonlinear networked control systems (NNCSs) gained considerable interest because of their efficient integration of nonlinear dynamics and network communication capabilities. These systems are widely applied in various fields, including industrial automation, smart grids, robotics, and intelligent transportation systems [1–4]. In general, the use of networked communication facilitates remote control and real-time adjustments, which significantly enhances the system reliability and efficiency [5–7]. Despite these advantages, NNCSs can be limited by constrained bandwidth and potential cyber-attacks, which necessitate the development of advanced control strategies to maintain system stability and performance.

The traditional time-triggered mechanism results in the transmission of redundant signals, even when the system has already achieved the desired control objective, thereby causing unnecessary resource consumption. To overcome this issue, an event-triggered mechanism (ETM) that can reduce the signal transmission rate has garnered significant

attention from researchers [8–11]. Recent advancements in event-triggered control have achieved significant results in several areas, including predictive control, H_∞ control, and output feedback control [12]. Based on these developments, a memory-event-triggered mechanism is introduced to improve communication resource utilization by utilizing historical sampled data [13,14]. Compared to traditional ETM, the memory-event-triggered scheme can reduce unnecessary data transmission during unexpected system fluctuations and improve data update efficiency when changes are smooth near critical troughs. For example, a memory event-triggered finite-time lane-keeping control strategy was designed for autonomous heavy trucks in [15]. A load frequency control problem of power systems is addressed in [16], where the adaptive-memory ETM was presented to optimize resource utilization. Moreover, dynamic ETM can further reduce bandwidth usage by adjusting the auxiliary variable or dynamic threshold [17–20]. For instance, a data-driven control of nonlinear systems under dual-channel memory ETM was studied in [21]. An anti-disturbance control method for switched cyber-physical systems was proposed in [22], where DMETM was considered. It should be noted that studying DMETM is crucial for optimizing resource utilization while maintaining system stability and performance.

In NNCSs, data transmission is not only constrained by limited bandwidth resources but also potentially threatened by cyber-attacks, both of which collectively impact the stability and security of the systems. Concerning cyber-attacks, the recent literature introduces most security control methods for NNCSs [23–26]. Cyber-attacks on NNCSs are generally divided into three main primary types: DoS attacks, replay attacks, and deception attacks [27]. Specifically, DoS attacks aim to disrupt data transmission by intentionally dropping or blocking data packets during the communication process, thereby preventing the normal exchange of information between system components. Replay attacks involve the interception and retransmission of previously captured data packets, which can mislead the system into making incorrect decisions based on outdated information. Deception attacks involve the injection of false or malicious data into the system, potentially leading to severe safety hazards. Despite these advancements, most existing research primarily focuses on addressing a single type of attack, with limited attention given to the more complex and realistic scenario of hybrid attacks, where multiple attack types may occur simultaneously or sequentially [28,29]. For example, the problem of discrete proportion–integration–differentiation control was coped with in [29] for interconnected power systems with hybrid attacks. In [30], a cooperative resilient control strategy was designed for energy storage systems with hybrid attacks, where false data injection and DoS attacks were taken into account.

Based on the above discussion, in the presence of hybrid attacks, two key challenges should be tackled: (1) how to jointly develop a DMETM and observer to estimate the output signals when the full system states are unavailable; (2) how to formulate the estimate-based dynamic memory-event-triggered control (DMETC) approach to obtain the mean square stability of NNCSs when the communication network is subjected to hybrid attacks. To overcome these challenges, an estimate-based DMETC is designed in this paper for NNCSs subject to hybrid attacks. The main contributions are summarized as follows:

1. By virtue of auxiliary variable and past sampled-data, this paper proposes DMETM, which offers a more effective balance between communication utilization and control performance in comparison to the traditional ETM with fixed threshold [8–10].
2. This paper considers a hybrid attack model that incorporates both DoS attacks and deception attacks. This control approach is more general than those considered in previous works [26,27], which primarily focused on single-attack scenarios.
3. Both the designed DMETM and memory-event-triggered output feedback controller are formulated in discrete time. This means that only the system output data are nec-

essary for the joint design of the memory-event-triggered controller and the DMETM, which makes the approach more practical and applicable to the actual system.

The structure of this paper is outlined as follows: Sections 2 and 3 present the problem formulation and the procedure for designing the estimate-based DMETC. Section 4 provides the stability analysis, and Section 5 demonstrates the effectiveness of the designed estimate-based DMETC approach through two examples. Section 6 reaches the conclusion of the designed results.

Notations: $\mathbb{N}$ and $\mathbb{R}$ stand for the sets of non-negative numbers and real numbers. $W \in \mathbb{R}^{n\times m}$ and W^T refer to the set of the $n \times m$ real matrix and the transpose of W. When $W = W^T \in \mathbb{R}^{m\times m}$, $\lambda_{\min}(W)$ and $\lambda_{\max}(W)$ denote the minimum and the maximum eigenvalues of W, respectively. $\|\cdot\|$ and I represent the 2-norm and the identity matrix.

2. Problem Formalization

As illustrated in Figure 1, the proposed estimate-based DMETC framework integrates the plant, the sampled-data state observer, the DMETM, and the memory-event-triggered controller. The DMETM exploits historical sampled data to reduce communication load, while hybrid attacks, including deception and DoS attacks, are modeled on the communication channel to represent threats to signal integrity and reliability.

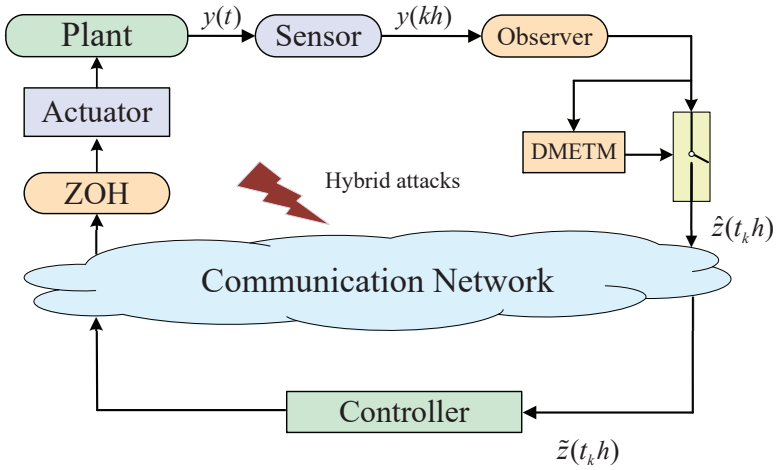


Figure 1. The configuration of estimate-based DMETC for NNCSs under hybrid attacks.

System Model

Consider an NNCS as follows:

$$\begin{cases} \dot{x}_i = x_{i+1} + f_i(\tilde{x}_i), 1 \le i \le n-1, \\ \dot{x}_n = u + f_n(x), \\ y = x_1 \end{cases} \tag{1}$$

where $x = [x_1, \ldots, x_n]^T \in \mathbb{R}^n$, $\tilde{x}_i = [x_1, \ldots, x_i]^T \in \mathbb{R}^i$, $u \in \mathbb{R}$, and $y \in \mathbb{R}$ refer to the state, control input, and system output; $f_i, i = 1, 2, \ldots, n$ stands for the nonlinear terms.

Motivated by [31], the following assumption on nonlinear uncertain terms is used.

Assumption 1. *For the nonlinear uncertain terms $f_i(t), i = 1, 2, \ldots, n$, there exists a constant $c_0 > 0$ such that*

$$|f_i(\tilde{x}_i)| \le c_0(|x_1| + \cdots + |x_i|). \tag{2}$$

Based on Assumption 1, this paper addresses the estimate-based DMETC issue for system (1) subject to hybrid attacks when only the output signals are available. By establishing sufficient conditions, the mean square stability of the NNCSs can be guaranteed while simultaneously minimizing the number of events to the greatest extent possible.

Define the following variables:

$$z_i = \frac{x_i}{\iota^{i-1}}, v = \frac{u}{\iota^n}, i = 1, 2, \ldots, n.$$

Then, (1) can be further described as

$$\begin{cases} \dot{z} = \iota A_0 z + \iota B_0 v + \tilde{f}(z), \\ y = C_0 z \end{cases} \tag{3}$$

where $z = [z_1, \ldots, z_n]^T$, $\tilde{f}(z) = [\frac{f_1}{\iota^0}, \ldots, \frac{f_n}{\iota^{n-1}}]^T$, $A_0 = \begin{bmatrix} 0_{(n-1)\times 1} & I_{(n-1)\times(n-1)} \\ 0 & 0_{1\times(n-1)} \end{bmatrix}$, $B_0 = \begin{bmatrix} 0_{(n-1)\times 1} \\ 1 \end{bmatrix}$, $C_0 = \begin{bmatrix} 1 & 0_{1\times(n-1)} \end{bmatrix}$.

3. Estimate-Based DMETC Design Against Hybrid Attacks

In this section, the aim of this study is to develop an estimate-based DMETC strategy for NNCSs (3), which includes three parts: (1) A sampled-data observer is presented to estimate the output, and a DMETM with dynamic variable is established to alleviate bandwidth pressure. (2) A hybrid attacks model encompassing DoS and deception attacks is considered, which has an impact on the transmission signals. (3) According to the hybrid attacks and the DMETM, a memory-event-triggered output feedback tracking controller is proposed.

3.1. Sampled-Data Observer Design

Let h, $\{t_k h\}_{k\in\mathbb{N}}$, and $t_{k,g}h = t_k h + gh$, $g = 1, 2, \ldots$ be the sampling period, the set of event-triggered instants, and the sampling instants, respectively. Based on (3), a sampled-data observer is built for $t \in [t_{k,g}h, t_{k,g+1}h)$

$$\dot{\hat{z}}(t) = \iota A_0 \hat{z}(t) + \iota B_0 v(t) + \iota H(y(t_{k,g}h) - C_0 \hat{z}(t)) \tag{4}$$

where $\hat{z}(t) = [\hat{z}_1(t), \ldots, \hat{z}_n(t)]^T$ stands for the estimate of $z(t)$, and $H = [h_1, \ldots, h_n]^T$ refers to the observer parameters.

Define the following estimation error: $e_i = z_i - \hat{z}_i, i = 1, \ldots, n$. With help of (3) and (4), the estimation error system is expressed as

$$\dot{e}(t) = \iota A_0 e(t) + \tilde{f}(z(t)) - \iota H(y(t_{k,g}h) - C_0 \hat{z}(t)), t \in [t_{k,g}h, t_{k,g+1}h) \tag{5}$$

where $e = [e_1, \ldots, e_n]^T$.

3.2. DMETM Design

By applying the average of historical system output, a DMETM is employed to decide whether the estimated signals should be released to a remote controller. Define

$$\mathbb{M}(t) = \sum_{m=1}^{\tilde{m}} \|\theta_m \epsilon_m(t)\| - \frac{\sigma}{\iota}\|\hat{z}(t_{k,g}h)\| - \frac{\eta}{\iota}\gamma(t_{k,g}h),$$
$$\epsilon_m(t) = \hat{z}(t_{k,g}h) - \hat{z}(t_{k-m+1}h)$$

where $\tilde{m}$ and $t_{k-m+1}h, m = 1, 2, \ldots, \tilde{m}$ stand for the maximum value of the historical event-triggered instant and the past event-triggered instant; θ_m denotes the weight of historical signals at instant $t_{k-m+1}h$; $\sigma \geq 0$, $\eta > 0$, $\gamma(t_{k,g}h)$ refers to the dynamic variable and satisfies the following adaptive law:

$$\dot{\gamma}(t) = -\bar{\eta}\gamma(t) + \frac{\sigma}{\iota}\|\hat{z}(t_{k,g}h)\| - \sum_{m=1}^{\tilde{m}} \|\theta_m \epsilon_m(t)\| \tag{6}$$

where $t \in [t_{k,g}h, t_{k,g+1}h)$, $\bar{\eta} > 0$, and $\gamma(0) \geq 0$ denote the initial condition. Then, the next triggered instant is determined by

$$t_{k+1}h = t_k h + \min_{g \geq 1} \Big\{ gh | \ \mathbb{M}(t) \geq 0 \Big\}. \tag{7}$$

Remark 1. *Different from memoryless ETM [17], the proposed DMETM (7) employs the average value of past data* $\sum_{m=1}^{\tilde{m}} \|\theta_m \epsilon_m(t)\|$ *with pre-assigned constant historical weights* θ_m*, where more recent event-triggered data are assigned larger weights, and older data receive smaller weights. This design emphasizes the influence of recent information, helping reduce unnecessary data transmissions caused by sudden changes in the system state while avoiding excessive sensitivity to outdated data. It should be noted that the historical information* $\hat{z}(t_{k-m+1}h)$ *is utilized in (7) to avoid unnecessary transmissions influenced by external factors.*

The subsequent lemma is employed to represent the key characteristics of the auxiliary variable $\gamma(t)$.

Lemma 1. *Consider the rule (6) with* $\gamma(0) \geq 0$*; if* $\eta > 0$ *and* $\bar{\eta} > 0$*, the sampling period h satisfies*

$$h < \frac{1}{\bar{\eta}} \ln\left(\frac{\iota\bar{\eta}}{\eta} + 1\right), \tag{8}$$

then, for all $t \in [0, \infty)$, $\gamma(t) \geq 0$ *holds.*

Proof. Based on the DMETM (7) that $\|\sum_{m=1}^{\tilde{m}} \theta_m \epsilon_m(t)\| \leq \frac{\sigma}{\iota}\|\hat{z}(t_{k,g}h)\| + \frac{\eta}{\iota}\gamma(t_{k,g}h)$, $\forall t \in [t_{k,g}h, t_{k,g+1}h)$. Integrating (6) from $t_{k,g}h$ to $t \in [t_{k,g}h, t_{k,g+1}h)$, one has

$$\begin{aligned}
\gamma(t) =& e^{-\bar{\eta}(t-t_{k,g}h)}\gamma(t_{k,g}h) + \int_{t_{k,g}h}^{t} e^{-\bar{\eta}(t-v)}dv\left(\frac{\sigma}{\iota}\|\hat{z}(t_{k,g}h)\| - \|\sum_{m=1}^{\tilde{m}} \theta_m \epsilon_m(t)\|\right) \\
\geq& e^{-\bar{\eta}(t-t_{k,g}h)}\gamma(t_{k,g}h) - \int_{t_{k,g}h}^{t} e^{-\bar{\eta}(t-v)}dv\frac{\eta\gamma(t_{k,g}h)}{\iota} \\
\geq& \left(e^{-\bar{\eta}h} - \frac{\eta(1-e^{-\bar{\eta}h})}{\iota\bar{\eta}}\right)\gamma(t_{k,g}h).
\end{aligned} \tag{9}$$

Taking (9) into consideration, it can be obtained that $\gamma(t) \geq 0$, where $t \in [t_{k,g}h, t_{k,g+1}h)$. Moreover, since $\gamma(t)$ is a continuous function, $\gamma(t^-_{k,g+1}h) = \gamma(t_{k,g+1}h)$, which implies that $\gamma(t_{k,g+1}h) \geq 0$. Obviously, it follows that $\gamma(t) \geq 0$, $\forall t \in [0, \infty)$. □

Remark 2. *For the proposed DMETM in (7), the inclusion of the dynamic variable* γ *enables potential noise attenuation, since the* γ *value can be interpreted as a filtered parameter of the error function* ϵ_m*. Unlike the traditional ETM with a fixed threshold [8,27], the DMETM (7) employs a more sophisticated triggering condition. This condition is inherently more challenging to satisfy due to the presence of the term* $\frac{\eta}{\iota}\gamma(t_{k,g}h)$*, which is always non-negative. As a result, the DMETM ensures that events are triggered only when significant changes occur, thereby reducing unnecessary transmissions and saving limited network resources.*

Remark 3. *In contrast to certain existing memory ETM approaches [13,14], the DMETM (7) in this paper is constructed based on the state estimates rather than relying on full states. The designed DMETM (7) incorporates three adjustable parameters: σ, η, and $\bar{\eta}$. By setting $\eta = 0$, the designed DMETM (7) simplifies to the conventional ETM [8]. Furthermore, when both σ and η are set to 0, the designed DMETM (7) simplifies to the time-triggered mechanism. Generally, smaller values of σ and η typically result in a higher transmission frequency, thereby improving the control performance. Therefore, it is crucial to carefully adjust these parameters to achieve an optimal trade-off between the transmission rate and the desired control performance.*

3.3. Hybrid Attacks

As depicted in Figure 1, the hybrid attacks studied in this paper consist of both deception and DoS attacks. Specifically, the deception attacks can tamper with the transmitted data and damage their integrity, while the DoS attacks can block the packets transmission, resulting in sampled signals being unable to reach the controller. When these two attacks occur simultaneously, the impact of the hybrid attacks exceeds that of a single attack, as it not only compromises the accuracy of the data but also disrupts its transmission.

The transmission signal affected by the hybrid attacks model is presented as

$$\tilde{z}(t_k h) = \beta_k(t)[\alpha_k(t)\hat{z}(t_k h) + (1-\alpha_k(t))g(\hat{z}(t_k h))] \tag{10}$$

where $g(\hat{z}(t_k h))$ stands for the nonlinear function created by deception attacks and satisfies $\|g(\hat{z}(t_k h))\| \leq c\|\hat{z}(t_k h)\|$, with $c > 0$. $\alpha_k(t) \in \{0,1\}$ and $\beta_k(t) \in \{0,1\}$ denote the Bernoulli distributed variable, with the associated probabilities given by

$$\begin{aligned} &\Pr\{\alpha_k(t) = 1\} = \bar{\alpha}_k, \Pr\{\alpha_k(t) = 0\} = 1 - \bar{\alpha}_k, \\ &\Pr\{\beta_k(t) = 1\} = \bar{\beta}_k, \Pr\{\beta_k(t) = 0\} = 1 - \bar{\beta}_k \end{aligned} \tag{11}$$

with $0 \leq \bar{\alpha}_k < 1$, and $0 \leq \bar{\beta}_k < 1$.

Remark 4. *According to (10), if $\beta_k(t) = 0$, this indicates that the sampled output suffers from DoS attacks. If $\beta_k(t) = 1$ and $\alpha_k(t) = 0$, the estimated signal $\hat{z}(t_k h)$ suffers from deception attacks, and the actual signal received by the controller is $g(\hat{Z}(t_k h))$. If $\beta_k(t) = 1$ and $\alpha_k(t) = 1$, this implies that the data are unaffected by the hybrid attacks and can reach the controller on time while maintaining its integrity.*

3.4. Output Feedback Controller Design

Based on (4) and (10), the control input $v(t)$ is defined by

$$v(t) = \iota^n u(t_k h) = -\iota^n \sum_{m=1}^{\tilde{m}} K\tilde{z}(t_{k-m+1} h), t \in [t_k h, t_{k+1} h) \tag{12}$$

where $K = [k_1, \ldots, k_n]$ denotes the controller parameters to be designed.

With the DMETM (7) and the hybrid attacks model (10) in mind, the event-triggered controller (12) is redesigned as

$$v(t) = -\sum_{m=1}^{\tilde{m}} \left[K\beta_k(t)\alpha_k(t)(\hat{z}(t_{k,g} h) - \epsilon_m(t)) + K\beta_k(t)(1-\alpha_k(t))g(\hat{z}(t_{k-m+1} h))\right] \tag{13}$$

where $t \in [t_{k,g} h, t_{k,g+1} h)$.

Then, combining (3) and (5), a closed-loop system is designed as

$$\begin{aligned}\dot{\rho}(t) =&\iota\Xi_1\rho(t) + \iota\Xi_2\sum_{m=1}^{\tilde{m}}\beta_k(t)\alpha_k(t)\epsilon_m(t) + F(z(t))\\ &- \iota\Xi_2\sum_{m=1}^{\tilde{m}}\beta_k(t)(1-\alpha_k(t))g(\hat{z}(t_{k-m+1}h))\\ &+ \iota\Xi_3\beta_k(t)\alpha_k(t)\rho(t_{k,g}h)) + \iota\Xi_4(z(t)-z(t_{k,g}h))\end{aligned} \tag{14}$$

where $t \in [t_{k,g}h, t_{k,g+1}h)$, $\rho = [z^T, e^T]^T$, $\Xi_1 = \begin{bmatrix} A_0 & 0 \\ 0 & A_0 - HC_0 \end{bmatrix}$, $\Xi_2 = \begin{bmatrix} B_0K \\ 0 \end{bmatrix}$, $\Xi_3 = \begin{bmatrix} B_0K \\ -B_0K \end{bmatrix}$, $\Xi_4 = \begin{bmatrix} 0 \\ HC_0 \end{bmatrix}$, $F(z(t)) = \begin{bmatrix} \tilde{f}(z(t)) \\ \tilde{f}(z(t)) \end{bmatrix}$.

4. Stability Analysis

To establish the stability analysis for the NNCSs, the following lemma is presented.

Lemma 2 ([31]). *Let $\vartheta : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}^n$. Consider the following differential equation:*

$$\dot{\vartheta}(j) = \mu(\vartheta(j), \vartheta(j_k)), \forall j \in [j_k, j_{k+1}), j_k = t_k h, k \in \mathbb{N}. \tag{15}$$

If $\mu(\vartheta(j), \vartheta(j_k))$ satisfies

$$\|\mu(\vartheta(j), \vartheta(j_k))\| \leq b_1(\|\vartheta(j) - \vartheta(j_k)\| + \|\vartheta(j_k)\|) \tag{16}$$

where b_1 denotes a positive constant; then, it holds that

$$\|\mu(\vartheta(j), \vartheta(j_k))\| \leq (e^{b_1(j-j_k)} - 1)\|\vartheta(j_k)\|, \forall j \in [j_k, j_{k+1}), k \in \mathbb{N}.$$

According to (14), there exists a positive matrix $P = P^T \in \mathbb{R}^{n\times n}$ such that $\Xi_1^T P + P\Xi_1 = -I$ holds, where Ξ_1 is a Hurwitz matrix. Then, the following theorem is presented to demonstrate the stability of NNCSs (14) under hybrid attacks.

Theorem 1. *Under Assumption 1, consider the NNCSs (3) subject to hybrid attacks and DMETM (7). If ι and h satisfy*

$$\bar{\omega} = \omega_1\lambda_{\min}(P) - 2\tilde{m}\|P\Xi_2\|\bar{\beta}_k(\bar{\alpha}_k + c(1-\bar{\alpha}_k))(\sigma+\eta) - 2\sigma > 0, \tag{17}$$

$$h < \Big\{\frac{1}{\bar{\eta}}\ln\Big(\frac{\iota\bar{\eta}}{\eta}+1\Big), \frac{1}{a_2}\ln\Big(1+\frac{\bar{\omega}}{\bar{\omega}_1}\Big)\Big\}, \tag{18}$$

where $a_1 = \frac{\eta\|\Xi_4\|}{a_2}$, $a_2 = \max\{\iota\|\Xi_1\| + \iota\|\Xi_2\| + c_1, \iota\|\Xi_1\| + \sigma\|\Xi_2\| + c_1\}$,

$$\begin{aligned}\bar{\omega}_1 =&\sqrt{2}c\tilde{m}\bar{\beta}_k(1-\bar{\alpha}_k)\|P\Xi_2\|(\iota+\sigma))(1+a_1) + 2(\sqrt{2}\tilde{m}\sigma\|P\Xi_2\|\bar{\beta}_k\bar{\alpha}_k + \iota\|P\Xi_4\|,\\ \omega_1 =&\min\{2\bar{\eta}, \frac{\iota - 2c_1\|P\| - 2\sqrt{2}\tilde{m}\sigma\|P\Xi_2\|\bar{\beta}_k\bar{\alpha}_k}{\lambda_{\max}(P)} - \frac{2\sqrt{2}c\tilde{m}\bar{\beta}_k(1-\bar{\alpha}_k)\|P\Xi_2\|(\iota+\sigma)}{\lambda_{\max}(P)}\} > 0,\\ \omega_2 =&\frac{2(\sqrt{2}\tilde{m}\sigma\|P\Xi_2\|\bar{\beta}_k\bar{\alpha}_k + \iota\|P\Xi_4\|)(1+a_1)(e^{a_2h}-1)}{\lambda_{\min}(P)}\\ &+ \frac{2\sqrt{2}c\tilde{m}\bar{\beta}_k(1-\bar{\alpha}_k)\|P\Xi_2\|(\iota+\sigma)(1+a_1)(e^{a_2h}-1)}{\lambda_{\min}(P)}\\ &+ \frac{2\tilde{m}\|P\Xi_2\|\bar{\beta}_k\eta(\bar{\alpha}_k + c(1-\bar{\alpha}_k)) + 2\sigma 2\iota\bar{\beta}_k\bar{\alpha}_k\|P\Xi_3\|}{\lambda_{\min}(P)},\end{aligned}$$

then, the system (14) is mean square stable.

Proof. For the system (14), construct the following Lyapunov function:

$$V(\tilde{\rho}) = \rho^T P \rho + \gamma^2 \tag{19}$$

where $\tilde{\rho} = [\rho^T, \gamma]^T$. Taking the mathematical expectation and derivation of $V(\tilde{\rho}(t))$ with respect to the (14) in the time interval $t \in [t_{k,g}h, t_{k,g+1}h)$ yields

$$\begin{aligned} E\{\mathfrak{L}V(\tilde{\rho}(t))\} \leq & -\iota\|\rho(t)\|^2 + 2\iota\rho^T(t)P\Xi_2 \sum_{m=1}^{\tilde{m}} \beta_k(t)\alpha_k(t)\epsilon_m(t) \\ & + 2\rho^T(t)PF(z(t)) + 2\iota\rho^T(t)P\Xi_4(z(t) - z(t_{k,g}h)) \\ & - 2\iota\rho^T(t)P\Xi_2 \sum_{m=1}^{\tilde{m}} \beta_k(t)(1-\alpha_k(t))g(\hat{z}(t_{k-m+1}h)) \\ & - 2\bar{\eta}\gamma^2(t) + \frac{2\sigma}{\iota}\|z(t_{k,g}h)\|\gamma(t) - 2\sum_{m=1}^{\tilde{m}} \|\theta_m\epsilon_m(t)\|\gamma(t) \\ & + 2\iota\rho^T(t)P\Xi_3\beta_k(t)\alpha_k(t)\rho(t_{k,g}h)). \end{aligned} \tag{20}$$

According to the DMETM (7) and Lemma 1, one can get

$$\begin{aligned} \iota\sum_{m=1}^{\tilde{m}} \|\epsilon_m(t)\| &\leq \tilde{m}(\sigma\|\hat{z}(t_{k,g}h)\| + \eta\|\gamma(t_{k,g}h)\|) \\ &\leq \tilde{m}(\sigma\|e(t) - e(t_{k,g}h)\| + \sigma\|e(t)\| \\ &\quad + \sigma\|z(t)\| + \sigma\|z(t) - z(t_{k,g}h)\| + \eta\|\gamma(t_{k,g}h)\|) \\ &\leq \sqrt{2}\tilde{m}\sigma(\|\rho(t) - \rho(t_{k,g}h)\| + \|\rho(t)\|) + \tilde{m}\eta\|\gamma(t_{k,g}h)\|. \end{aligned} \tag{21}$$

Based on the definition of the hybrid attacks model (11), one has

$$\begin{aligned} & E\left[2\iota\rho^T(t)P\Xi_2 \sum_{m=1}^{\tilde{m}} \beta_k(t)(1-\alpha_k(t))g(\hat{z}(t_{k-m+1}h))\right] \\ \leq & 2\iota c\tilde{m}\bar{\beta}_k(1-\bar{\alpha}_k)\|P\Xi_2\|\|\rho(t)\|\|\hat{z}(t_kh)\| \\ \leq & 2\iota c\tilde{m}\bar{\beta}_k(1-\bar{\alpha}_k)\|P\Xi_2\|\|\rho(t)\|(\|\epsilon_m(t)\| + \|\hat{z}(t_{k,g}h)\|). \end{aligned} \tag{22}$$

By (21), (22) is equivalent to the following inequality:

$$\begin{aligned} & E\left[2\iota\rho^T(t)P\Xi_2 \sum_{m=1}^{\tilde{m}} \beta_k(t)(1-\alpha_k(t))g(\hat{z}(t_{k-m+1}h))\right] \\ & \leq 2\iota c\tilde{m}\bar{\beta}_k(1-\bar{\alpha}_k)\|P\Xi_2\|\|\rho(t)\|(\|\epsilon_m(t)\| + \|z(t_{k,g}h)\| + \|e(t_{k,g}h)\|) \\ & \leq 2\iota c\tilde{m}\bar{\beta}_k(1-\bar{\alpha}_k)\|P\Xi_2\|\|\rho(t)\|(\|\epsilon_m(t)\| + \sqrt{2}\|\rho(t)\| + \sqrt{2}\|\rho(t) - \rho(t_{k,g}h)\|). \end{aligned} \tag{23}$$

With Assumption 1 in mind, one can get

$$2\rho^T(t)PF(z(t)) \leq 2c_1\|P\|\|\rho(t)\|^2 \tag{24}$$

where $c_1 = c_0\sqrt{2n(n+1)}$.

According to Lemma 2 and the Gronwall–Bellman inequality in [32], $\forall t \in [t_{k,g}h, t_{k,g+1}h)$, it holds that

$$\left\|z(t) - z(t_{k,g}h)\right\| \leq \left\|\rho(t) - \rho(t_{k,g}h)\right\|$$

$$\begin{aligned}&\leq \int_{t_{k,g}h}^{t} \|\dot{\rho}(v)\| dv \\ &\leq (e^{a_2(t-t_{k,g}h)} - 1)(\|\rho(t_{k,g}h)\| + a_1\gamma(t_{k,g}h)) \end{aligned} \tag{25}$$

where $a_1 = \frac{\eta\|\Xi_4\|}{a_2}$, $a_2 = \max\{\iota\|\Xi_1\| + \iota\|\Xi_2\| + c_1, \iota\|\Xi_1\| + \sigma\|\Xi_2\| + c_1\}$.

For $\forall t \in [t_{k,g}h, t_{k,g+1}h)$, substituting (21)–(25) into (20) results in

$$\begin{aligned} E\{\mathfrak{L}V(\tilde{\rho}(t))\} \leq & -(\iota - 2c_1\|P\|)\|\rho(t)\|^2 - 2\bar{\eta}\gamma^2(t) + \frac{2\sigma}{\iota}\|z(t_{k,g}h)\|\gamma(t) \\ & + 2\tilde{m}\|P\Xi_2\|\bar{\beta}_k\bar{\alpha}_k\|\rho(t)\|\left[\eta\|\gamma(t_{k,g}h)\| + \sqrt{2}\sigma(\|\rho(t) - \rho(t_{k,g}h)\| + \|\rho(t)\|)\right] \\ & + 2\iota\|P\Xi_4\|\|\rho(t)\|(\|\rho(t_{k,g}h)\| + a_1\|\gamma(t_{k,g}h)\|)(e^{a_2h} - 1) \\ & + 2\iota\bar{\beta}_k\bar{\alpha}_k\|P\Xi_3\|\|\rho(t)\|\|\rho(t_{k,g}h))\| + 2\iota c\tilde{m}\bar{\beta}_k(1 - \bar{\alpha}_k)\|P\Xi_2\|\|\rho(t)\| \\ & \times (\|\epsilon_m(t)\| + \sqrt{2}\|\rho(t)\| + \sqrt{2}\|\rho(t) - \rho(t_{k,g}h)\|). \end{aligned} \tag{26}$$

By assigning $\iota > 2c_1\|P\|$, it follows from (26) that

$$E\{\mathfrak{L}V(\tilde{\rho}(t))\} \leq -\omega_1 E\{V(\tilde{\rho}(t))\} + \omega_2 E\{\sqrt{V(\tilde{\rho}(t))V(\tilde{\rho}(t_{k,g}h))}\} \tag{27}$$

where ω_1 and ω_2 are given in Theorem 1.

It can be derived from (27) that

$$E\{\mathfrak{L}\sqrt{V(\tilde{\rho}(t))}\} \leq -\frac{\omega_1}{2}E\{\sqrt{V(\tilde{\rho}(t))}\} + \frac{\omega_2}{2}E\{\sqrt{V(\tilde{\rho}(t_{k,g}h))}\},\ t \in [t_{k,g}h, t_{k,g+1}h). \tag{28}$$

By integrating $\sqrt{V(\tilde{\rho}(t))}$ from $t_{k,g}h$ to $t_{k,g+1}h$, one has

$$E\{\sqrt{V(\tilde{\rho}(t_{k,g+1}h))}\} \leq \omega_3 E\{\sqrt{V(\tilde{\rho}(t_{k,g}h))}\} \tag{29}$$

where $\omega_3 = \frac{\omega_2}{\omega_1}(1 - e^{-\frac{\omega_2}{2}h}) + e^{-\frac{\omega_1}{2}h}$.

It can be concluded from (29) that when $t_{k,g}h$ tends to infinity, one can obtain that $\tilde{\rho}(t_{k,g+1}h))$ asymptotically converges to zero. Furthermore, if the conditions (17) and (18) are met, the NNCSs (3) under hybrid attacks and DMETM (7) have mean square stability. This completes the proof of the theorem. □

Remark 5. *The stability conditions (17) and (18) in Theorem 1 constitute sufficient but not necessary and sufficient conditions for system stability. Hence, these conditions are inherently conservative to some extent. Deriving necessary and sufficient stability conditions for secure control under hybrid attacks is a challenging problem due to the inherent complexity and uncertainty of the NNCSs. Therefore, developing less conservative or tighter stability criteria remains a significant topic for future research.*

5. Simulation Example

In this section, a numerical simulation and a practical example of a single-link robot arm system are utilized to demonstrate the superiority of the designed DMETC strategy.

Example 1. *Consider the following system:*

$$\begin{cases} \dot{x}_1 = x_2 + 2\sin(x_1) \\ \dot{x}_2 = u - \ln(1 + x_1^2) - \sin(t)x_2 \\ y = x_1 \end{cases} \tag{30}$$

The controller and observer parameters are chosen as $K = [26, 31]$, $H = [11, 59]^T$, *and* $\iota = 3$. *The sampling period is selected as* $h = 0.002s$. *For hybrid attacks, the nonlinear function is set as* $g(\hat{z}(t_k h)) = -\tanh(0.6\hat{z}(t_k h))$, $\bar{\alpha}_k = 0.3$, *and* $\bar{\beta}_k = 0.6$. *The initial values of the system and observer states are given by* $x = [1, -1]^T$ *and* $\hat{z} = [0, 0]^T$. *For the designed DMETM,* $\sigma = 0.2$, $\eta = 0.2$, $\bar{\eta} = 0.8$, $\theta_1 = 0.5$, $\theta_2 = 0.3$, $\theta_3 = 0.2$, *and* $\gamma(0) = 1$.

The response curves of the state x *and observer* $\hat{z}$ *are depicted in Figures 2 and 3. Figure 4 presents the event instants and intervals under the Conventional ETM [8], where the numbers of triggered data are 999. The trajectories of the state* x *are illustrated in Figure 5, from which one can discern that the designed controller stabilizes the system under hybrid attacks. The response curves of observer* $\hat{z}$ *are illustrated in Figure 6. Figure 7 presents the event instants and intervals under the DMETM, where the numbers of event are 613. Figure 8 depicts the evolution of the controller.*

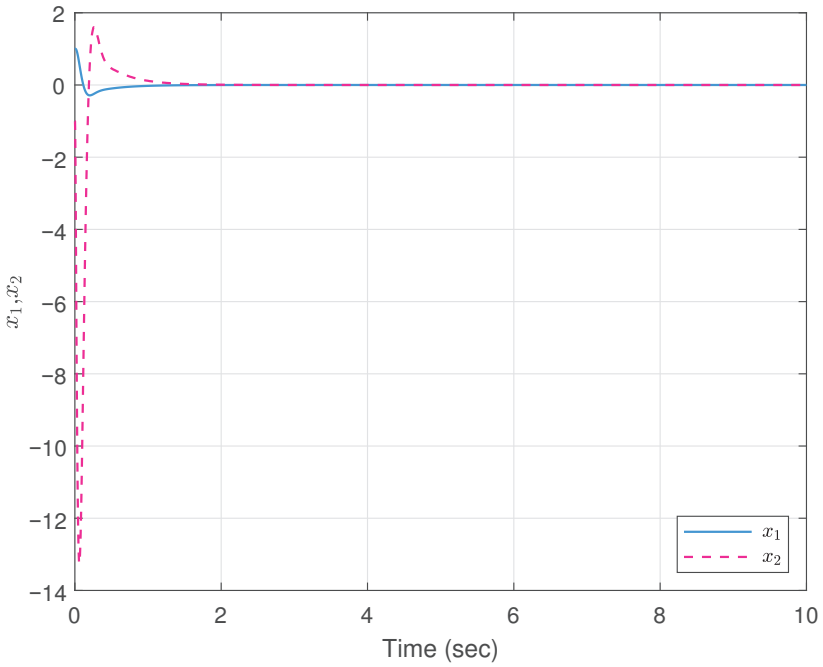


Figure 2. Trajectories of system state x under the conventional ETM [8] in Example 1.

The effectiveness of the designed DMETC strategy has been validated through a table by comparing it with the time-triggered mechanism and the conventional ETM [8]. The numbers of event-triggered packets under different communication mechanisms are presented in Table 1, in which $\mathfrak{R}$ *refers to the ratio between data packets under different ETMs and the time-triggered numbers. As shown in this table, the proposed DMETM (7) significantly reduces the number of transmission signals compared to the conventional ETM and time-triggered mechanism. Specifically, the proposed DMETM (7) decreases the network bandwidth consumption by* 87.74% *compared to the time-triggered method and by* 7.72% *compared to the conventional ETM.*

Table 1. Event-triggered numbers under different mechanism.

Method	Event-Triggered Packets	$\mathfrak{R}$
Time-triggered mechanism	5000	100%
Conventional ETM	999	19.98%
DMETM (7)	613	12.26%

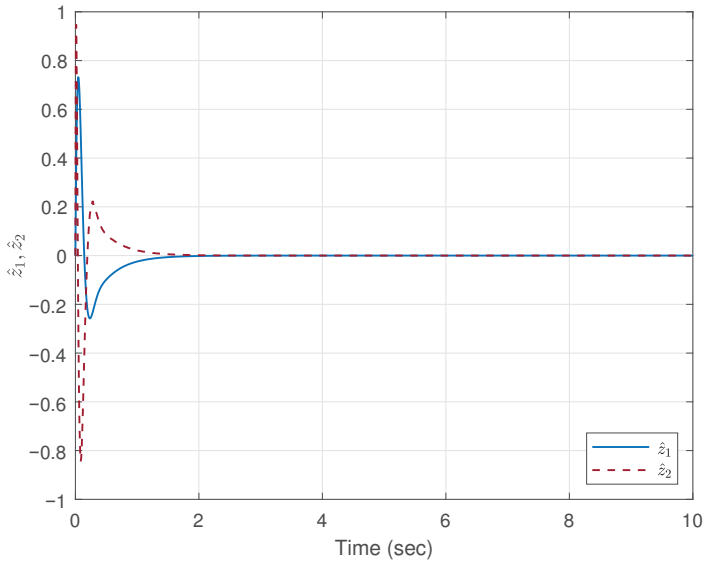


Figure 3. Trajectories of observer state $\hat{z}$ under the conventional ETM [8] in Example 1.

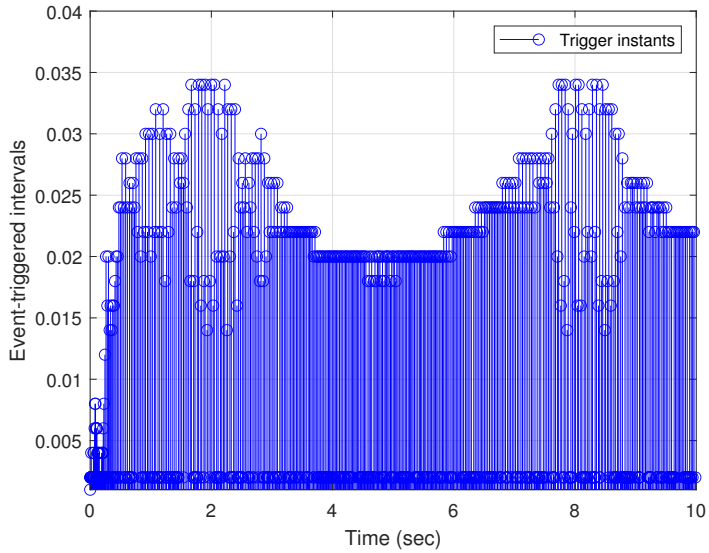


Figure 4. Event-triggered instants and intervals under the conventional ETM [8] in Example 1.

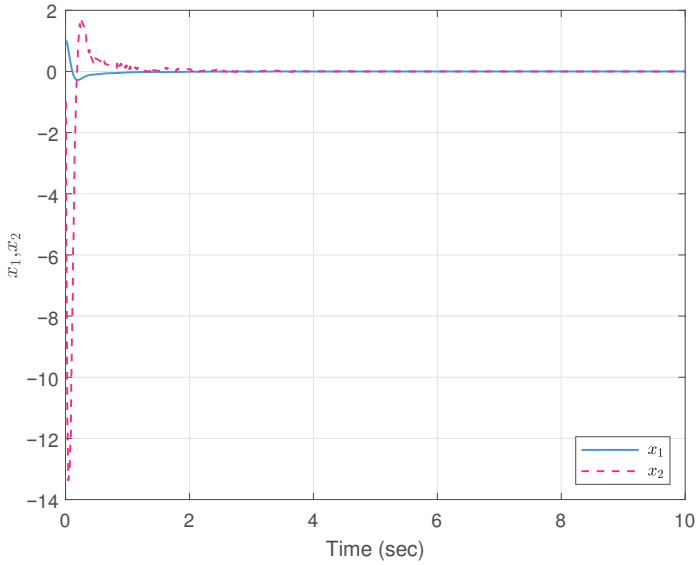


Figure 5. Trajectories of system state x under the proposed method in Example 1.

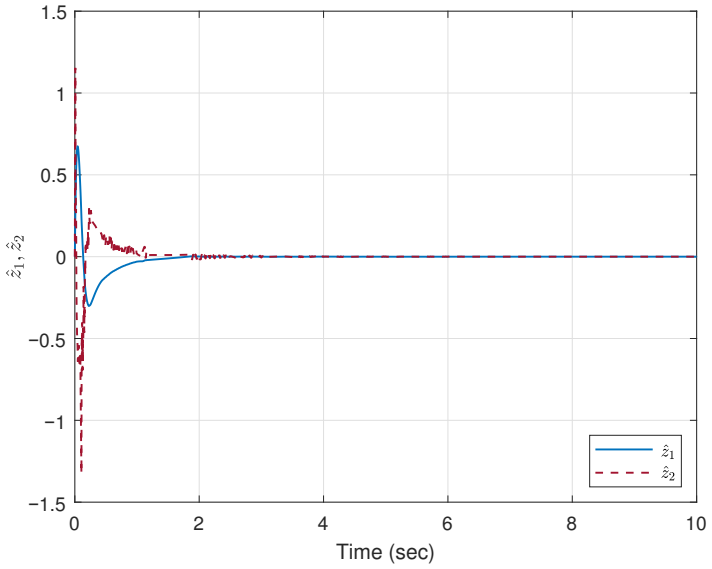


Figure 6. Trajectories of observer state $\hat{z}$ under the proposed method in Example 1.

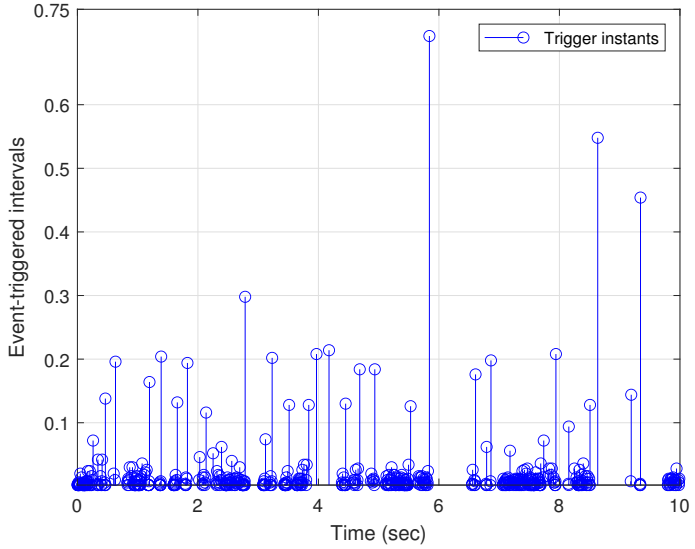


Figure 7. Event-triggered instants and intervals under the proposed method in Example 1.

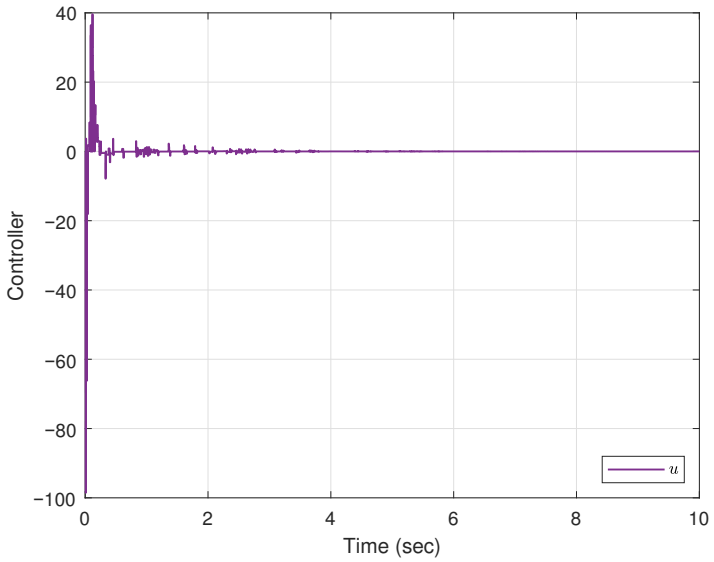


Figure 8. Trajectories of the controller under the proposed method in Example 1.

Example 2. *Consider the following robot arm system [33]:*

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = u - \frac{M\bar{g}\bar{h}}{G}\sin(x_1) - \frac{J}{G}x_2 \\ y = x_1 \end{cases} \tag{31}$$

where $M = 1.1$ *kg, and* $\bar{h} = 0.6$ *m stands for the mass and the length of the arm;* $\bar{g} = 9.81$ *m/s*^{2}*,* $G = 1$ *kg*$\cdot$ *m*^{2}*, and* $J = 2$ *N*$\cdot$*m*$\cdot$*s/rad refer to the gravity acceleration, the viscous friction coefficients, and the moment of inertia, respectively.*

The values for the control strategy are selected as follows: the sampling period $h = 0.002$ *s, the observer parameters* $\iota = 2.5$ *and* $H = [8, 20]^T$*, and the controller parameter* $K = [16, 5]$*. For hybrid attacks, the nonlinear function is given by* $g(\hat{z}(t_k h)) = -\tanh(0.2\hat{z}(t_k h))$*,* $\bar{\alpha}_k = 0.5$*, and* $\bar{\beta}_k = 0.5$*. The initial values are defined by* $x = [0.7, -0.5]^T$ *and* $\hat{z} = [0, 0]^T$*. For the designed DMETM,* $\sigma = 0.3$*,* $\eta = 0.3$*,* $\bar{\eta} = 0.8$*,* $\theta_1 = 0.5$*,* $\theta_2 = 0.3$*,* $\theta_3 = 0.2$*, and* $\gamma(0) = 0.9$*.*

In the absence of hybrid attacks, the trajectory of the state x *is shown in Figure 9, and the trajectory of observer* $\hat{z}$ *is presented in Figure 10. The event instants and intervals are given in Figure 11, where the event-triggered numbers generated by DMETM are 156. Figure 12 displays the curves of the controller. Figures 13 and 14 depict the trajectories of the state* x *and observer* $\hat{z}$ *under hybrid attacks. Figure 15 shows the event instants and intervals, where the event-triggered packets generated by DMETM are 326. The evolution of the controller is presented in Figure 16. According to Figures 9–16, compared with the attack-free scenario, the hybrid attacks inevitably introduce certain performance degradations to the system. Nevertheless, the designed DMETC strategy effectively compensates for these adverse effects, enabling the system to achieve superior steady-state performance even under the influence of hybrid attacks. This highlights the capability of the designed strategy to maintain system stability and performance in the presence of hybrid attacks threats.*

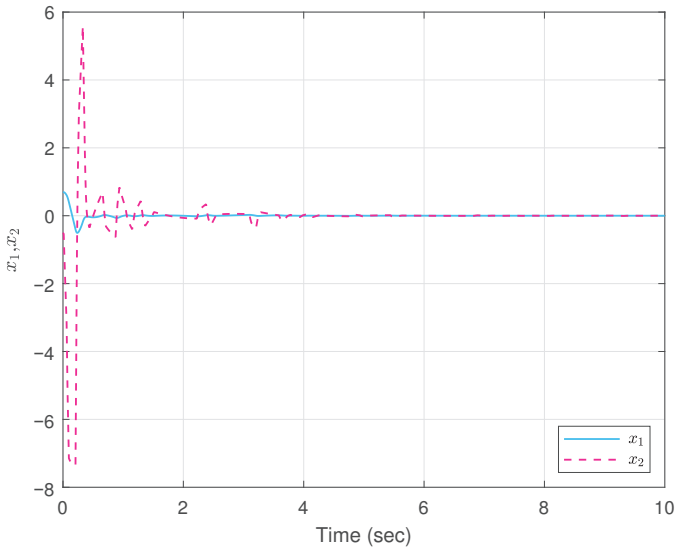


Figure 9. Trajectories of system state x without hybrid attacks in Example 2.

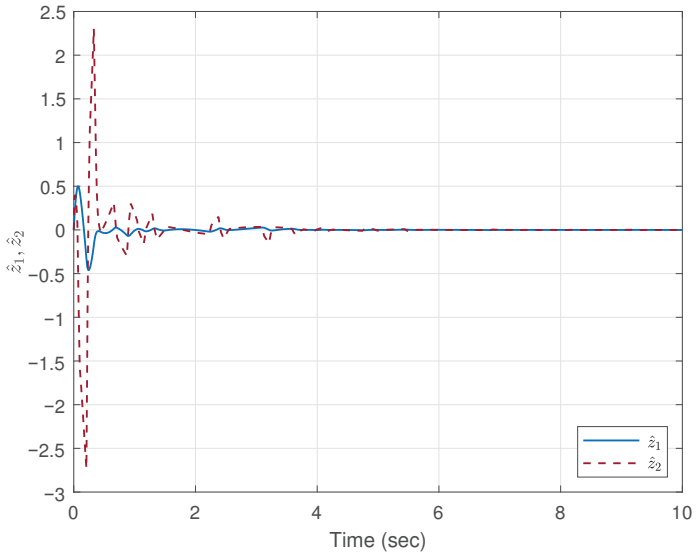


Figure 10. Trajectories of observer state $\hat{z}$ without hybrid attacks in Example 2.

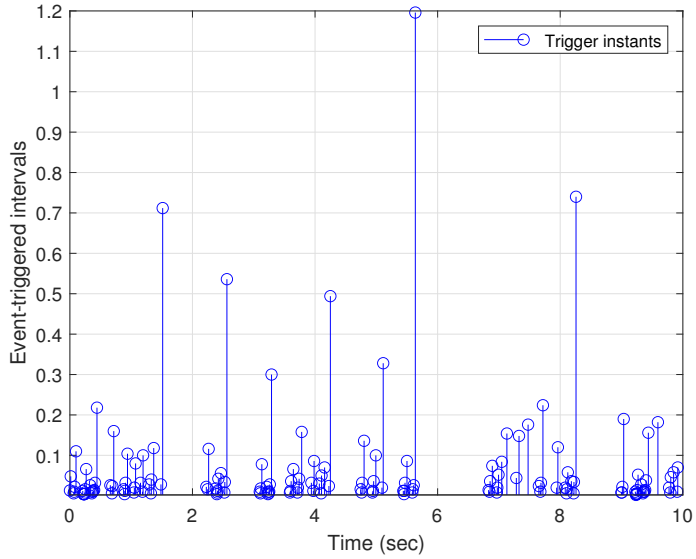


Figure 11. Event-triggered instants and intervals without hybrid attacks in Example 2.

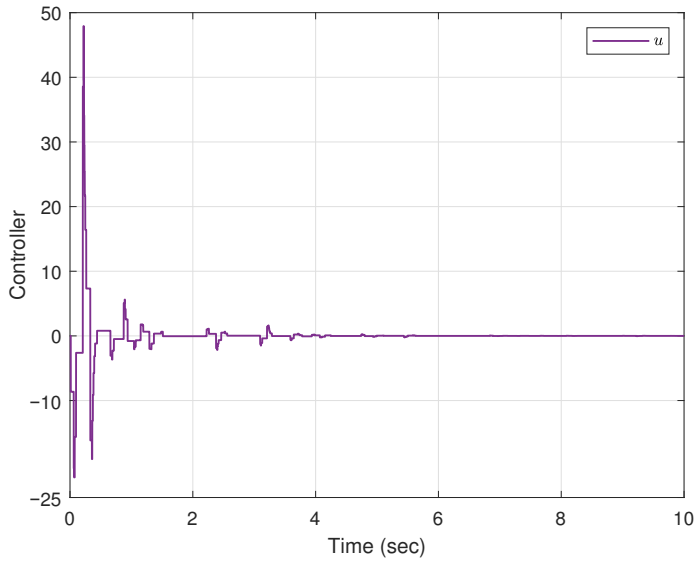


Figure 12. Trajectories of the controller without hybrid attacks in Example 2.

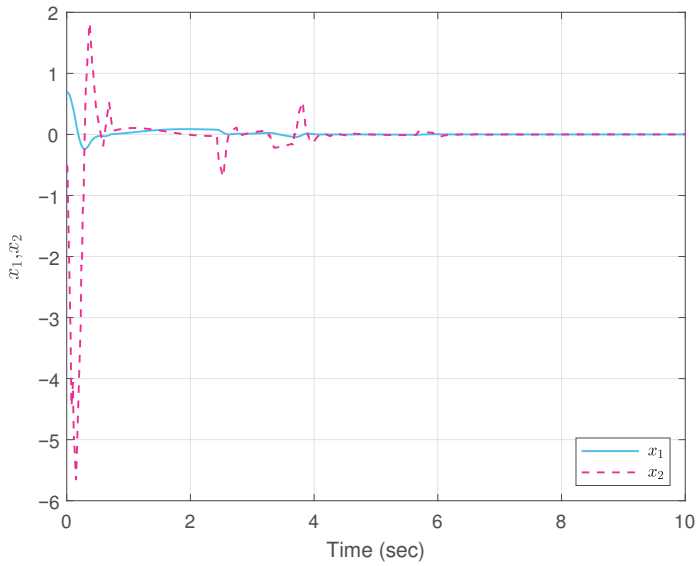


Figure 13. Trajectories of system state x under hybrid attacks in Example 2.

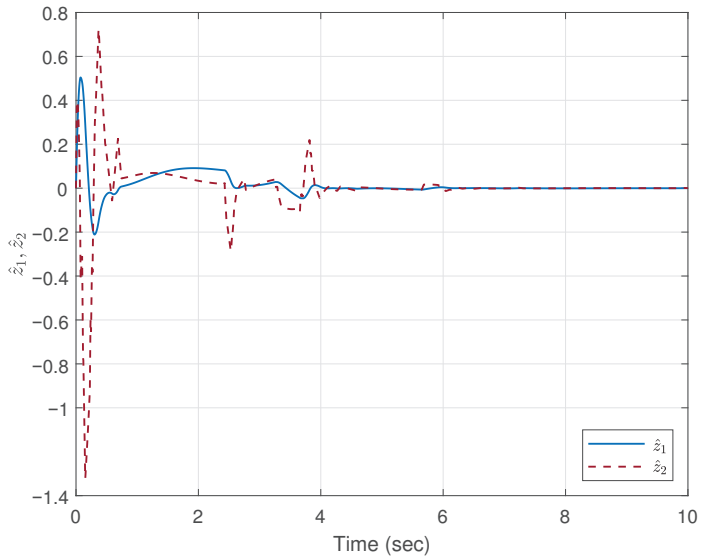


Figure 14. Trajectories of observer state $\hat{z}$ under hybrid attacks in Example 2.

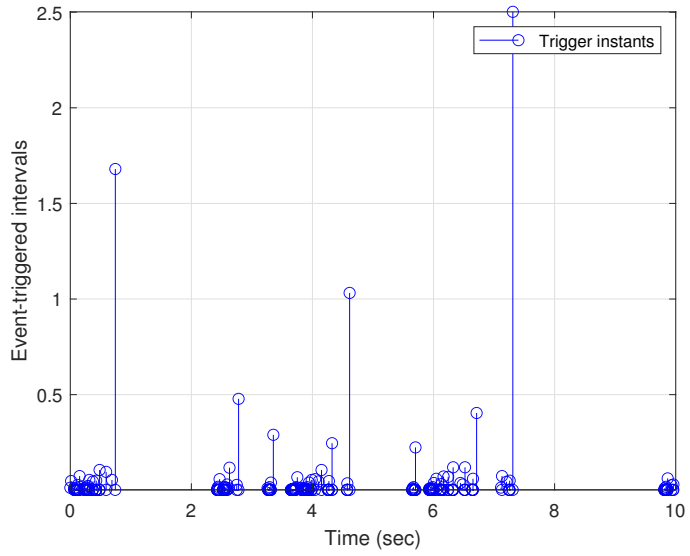


Figure 15. Event-triggered instants and intervals under hybrid attacks in Example 2.

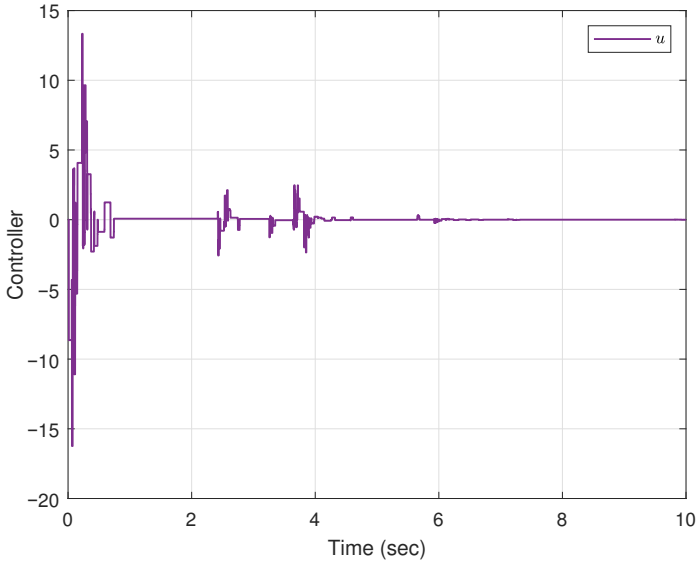


Figure 16. Trajectories of the controller under hybrid attacks in Example 2.

6. Conclusions

In this paper, the estimate-based DMETC issue has been presented for a class of NNCSs under hybrid attacks. When only the measurable signals are available, the sampled-data observer has been utilized to estimate the system output. To save the bandwidth resources, the DMETM and the auxiliary variable update law have been developed, which effectively utilize the advantages of historical sampled-data estimates. The hybrid attack model that accounts for the combined effects of both deception and DoS attacks has been put forward to describe the potential threats during network data transmission. Then, the memory-event-triggered output feedback controller has been designed to ensure that the NNCSs can achieve the mean square stability. Finally, the results of two examples have been given, which illustrate that the estimate-based DMETC method can be validated under hybrid attacks. A potential research for future work is to expand the developed DMETC method to disturbance rejection control, and finite-time security control will also be investigated.

Author Contributions: Methodology, B.Z. and M.Y.; Software, Y.W.; Formal analysis, T.Z.; Investigation, M.Y.; Writing—original draft, Z.X. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Key Research and Development Program of China, grant number 2022YFB3104300.

Data Availability Statement: The original contributions presented in the study are included in the article; further inquiries can be directed to the corresponding author.

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

References

1. Song, J.; Wang, Y.; Niu, Y.; Lam, H.; He, S.; Liu, H. Periodic event triggered terminal sliding mode speed control for networked PMSM system: A GA-optimized extended state observer approach. *IEEE/ASME Trans. Mechatron.* **2022**, *27*, 4153–4164. [CrossRef]
2. Fu, A.; McCann, J.A. Dynamic decentralized periodic event-triggered control for wireless cyber-physical systems. *IEEE Trans. Control Syst. Technol.* **2021**, *29*, 1783–1790. [CrossRef]
3. Wang, L.; Hu, M.; Bian, Y.; Guo, G.; Li, S.; Chen, B.; Zhong, Z. Periodic event-triggered fault detection for safe platooning control of intelligent and connected vehicles. *IEEE Trans. Veh. Technol.* **2024**, *73*, 5064–5077. [CrossRef]

4. Wang, F.-Y.; Gao, Y. On frequency sensitivity and mode orthogonality of flexible robotic manipulators. *IEEE/CAA J. Autom. Sin.* **2016**, *3*, 394–397. [CrossRef]
5. Zhang, X.-M.; Han, Q.-L.; Yu, X. Survey on recent advances in networked control systems. *IEEE Trans. Ind. Inform.* **2016**, *12*, 1740–1752. [CrossRef]
6. Ge, X.H.; Yang, F.W.; Han, Q.-L. Distributed networked control systems: A brief overview. *Inf. Sci.* **2017**, *380*, 117–131. [CrossRef]
7. Lu, Q.; Han, Q.-L.; Zhang, B.T.; Liu, D.L.; Liu, S.R. Cooperative control of mobile sensor networks for environmental monitoring: An event-triggered finite-time control scheme. *IEEE Trans. Cybern.* **2017**, *47*, 4134–4147. [CrossRef]
8. Yue, D.; Tian, E.; Han, Q.-L. A delay system method for designing event-triggered controllers of networked control systems. *IEEE Trans. Autom. Control* **2013**, *58*, 475–481. [CrossRef]
9. Peng, C.; Han, Q.-L.; Yue, D. To transmit or not to transmit: A discrete event-triggered communication scheme for networked takagi-sugeno fuzzy systems. *IEEE Trans. Fuzzy Syst.* **2013**, *21*, 164–170. [CrossRef]
10. Choi, Y.H.; Yoo, S.J. Decentralized event-triggered tracking of a class of uncertain interconnected nonlinear systems using minimal function approximators. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *51*, 1766–1788. [CrossRef]
11. Wu, C.; Zhao, X.; Zhao, N.; Xu, N. Periodic and dynamic periodic event-triggered control for nonlinear cyber-physical systems under DoS attacks via a hybrid system approach. *IEEE Trans. Control Netw. Syst.* **2024**, *11*, 221–232. [CrossRef]
12. Liu, J.; Zhang, N.; Li, Y.; Xie, X.; Tian, E.; Cao, J. Learning-based event-triggered tracking control for nonlinear networked control systems with unmatched disturbance. *IEEE Trans. Syst. Man Cybern.* **2023**, *53*, 3230–3240. [CrossRef]
13. Gu, Z.; Huang, X.; Sun, X.; Xie, X.; Park, J.H. Memory-event-triggered tracking control for intelligent vehicle transportation systems: A leader-following approach. *IEEE Trans. Intell. Transp. Syst.* **2024**, *25*, 4021–4031. [CrossRef]
14. Yan, S.; Gu, Z.; Ahn, C.K. Memory-event-triggered H-infinity filtering of unmanned surface vehicles with communication delays. *IEEE Trans. Circuits Syst. I Reg. Pap.* **2021**, *68*, 2463–2467.
15. Ding, F.; Zhu, K.; Liu, J.; Peng, C.; Wang, Y.; Lu, J. Adaptive memory event-triggered output feedback finite-time lane-keeping control for autonomous heavy truck with roll prevention. *IEEE Trans. Fuzzy Syst.* **2024**, *32*, 6607–6621. [CrossRef]
16. Wang, Z.; Zhang, H. Adaptive-memory event-triggered load frequency control for multi-input-delay power systems against FDI attacks and sensor faults. *IEEE Trans. Circuits Syst. II Exp. Briefs* **2024**, *71*, 4919–4923. [CrossRef]
17. Sun, J.; Yang, J.; Zheng, W.X.; Li, S. Periodic event-triggered control for a class of nonminimum-phase nonlinear systems using dynamic triggering mechanism. *IEEE Trans. Circuits Syst. I Reg. Pap.* **2022**, *69*, 1302–1311. [CrossRef]
18. He, W.; Xu, B.; Han, Q.-L.; Qian, F. Adaptive consensus control of linear multiagent systems with dynamic event-triggered strategies. *IEEE Trans. Cybern.* **2020**, *50*, 2996–3008. [CrossRef]
19. Ge, X.; Xiao, S.; Han, Q.-L.; Zhang, X.-M.; Ding, D. Dynamic event-triggered scheduling and platooning control co-design for automated vehicles over vehicular ad-hoc networks. *IEEE/CAA J. Autom. Sin.* **2022**, *9*, 31–46. [CrossRef]
20. Girard, A. Dynamic triggering mechanisms for event-triggered control. *IEEE Trans. Autom. Control* **2015**, *60*, 1992–1997. [CrossRef]
21. Chen, G.; Dong, J. Data-driven control for discrete-time nonlinear systems with dual-channel dynamic event-triggered mechanism. *IEEE Trans. Circuits Syst. II Exp. Briefs* **2023**, *10*, 4439–4443. [CrossRef]
22. Zhao, Y.; Qin, X.; Niu, B. Dynamic memory event-triggered anti-disturbance control for switched cyber-physical systems and its application to switched RLC circuit. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2024**, *71*, 6034–6043. [CrossRef]
23. Ye, F.; Cheng, Z.; Cao, X.; Chow, M.-Y. A random-weight privacy-preserving algorithm with error compensation for microgrid distributed energy management. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 4352–4362. [CrossRef]
24. Yang, M.; Zhai, J. Predictor-based decentralized event-triggered secure control for nonlinear cyber-physical systems under replay attacks and time delay. *IEEE Trans. Control Netw. Syst.* **2024**, *11*, 150–160. [CrossRef]
25. Ye, F.; Cao, X.; Cheng, Z.; Chow, M.-Y. CASL: A novel collusion attack against distributed energy management systems. *IEEE Trans. Smart Grid* **2023**, *14*, 4717–4728. [CrossRef]
26. Gao, Y.; Niu, B.; Chen, W.; Wang, H.; Mu, C.; Wen, G. Adaptive control of constrained nonlinear CPSs under deception attacks through sensor and actuator networks. *IEEE Trans. Circuits Syst. II Exp. Briefs* **2024**, *71*, 1241–1245. [CrossRef]
27. Peng, C.; Sun, H. Switching-like event-triggered control for networked control systems under malicious denial of service attacks. *IEEE Trans. Autom. Control* **2020**, *65*, 3943–3949. [CrossRef]
28. Wan, Y.; Long, C.; Deng, R.; Wen, G.; Yu, X.; Huang, T. Distributed event-based control for thermostatically controlled loads under hybrid cyber attacks. *IEEE Trans. Cybern.* **2021**, *52*, 5314–5327. [CrossRef] [PubMed]
29. Cheng, Z.; Hu, S.; Yue, D.; Dou, C.; Shen, S. Resilient distributed coordination control of multiarea power systems under hybrid attacks. *IEEE Trans. Syst. Man Cybern.* **2022**, *52*, 7–18. [CrossRef]
30. Tang, Q.; Deng, C.; Fan, S.; Wang, Y.; Yue, D.; Wang, B. A novel cooperative resilient control method for energy storage systems under hybrid attacks. *IEEE Trans. Ind. Electron.* **2025**, *72*, 3943–3949. [CrossRef]
31. Yang, J.; Sun, J.; Zheng, W.X.; Li, S. Periodic event-triggered robust output feedback control for nonlinear uncertain systems with time-varying disturbance. *Automatica* **2018**, *94*, 324–333. [CrossRef]

32. Apostol, T.M. *Mathematical Analysis*, 2nd ed.; Addison-Wesley: Reading, MA, USA, 1974.
33. Yang, M.; Zhai, J. Observer-based switching-like event-triggered control of nonlinear networked systems against dos attacks. *IEEE Trans. Control Netw. Syst.* **2022**, *9*, 1375–1384. [CrossRef]

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.