

Article

Event-Triggered Resilient Cooperative Control Strategy for Urban Rail Transit Virtually Coupled Train Sets Against Cyber-Attacks

Jianen Yang ¹ , Yuchen Dai ^{1,*} , Junyi Li ² , Jiehao Chen ¹, Lei Li ¹ and Shuangfei Ni ³

¹ College of Engineering, Zhejiang Normal University, Jinhua 321004, China

² College of Computer and Information Technology, China Three Gorges University, Yichang 443002, China

³ Changzhou Jintan District Power Supply Branch, State Grid Jiangsu Electric Power Co., Ltd., Changzhou 213000, China

* Correspondence: daiyuchen@zjnu.edu.cn

Abstract

The virtually coupled train set (VCTS) system is a promising urban rail transit paradigm that replaces physical couplers with train-to-train (T2T) wireless communication, enabling dynamic marshaling to achieve the precise matching of transportation demand and resources. However, existing VCTS control strategies either assume perfect leader state availability, rely on continuous communication, or lack guaranteed transient/steady-state performance under Denial-of-Service (DoS) attacks. To address these critical limitations, this paper proposes a unified finite-time resilient event-triggered cooperative control framework for VCTSs against malicious DoS attacks. The proposed framework integrates three synergistic components: a distributed finite-time leader state estimator to reconstruct leader information under intermittent communication interruptions, a prescribed performance finite-time controller to bound tracking error fluctuations and accelerate convergence, and an adaptive event-triggered communication protocol to reduce controller update frequency. The closed-loop system stability, finite-time convergence, and prescribed performance guarantees are rigorously proven via Lyapunov analysis, and Zeno behavior is strictly excluded. Extensive comparative simulations demonstrate that the proposed framework outperforms representative state-of-the-art methods in terms of tracking accuracy, attack resilience, and communication efficiency, achieving a significance reduction of approximately 70% in controller update frequency while maintaining system stability under the considered DoS attack scenarios.

Keywords: virtually coupled; Denial-of-Service (DoS) attacks; event-triggered; resilient cooperative control



Academic Editor: Chengxi Zhang

Received: 25 May 2026

Revised: 18 June 2026

Accepted: 24 June 2026

Published: 27 June 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.

1. Introduction

The virtually coupled train set (VCTS) system represents a next-generation economical, low-carbon and sustainable urban rail transportation system with advantages such as high speed, low pollution, low carbon emission and high energy efficiency [1]. Traditional urban rail trains use a fixed operation and control mode, which limits dynamic matching between transportation capacity and real-time passenger flow, resulting in energy waste and increased carbon emissions. The VCTS leverages the train-to-train (T2T) communication mechanism, which replaces the traditional hard-wired structure between train units, introducing extra flexibility and intelligence to train sets [2,3]. A more accurate real-time

supply of transportation capacity resources is achieved in VCTSs, further enhancing energy efficiency and environmental friendliness. However, safety issues remain the main concerns for the VCTS system in terms of the high-speed operations of urban trains and vulnerable wireless communication networks. More accurate cooperative controllers and higher state variable update frequencies are demanded. Moreover, in modern VCTS systems, malicious DoS attacks are observed and cause serious damages to data updates on wireless communication networks [4]. When erroneous operational states of the urban rail train are introduced in the control system, the stability of the system is compromised, potentially leading to catastrophic accidents [5,6]. Addressing these challenges is integral to the broader vision of sustainable urban mobility, where data-driven methods are increasingly leveraged to optimize environmental performance and resource efficiency in city systems [7,8].

The performance of a VCTS system is influenced by multiple external factors, including environmental conditions and external disturbances. Considering these external factors, various techniques are proposed to stabilize the performance of the VCTS system [9]. For example, the event-triggered technique was introduced to stabilize the VCTS system's controllers' performance [10–12]. An adaptive cooperative control strategy considering formation performance constraints was proposed to limit the operating state of train units [13]. In [14], a robust control strategy was introduced that considers the service quality of the communication network. This strategy aims to counteract the detrimental effects of jamming attacks on the VCTS system, particularly within the industrial Internet of Things (IoT) environment [15]. However, the VCTS system faces challenges in managing its complex operating environment, as the proposed strategy ignores the detrimental effects of unknown perturbations on system performance [16]. In [17], data-driven event-triggered cooperative control was proposed to monitor the headway and speed of the train set during a topology change. The strategy fails to implement effective methods to cope with tracking errors, prolonging the time required for the system to stabilize [18]. Considering all the above-mentioned limitations in the existing literature, in this study, we propose a resilient multi-agent cooperative control strategy that incorporates various influencing factors for the VCTS system, addressing the state tracking error within a specified range.

In addition, timely and precise information exchange is essential for achieving consistent control within multi-agent systems. The system's communication infrastructure is vulnerable to disturbances and malicious attacks, which can significantly undermine its operational integrity. In extreme scenarios, such adversities may lead to the complete loss of controller stability. Based on the above-mentioned assumptions, data communication network security between trains has become one of the most significant concerns in VCTS systems [19–21]. Currently, research on system security control strategies under cyber-attacks mainly focuses on compensation and fault tolerance [22–26]. S. Feng et al. [27] designed a robust impulse control strategy based on a finite-time dynamic observer, ensuring the input-to-state stability of a network control system under DoS attacks. X. Guo et al. [28] proposed a novel anti-disturbance event-triggered control strategy for an adaptive memory observer. A buffer is added to the output to improve the accuracy of the observer. The adaptive memory event-triggered mechanism is adopted to exclude the Zeno behavior of the system. Since DoS attacks may cause the mismatch behavior of modes between the system and controller, asynchronous security controllers are obtained utilizing iterative computation in [29]. DoS attacks disrupt the transmission of critical control information through essential communication channels, thereby degrading controller reliability and compromising overall system performance. To safeguard the stable operation of the VCTS system, tolerance and compensation measures against communication attacks are demanded.

Despite the valuable insights provided by the aforementioned studies, a critical gap remains in the existing literature. Most current VCTS control strategies either assume perfect leader state availability, rely on continuous and ideal communication networks, or lack guaranteed transient and steady-state tracking performance when subjected to malicious DoS attacks. Existing event-triggered or robust control methods often address these challenges in isolation, failing to provide a comprehensive defense mechanism.

To address these critical limitations and clearly differentiate our method from existing approaches, this work presents a unified finite-time resilient event-triggered cooperative control framework for VCTSs against malicious DoS attacks. Unlike prior methods [14,17,28] that merely tolerate communication delays or lack strict tracking error constraints, the proposed framework integrates finite-time convergence, prescribed performance bounds, and an adaptive event-triggered mechanism into a single synergistic architecture. This mitigates the frequent acceleration and deceleration operation of trains caused by unreliable communications and accelerates the convergence of the tracking error, ultimately improving the communication efficiency and operational stability of the VCTS system. The main novelties and contributions of this work are as follows.

1. **Novel Finite-Time State Estimation:** Unlike conventional observers that struggle with discontinuous data under cyber-attacks, multi-agent technology is integrated to design a distributed finite-time leader state estimator. This allows for a more accurate reconstruction of the leader train's operational state, effectively mitigating the impact of communication interruptions and energy wastage caused by DoS attacks.
2. **Guaranteed Transient and Steady-State Performance:** Compared to traditional cooperative controllers that cannot guarantee tracking precision under severe network disruptions, a prescribed performance control strategy is explicitly designed. This bounds the fluctuation range of the overall tracking error of the VCTS system and adjusts its responses to disrupted communication signals, thereby significantly improving the overall tracking precision of the VCTS system.
3. **Synergistic Event-Triggered Communication:** Distinct from standard time-triggered or unconstrained event-triggered methods, by combining finite-time convergence theory and an adaptive event-triggered mechanism, the VCTS system strictly excludes Zeno behavior while substantially reducing the energy consumption of communication, achieving a much lower frequency of controller updates.

The remaining parts of this work are structured as follows. The relevant dynamics of the VCTS are modeled in Section 2, where the primitives required for stability proofs are mentioned. The leader state observer is devised in Section 3, where the cooperative control strategy is conceptualized based on the prescribed performance method and event-triggered mechanism. Section 4 demonstrates the performance of the proposed control method. A comparative analysis is conducted. Section 5 draws a conclusion regarding the proposed method.

2. System Description and Related Lemmas

2.1. Principle of VCTS Technology

In a VCTS system, the leader train unit receives dispatching information from the command center and distributes the message to the following train units through a wireless communication network. The VCTS monitors network safety and coordinates the operations of all train units. The basic structure of the VCTS system is shown in Figure 1. Differences in braking performance between train units result in different braking distances. Safety margins are added to different braking distances for safe operations between VCTS trains. The guarding method, whose use is no longer determined by the braking distance

of any single train unit, significantly reduces the minimum operating spacing between the trains and increases the transportation capacity of the overall VCTS system [30]. In addition, an efficient cooperative controller is required for stable information updates. Malicious DoS attacks may block the communication channels of the VCTS system. When the control system fails to obtain the required state information, tracking errors rapidly increase, potentially leading to fatal accidents [31]. As a result, more robust control strategies are urgently demanded to improve the stability of VCTS control strategies.

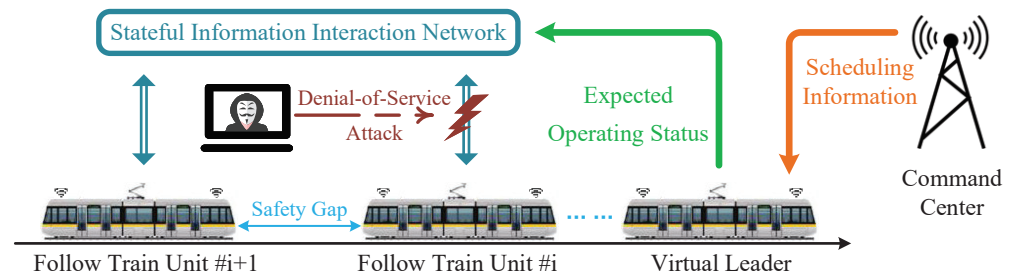


Figure 1. Schematic diagram of VCTS system operation principle.

2.2. Dynamical Model of VCTS

Train units of the consistent configuration are selected to form the VCTS, reducing the complexity of control strategies. The dynamical model is expressed as follows [32]:

$$\begin{aligned}\dot{x}_i &= v_i \\ \dot{v}_i &= u_i - \frac{1}{m_i} [f_{ui} + f_{vi} + f_i]\end{aligned}\quad (1)$$

where x_i , v_i and m_i represent the position, speed and mass of each train unit; u_i is the provided acceleration; f_{vi} , f_{ui} and f_i represent slope resistance, basic resistance and unknown disturbance.

Slope resistance varies with the size of the slope and is expressed as follows:

$$f_{vi} = m_i g \sin \theta \quad (2)$$

where θ is the body tilt angle.

According to the Davis formula, basic resistance is as follows:

$$f_{ui} = c_0 + c_1 v_i + c_2 v_i^2 \quad (3)$$

where c_0 , c_1 and c_2 are the Davis coefficients.

To ensure the security of the VCTS system, the spacing between train units has to satisfy the following:

$$x_{i-1} - x_i - L \geq H \quad (4)$$

where L is the length of each train unit. The distance between train units is composed of relative braking distance and safety margin S_m , which meets the following criteria [33]:

$$H = S_m + \max\left(0, \frac{v_{i-1}^2}{2u_{i-1}} - \frac{v_i^2}{2u_i}\right) \quad (5)$$

In real-world high-speed urban rail transit, heterogeneous braking performance necessitates a dynamic safety distance to avoid safety-critical collisions. However, the primary focus of this study is to address the cyber-physical vulnerabilities of the VCTS under DoS attacks within a cooperative multi-agent framework. To isolate the effects of network

disruptions and simplify the controller structure, a specific operational constraint is considered: a homogeneous VCTS configuration. In this scenario, all train units are assumed to share identical mechanical and braking capabilities (i.e., $u_{i-1} \approx u_i$). Under this constraint, when the train set maintains a consistent operating state, the relative braking distance term in (5) effectively approaches zero. Consequently, the desired running distance H can be mathematically and logically simplified to a constant safety margin S_m . It is worth noting that for heterogeneous train sets in actual safety-critical environments, dynamically varying spacing bounds must be rigorously enforced, which will be considered in our future research on VCTS cyber-security.

2.3. Directed Graph Theory

The communication relations of the multi-agent system are articulated through the framework of a directed graph [34]. The relationship between nodes and their communication is described through $A = [a_{ij}]_{n \times n}$, where $i, j \in (1, n)$ denote the communication node. When the element a_{ij} in the communication relationship matrix holds the state of 1, it signifies that node i conveys its operational state to node j . Conversely, if there is no information exchange between the two nodes in communication, the state of element a_{ij} is set to 0. The total number of messages received at each node is indicated by $D = \text{diag}(d_1, d_2, \dots, d_n)$, $d_i = \sum_{j=1}^n a_{ij}$, and the relationship between nodes and the leader is represented as $B = \text{diag}(b_1, b_2, \dots, b_n)$.

2.4. Related Lemmas

Lemma 1 ([35]). *A positive definite system V converges at finite time, and the convergence time fulfills this if it satisfies $\dot{V}(x) \leq -\mathcal{A}V^m(x) - \mathcal{B}V^n(x) + C$, where $\mathcal{A}$, $\mathcal{B}$ and C are all positive numbers, and C is relatively small. The convergence time is satisfied:*

$$t \leq \frac{1}{\mathcal{A}(2^m - 1)(1 - m)} + \frac{1}{\mathcal{B}(1 - n)} \quad (6)$$

When C equals 0, the convergence time is satisfied:

$$t \leq \frac{1}{\mathcal{A}(1 - m)} + \frac{1}{\mathcal{B}(1 - n)} \quad (7)$$

Lemma 2 ([36]). *Young's inequality is satisfied: for real numbers ι_1 and ι_2 , any positive odd numbers y_1 and y_2 satisfy*

$$\iota_1^{y_1} \iota_2^{y_2} \leq |\iota_1|^{y_1} |\iota_2|^{y_1} \leq \frac{1}{y_3} |\iota_1|^{y_1+y_3} + \frac{1}{y_4} |\iota_2|^{y_2+y_4} \quad (8)$$

where $y_3 > 1$, $y_4 < 1$, $y_3 + y_4 = y_3 y_4$.

Lemma 3 ([37]). *The inequality satisfies the following:*

$$\begin{aligned} \left(\sum_{i=1}^m |f_i| \right)^n &\leq \sum_{i=1}^m |f_i|^n, 0 < n \leq 1 \\ m^{1-n} \left(\sum_{i=1}^m |f_i| \right)^n &\leq \sum_{i=1}^m |f_i|^n, n > 1 \end{aligned} \quad (9)$$

3. Design of Cooperative Control Strategy

In this section, several control strategies are specifically designed to develop a resilient event-triggered cooperative control strategy for the VCTS system. A directed graph speci-

fies the direction of communication between trains, allowing individual train units to be combined into train sets by the virtually coupled technology. The localized measurement of the tracking system ensures that the leader's status is precisely estimated, which improves the resilience performance of the system. The range of the variation in tracking error is explicitly constrained, reducing time complexity for system convergence. Moreover, an event-triggered mechanism is implemented to reduce the update frequency of each controller. The underlying structure of the control strategy is shown in Figure 2.

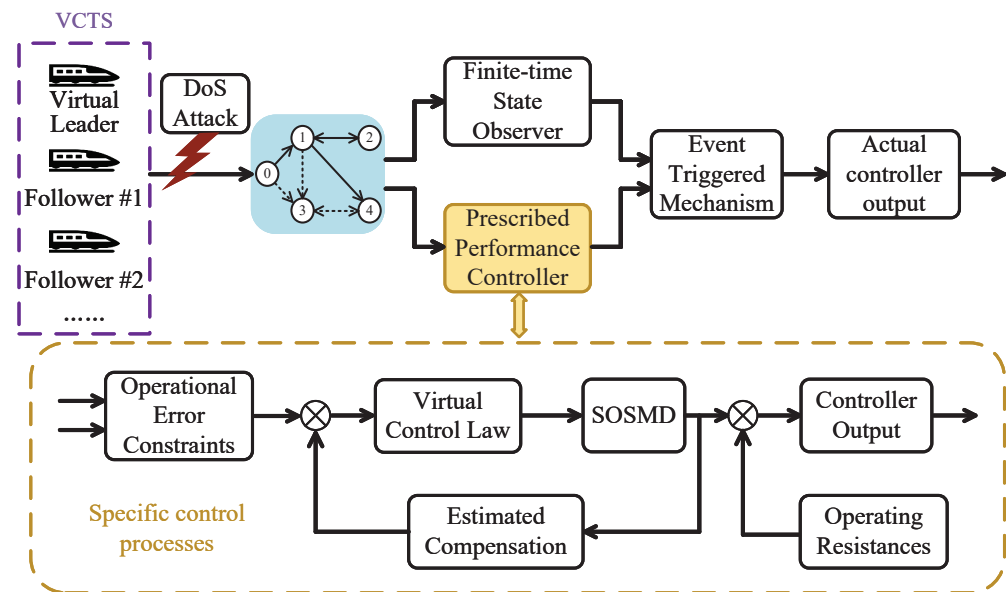


Figure 2. Underlying structure of resilient event-triggered cooperative control strategy against DoS attacks.

3.1. Design of DoS Attack Defense Mechanisms

Active DoS attacks disrupt VCTS communication lines, which causes train units to lose their peer tracking targets. To improve the resilience of the VCTS system, all train units must be capable of accurately estimating the status of the leader train through observers. Even when the communication network is interrupted, the observers can still provide an estimated status of the leader train, thus mitigating the fluctuating error that occurs when communication is recovered and further improving the fault tolerance of the VCTS system. Since the leader's acceleration is bounded and fulfills $|u_0| \leq U$, $|\dot{u}_0| \leq \dot{U}$, combined with Lemma 1, the observer is designed as follows:

$$\begin{aligned}\dot{\chi}_i &= \psi_i, \dot{\psi}_i = \mu_i \\ \mu_i &= -\alpha_1 \text{sig}(\varphi_i)^m - \alpha_2 \text{sig}(\varphi_i)^n - \varphi \\ \dot{\varphi} &= \alpha_3 \text{sign}(\varphi_i) \\ \varphi_i &= \sum_{j=1}^n a_{ij}(\psi_i - \psi_j) + b_i(\psi_i - v_0)\end{aligned}\quad (10)$$

for each following train unit, χ_i , ψ_i and μ_i represent the estimate of the position, speed and acceleration of the lead train. φ_i denotes the estimation error when adopting the multi-agent technology. α_1 , α_2 and α_3 are coefficients to be calculated, where $0 < m < 1$, $n > 1$. Additionally, the function $\text{sig}(x)$ is designed as $\text{sig}(x) = |x|\text{sign}(x)$.

Theorem 1. The designed finite-time observer estimates the operational state of the leader, with the convergence time of the estimation error, which satisfies the following:

$$t_i \leq \left(\frac{1}{\alpha_1(1-m)} - \frac{1}{\alpha_2(1-n)} \right) \left(1 + \frac{H_1/H_2}{1-H_1H_3/\alpha_1} \right) \quad (11)$$

where $\alpha_1 > H_1H_3$, $\alpha_3 > \dot{U}_0$, $H_1 = \alpha_3 + \dot{U}_0$, $H_2 = \alpha_3 - \dot{U}_0$, $H_3 = 1/\alpha_1 + (2e/H_2\alpha_1)^{1/3}$.

Proof. In initialization, we assume that the state observer on each train acquires the expected tracking target, with the tracking error denoted as $\varphi_i = \psi_i - v_0$. When the speed of the leader train decreases, we have the following:

$$\begin{aligned} \dot{\psi}_i - \dot{v}_0 &= -\alpha_1 \text{sig}(\varphi_i)^m - \alpha_2 \text{sig}(\varphi_i)^n - \varphi_0 \\ \dot{\varphi}_0 &= \alpha_3 \text{sign}(\varphi_i) + \dot{u}_0 \end{aligned} \quad (12)$$

Considering that the estimation of the observer lags behind the actual values, $\dot{\varphi}_0 > 0$. Therefore, it satisfies the following:

$$\varphi_i \leq -\alpha_1 \text{sig}(\varphi_i)^m - \alpha_2 \text{sig}(\varphi_i)^n \quad (13)$$

According to Lemma 1, convergence time satisfies the following:

$$t_1 \leq \frac{1}{\alpha_1(1-m)} - \frac{1}{\alpha_2(1-n)} \quad (14)$$

For the intermediate variable φ_0 , it is clear that $H_1 t_1 \geq |\varphi_0(t_1)|$ is satisfied at t_1 . According to [38], the observer error convergence time satisfies $t_2 \leq \varphi(\Delta T)/H_2$, where ΔT denotes the time interval for system error convergence. In addition, according to [39], there exists $|\varphi(T_{i+1})/\varphi(T_i)| \leq H_1H_3/\alpha_1 < 1$. Thus, convergence time satisfies the following:

$$t_2 \leq \frac{H_1 t_1 / H_2}{1 - H_1 H_3 / \alpha_1} \quad (15)$$

In summary, the total time for the observer error to achieve convergence is expressed as follows:

$$\begin{aligned} t &= t_1 + t_2 \\ &\leq \left(\frac{1}{\alpha_1(1-m)} - \frac{1}{\alpha_2(1-n)} \right) \left(1 + \frac{H_1/H_2}{1-H_1H_3/\alpha_1} \right) \end{aligned} \quad (16)$$

□

Furthermore, the observer of each train unit realizes the state estimations of the leader, φ_i and its derivatives are also constrained, indicated as follows:

$$|\varphi_i| \leq \phi, |\dot{\varphi}_i| \leq \dot{\phi} \quad (17)$$

3.2. Conversion of Error Constraint Forms

The actual tracking error, s_i , and the estimated tracking error provided by the observer for each train unit, $\bar{s}_i$, are defined as follows:

$$\begin{aligned} s_i &= x_i - x_0 + iH \\ \bar{s}_i &= x_i - \chi_i + iH \end{aligned} \quad (18)$$

By integrating multi-agent system technology, T2T communication enables each train unit to obtain state information regarding the VCTS system. Utilizing Lemma 1 as a reference, the tracking error is defined as follows:

$$\begin{aligned}\zeta_i &= \sum_{j=1}^n a_{ij}[s_i - s_j] + b_i s_i + \bar{s}_i \\ &= (d_i + b_i + 1)s_i - \sum_{j=1}^n a_{ij}s_j + x_0 - \chi_i\end{aligned}\quad (19)$$

When the communication of the VCTS system is interrupted by DoS attacks, the control system may fail to obtain accurate control information, causing a rapid increase in the number of tracking errors. The prescribed performance control enables the controller to adjust its response to disrupted communication signals, ensuring rapid convergence to the desired position and enhancing tracking precision for the VCTS system.

The general form of the performance function is defined as follows:

$$\ell = (\ell_0 - \ell_\infty)e^{-\iota t} + \ell_\infty \quad (20)$$

where ℓ_0 and ℓ_∞ are the initial and final values of the performance function, and ι is the convergence rate. Specifically, these error limits are rationally selected based on the physical safety constraints of the VCTS. The initial boundary ℓ_0 is mathematically defined such that $\ell_0 > \max |s_i(0)|$, ensuring that the initial tracking error of all train units strictly resides within the valid bounded region. The steady-state boundary ℓ_∞ is fundamentally determined by the stringent safety margin requirement of the train sets (e.g., rigorously restricted to 1 m in this study) to guarantee collision-free operations. The parameter ι dictates the minimum required transient convergence speed for the system to recover from tracking deviations under attacks.

Establish $\bar{\ell}$ and $\underline{\ell}$ as the constraint boundaries of the objective, denoted as follows:

$$\underline{\ell} < \zeta_i < \bar{\ell} \quad (21)$$

The inequality constraints are transformed into reasonable equation constraints to realize the design of the control law. The transformed error constraint function is expressed as follows:

$$\tau_i = \cot(\pi\eta_i), \eta_i = \frac{\zeta_i - \bar{\ell}}{\underline{\ell} - \bar{\ell}} \quad (22)$$

The derivative form of (22) is expressed as follows:

$$\begin{aligned}\dot{\tau}_i &= \frac{\pi}{(\bar{\ell} - \underline{\ell})\sin^2(\pi\eta_i)} \left[\dot{\zeta}_i - \frac{\dot{\bar{\ell}}(\zeta_i - \underline{\ell}) - \underline{\ell}(\dot{\zeta}_i - \dot{\bar{\ell}})}{\bar{\ell} - \underline{\ell}} \right] \\ &= P_i[\dot{\zeta}_i - Q_i]\end{aligned}\quad (23)$$

Meanwhile, given that

$$\frac{\partial \tau_i}{\partial \zeta_i} = \frac{\pi}{(\bar{\ell} - \underline{\ell})\sin^2(\pi\eta_i)} > 0 \quad (24)$$

this proves that the designed conversion error is positively correlated with the actual tracking error. Both errors can achieve convergence.

3.3. Event-Triggered Cooperative Controller Design

The speed tracking error is defined as follows:

$$\delta_i = v_i - \hat{\varsigma}_i \quad (25)$$

The virtual control law $\hat{\zeta}_i$, crafted with a second-order sliding mode differentiator (SOSMD), targets precise speed estimation for each train unit. It simultaneously tackles the differential expansion issue stemming from derivative calculations. With the above requirements, the structure of $\hat{\zeta}_i$ is designed as follows:

$$\begin{aligned}\dot{\hat{\zeta}}_i &= -\beta_1 |\hat{\zeta}_i - \varsigma_i|^{\frac{1}{2}} \text{sign}(\hat{\zeta}_i - \varsigma_i) + \varsigma \\ \dot{\varsigma} &= -\beta_2 \tanh(\varsigma - \hat{\zeta}_i)\end{aligned}\quad (26)$$

where ς is the intermediate variable. β_1 and β_2 are positive constants. To minimize the impact of the estimation error on system control performance, the compensation function is designed as follows:

$$\begin{aligned}\dot{\zeta}_{i1} &= -M_1 \zeta_{i1}^m - M_2 \zeta_{i1}^n + P_i(d_i + b_i + 1)(\zeta_{i2} + \hat{\zeta}_i - \varsigma_i) \\ \dot{\zeta}_{i2} &= -M_3 \zeta_{i2}^m - M_4 \zeta_{i2}^n - P_i(d_i + b_i + 1)\zeta_{i1}\end{aligned}\quad (27)$$

where M_1 , M_2 , M_3 and M_4 are all positive constants.

Furthermore, the tracking error is defined as follows:

$$\gamma_{i1} = \tau_i - \zeta_{i1}, \gamma_{i2} = \delta_i - \zeta_{i2}\quad (28)$$

Then, the virtual control law is constructed as follows:

$$\begin{aligned}\varsigma_i &= \frac{1}{d_i + b_i + 1} \left[-\frac{M_1}{P_i} \gamma_{i1}^m - \frac{M_2}{P_i} \gamma_{i1}^n \right. \\ &\quad \left. + (d_i + b_i)v_0 + \psi_i + \sum_{j=1}^n a_{ij}\dot{s}_j + Q_i \right]\end{aligned}\quad (29)$$

The event-triggered mechanism alleviates the burden of data updating in the VCTS system, which is designed as follows:

$$\begin{aligned}u_{ih}(t) &= u_{it}(t_i^k), \forall t \in [t_i^k, t_i^{k+1}) \\ \rho_i &= u_{ih}(t) - u_{it}(t_i^k) \\ t_i^{k+1} &= \inf \left\{ t > t_i^k \mid |\rho_i| \geq N_1 \mu_i^m + N_2 \mu_i^n + N_3 \right\}\end{aligned}\quad (30)$$

where t_i^k and t_i^{k+1} denote the moments when the trigger condition is satisfied. u_{it} and u_{ih} represent the control amount calculated by the system and the actual control amount applied, respectively. The decision of whether to update the controller is made by judging the state of the trigger error ρ_i . N_1 , N_2 , and N_3 are coefficients to be determined.

The finite-time cooperative control strategy is designed as follows:

$$\begin{aligned}u_{it} &= -M_3 \gamma_{i2}^m - M_4 \gamma_{i2}^n + \dot{\hat{\zeta}}_i \\ &\quad - P_i(d_i + b_i + 1)\tau_i + \frac{f_{ui} + f_{vi} + f_i}{m_i}\end{aligned}\quad (31)$$

Theorem 2. Under the event-triggered mechanism (30), the proposed control strategy (31) ensures the tracking error converges within a finite-time frame, achieving a substantial time complexity reduction in the amount of T2T communication.

Proof. To prove the stability of the closed-loop system, a composite Lyapunov candidate function is constructed as follows:

$$V_i = \frac{1}{2} \left(\gamma_{i1}^2 + \zeta_{i1}^2 + \gamma_{i2}^2 + \zeta_{i2}^2 \right)\quad (32)$$

The time derivative of V_i over $[t_i^k, t_i^{k+1})$ is calculated as follows:

$$\begin{aligned}\dot{V}_i &= \gamma_{i1}\dot{\gamma}_{i1} + \xi_{i1}\dot{\xi}_{i1} + \gamma_{i2}\dot{\gamma}_{i2} + \xi_{i2}\dot{\xi}_{i2} \\ &= M_1\gamma_{i1}\xi_{i1}^m + M_2\gamma_{i1}\xi_{i1}^n - M_1\gamma_{i1}^{m+1} - M_2\gamma_{i1}^{n+1} \\ &\quad - M_1\xi_{i1}^{m+1} - M_2\xi_{i1}^{n+1} + M_3\gamma_{i2}\xi_{i2}^m + M_4\gamma_{i2}\xi_{i2}^n \\ &\quad - M_3\xi_{i2}^{m+1} - M_4\xi_{i2}^{n+1} - M_3\gamma_{i2}^{m+1} - M_4\gamma_{i2}^{n+1} \\ &\quad + P_i\xi_{i1}(d_i + b_i + 1)(\eta_i^c - \eta_i)\end{aligned}\quad (33)$$

According to Lemma 2,

$$\begin{aligned}M_1\gamma_{i1}\xi_{i1}^m &\leq M_1\left(\frac{1}{m+1}\gamma_{i1}^{m+1} + \frac{m}{m+1}\xi_{i1}^{m+1}\right) \\ M_2\gamma_{i1}\xi_{i1}^n &\leq M_2\left(\frac{1}{n+1}\gamma_{i1}^{n+1} + \frac{n}{n+1}\xi_{i1}^{n+1}\right) \\ M_3\gamma_{i2}\xi_{i2}^m &\leq M_3\left(\frac{1}{m+1}\gamma_{i2}^{m+1} + \frac{m}{m+1}\xi_{i2}^{m+1}\right) \\ M_4\gamma_{i2}\xi_{i2}^n &\leq M_4\left(\frac{1}{n+1}\gamma_{i2}^{n+1} + \frac{n}{n+1}\xi_{i2}^{n+1}\right)\end{aligned}\quad (34)$$

The estimation error of the virtual control law is bounded when the tracking errors of the VCTS system achieve convergence in finite time. Therefore, the estimation error satisfies the following:

$$|P_i\xi_{i1}(d_i + b_i + 1)(\eta_i^c - \eta_i)| \leq \sigma_i \quad (35)$$

Combining (34) and (35), (33) is further simplified to the following:

$$\begin{aligned}\dot{V}_i &\leq -M_1\left(\frac{m}{m+1}\gamma_{i1}^{m+1} + \frac{1}{m+1}\xi_{i1}^{m+1}\right) \\ &\quad - M_2\left(\frac{n}{n+1}\gamma_{i1}^{n+1} + \frac{1}{n+1}\xi_{i1}^{n+1}\right) \\ &\quad - M_3\left(\frac{m}{m+1}\gamma_{i2}^{m+1} + \frac{1}{m+1}\xi_{i2}^{m+1}\right) \\ &\quad - M_4\left(\frac{n}{n+1}\gamma_{i2}^{n+1} + \frac{1}{n+1}\xi_{i2}^{n+1}\right) + \sigma_i\end{aligned}\quad (36)$$

To analyze the performance of the VCTS system, we define the Lyapunov function as $V = \sum_i V_i$. Based on Lemma 3, its derivative is calculated as follows:

$$\begin{aligned}\dot{V} &\leq \sum_{i=1}^n \left[-M_1\left(\frac{m}{m+1}\gamma_{i1}^{m+1} + \frac{1}{m+1}\xi_{i1}^{m+1}\right) \right. \\ &\quad - M_2\left(\frac{n}{n+1}\gamma_{i1}^{n+1} + \frac{1}{n+1}\xi_{i1}^{n+1}\right) \\ &\quad - M_3\left(\frac{m}{m+1}\gamma_{i2}^{m+1} + \frac{1}{m+1}\xi_{i2}^{m+1}\right) \\ &\quad \left. - M_4\left(\frac{n}{n+1}\gamma_{i2}^{n+1} + \frac{1}{n+1}\xi_{i2}^{n+1}\right) + \sigma_i \right] \\ &\leq -L_1 V^{\frac{m+1}{2}} - L_2 V^{\frac{n+1}{2}} + L_3\end{aligned}\quad (37)$$

where $L_1 = 2^{\frac{m+1}{2}} \min\left\{\frac{M_1 m}{m+1}, \frac{M_1}{m+1}, \frac{M_3 m}{m+1}, \frac{M_3}{m+1}\right\}$, $L_2 = 2^{\frac{n+1}{2}} \min\left\{\frac{M_2 n}{n+1}, \frac{M_2}{n+1}, \frac{M_4 n}{n+1}, \frac{M_4}{n+1}\right\}$, $L_3 = \sum_i \sigma_i$.

According to Lyapunov stability theory and *Lemma 1*, it is rigorously proven that the systematic error of the VCTS achieves convergence in finite time t_s bounded by the following:

$$t_s \leq \frac{1}{L_1(2^{(m+1)/2} - 1)} \frac{2}{1-m} - \frac{1}{L_2} \frac{2}{1-n} \quad (38)$$

In addition, Zeno behavior is prevented following the proposed event-triggered mechanism. Consider that

$$\frac{d|\rho_i|}{dt} = \frac{d}{dt}(\rho_i \rho_i)^{\frac{1}{2}} = \text{sign}(\rho_i) \dot{\rho}_i \leq |\dot{\mu}_i| \leq \bar{\mu} \quad (39)$$

The derivative of the trigger error ρ_i on $[t_i^k, t_i^{k+1})$ satisfies the following:

$$\frac{d|\rho_i|}{dt} < (mN_1\mu_i^{m-1} + nN_2\mu_i^{n-1})|\dot{\mu}_i| \quad (40)$$

Meanwhile, the absolute value of the derivative of μ_i can be expressed as follows:

$$\begin{aligned} |\dot{\mu}_i| &= \left| \alpha_1(|\varphi_i|^m)' + \alpha_2(|\varphi_i|^n)' + \alpha_3 \right| \\ &\leq \left| \alpha_1(\phi_i^m)' + \alpha_2(\phi_i^n)' + \alpha_3 \right| \\ &\leq m\alpha_1\phi_i^{m-1}\dot{\phi}_i + n\alpha_2\phi_i^{n-1}\dot{\phi}_i + \alpha_3 \end{aligned} \quad (41)$$

Setting the boundary value of $|\dot{\mu}_i|$ to κ , ρ_i has the following property:

$$|\rho_i| < \int_{t_i^k}^{t_i} \kappa (mN_1\mu_i^{m-1} + nN_2\mu_i^{n-1}) dt \quad (42)$$

According to (30), Equation (42) satisfies the following:

$$\begin{aligned} \left| \rho_i(t_i^{k+1}) \right| &\leq N_1\mu_i^m(t_i^{k+1}) + N_2\mu_i^n(t_i^{k+1}) + N_3 \\ &< \int_{t_i^k}^{t_i} \kappa (mN_1\mu_i^{m-1} + nN_2\mu_i^{n-1}) dt \end{aligned} \quad (43)$$

Consequently, the minimum event-triggering interval for each train unit is computed as follows:

$$\Delta T = \frac{N_3}{\kappa (mN_1\mu_i^{m-1} + nN_2\mu_i^{n-1})} \quad (44)$$

□

4. Results and Analysis

This study digitally simulates a segment of the VCTS operational procedure within the Simulink platform. This simulation is conducted to substantiate the efficacy of the proposed control strategy, particularly under the context of DoS attacks. Train unit $\#i$ ($i = 1, 2, 3, 4$) represents the following train unit that represents the sequential approach to the lead train, while the virtual leader train is recorded as train unit $\#0$. The operation status of the leader train is shown in Figure 3, which represents the tracking target of the train under normal circumstances.

For safety reasons, when the train in motion fails to receive external information for an extended period, it will switch to a special control mode, which is not covered in this paper. Under the simulation conditions presented here, the communication of the VCTS system will intermittently face multiple DoS attacks over a brief period. The duration of

these attacks detailed in Figure 4a, state 1, indicates that the DoS attacks are active, while the attacks are dormant in state 0.

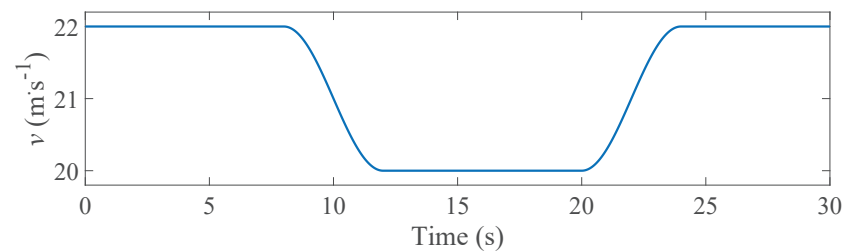


Figure 3. The operational status of the leader train.

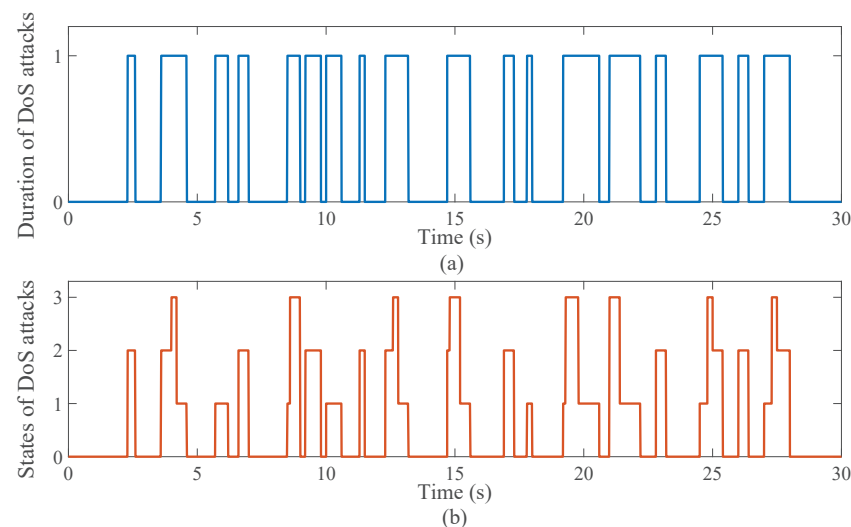


Figure 4. Duration and states of DoS attacks. (a) Duration of DoS attacks; (b) States of DoS attacks.

Since train #3 joins a new train set, its tracking target and communication object change significantly, which makes it an easier target for DoS attacks. Figure 5 depicts the structure of the T2T communication network under several attack scenarios addressed in this study. In Case 1, the communication between all train units is maintained in a normal state, all lines of communication are kept open and control information interacts normally. In Case 2, the interruption of communication between train #3 and the leader train due to a DoS attack is simulated, and the ability to obtain information about its own state only from local sensors and synchronization error information from neighboring trains will lead to an increase in the tracking error with the leader train. In Case 3, the interruption of communication between train #3 and the neighboring trains is simulated, and only the local sensors are able to obtain information about their own state and the leader train to obtain information about the leader's tracking error, which will lead to an increase in the synchronization error with the neighboring trains. In the most severe Case 4, communication between the leader train and neighboring trains will be blocked at the same time, and train #3 will not be able to receive any valid communication messages for a while, resulting in the disruption of VCTS system consistency. Taking into account the varying intensities of DoS attacks and their direct impact on system stability, the duration of each attack is categorized into distinct states ranging from 1 to 3 in Figure 4b, which is based on the varying number of communication channels affected by DoS attacks.

The following train units have different operating states at the initial moment, which are shown in Table 1. To demonstrate the practical applicability of the proposed method, the physical parameters of the train units are selected based on the typical specifications of a standard 6-car Type-A urban subway train, with a total mass of $m_i = 5 \times 10^5$ kg.

Furthermore, to verify the controller's capability in a realistic dynamic marshaling scenario (i.e., the virtual coupling process), the initial positions and speeds of the following trains are deliberately set with varying initial tracking errors relative to the virtual leader. The parameters of the proposed controller and event-triggered mechanism, determined through theoretical stability constraints and quantitative empirical tuning, are shown in Table 2.

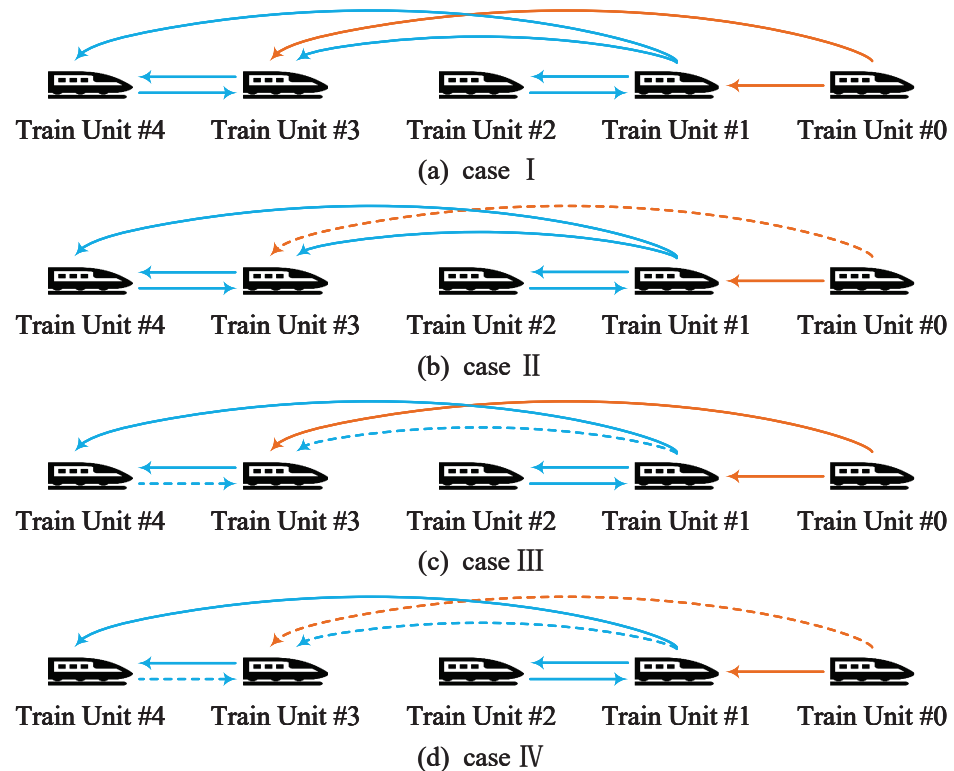


Figure 5. Communication topology between train units under different DoS attacks.

Table 1. The initial operating state of the train unit.

State	Value	State	Value	State	Value
m_i	$5 \times 10^5 \text{ kg}$	x_1	115.5 m	v_1	21.2 m/s
g	9.8 m/s^2	x_2	79 m	v_2	23.6 m/s
x_0	150 m	x_3	43 m	v_3	24.4 m/s
v_0	22 m/s	x_4	9.5 m	v_4	22.5 m/s

Table 2. Controller parameters.

Parameter	Value	Parameter	Value	Parameter	Value
m, n	3/5, 5/3	α_1	15	α_2	5
α_3	5	β_1, β_2	20, 1	M_1	0.5
M_2	1	M_3	50	M_4	40
N_1	0.3	N_2	0.2	N_3	0.5

Remark 1. The detailed quantitative steps for parameter adjustment in Table 2 are illustrated as follows: (1) Theoretical Initialization: According to the finite-time convergence conditions in Lemma 1, the fractional power parameters are strictly constrained to $m \in (0, 1)$ and $n > 1$. Here, we select $m = 3/5$ and $n = 5/3$ to mathematically balance the convergence rates both far from and near the equilibrium. (2) Baseline Parameter Tuning: The observer gains ($\alpha_1, \alpha_2, \alpha_3$) and controller gains (M_1 to M_4) are quantitatively calibrated under normal operating conditions. The primary control gains $M_3 = 50$ and $M_4 = 40$ are sized to guarantee that the tracking error remains strictly

within the prescribed performance bounds while simultaneously ensuring the generated control effort does not exceed the maximum physical traction/braking limits of the train. (3) Event-Trigger Optimization: Finally, DoS attacks and nonlinear disturbances are introduced. The event-triggering thresholds (N_1, N_2, N_3) are tuned via a quantitative trade-off: increasing N_1 and N_2 drastically reduces communication update frequency (alleviating network congestion during DoS attacks) but slightly inflates the steady-state tracking error. The values $N_1 = 0.3$, $N_2 = 0.2$, and $N_3 = 0.5$ are selected as the optimal thresholds that achieve a roughly 70% reduction in updates while maintaining the tracking error rigorously within the strict 1-m safety margin.

For each following train unit, the estimation results and the actual tracking errors are shown in Figure 6. In 0–8 s, the leader train maintains a constant speed, and the DoS attacks will not affect the observers since the initial observation errors are always kept at 0. In 8–12 s, the leader train decelerates. During a total communication interruption, the observer is inhibited from accessing accurate data, forcing the reliance on the most recent output as by default. Although the output of the observer will show small errors compared to the actual value, convergence will be reached efficiently at the moment of communication restoration.

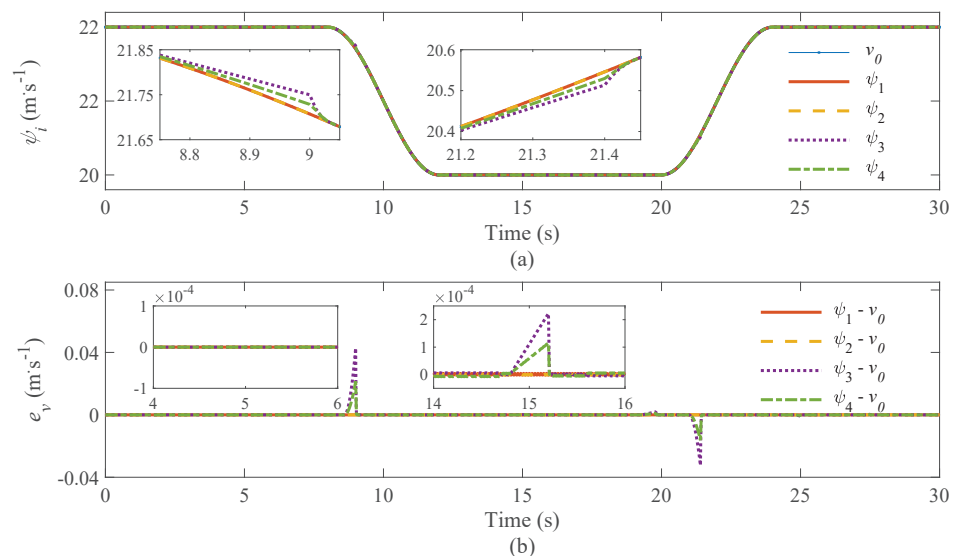


Figure 6. Tracking status and error of each train unit. (a) Tracking status; (b) Tracking error.

The combined tracking error of the VCTS system and its constraint range are shown in Figure 7. At the initial stage, the following train units have different operating states and generally have tracking errors. The parameters of the appropriate prescribed performance function are set, with various error constraints of the system being addressed. At $t = 2.5$ s, the initial tracking error of the formation unit achieves convergence. Given that the leader state observers operate efficiently, the short interruption of communication will not affect the stability of the system. Meanwhile, the event-triggered mechanism is designed to reduce the frequency of controller updates, but minor tracking errors do not significantly influence the overall performance of the VCTS system.

The control strategy proposed in this study is compared with those in [12,31] for developing resilient cooperative control strategies. As is shown in Figure 5, when train unit #3 suffers DoS attacks, it is noteworthy that train unit #4 remains capable of receiving control variables from the attacked train unit #3. Under the circumstances above, different operational states are selected for in-depth analysis to determine the impact of DoS attacks on tracking capabilities across various control strategies. The outcomes are displayed in Figure 8.

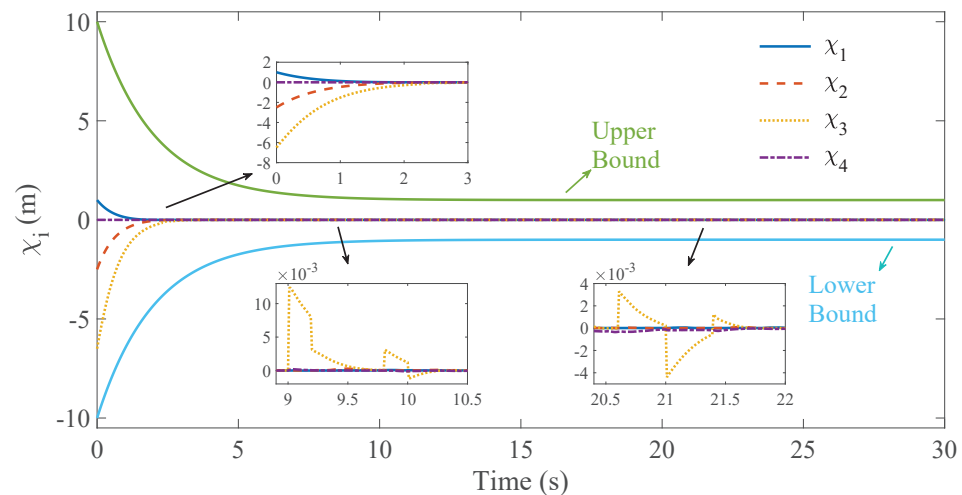


Figure 7. Formation tracking error and its constraints.

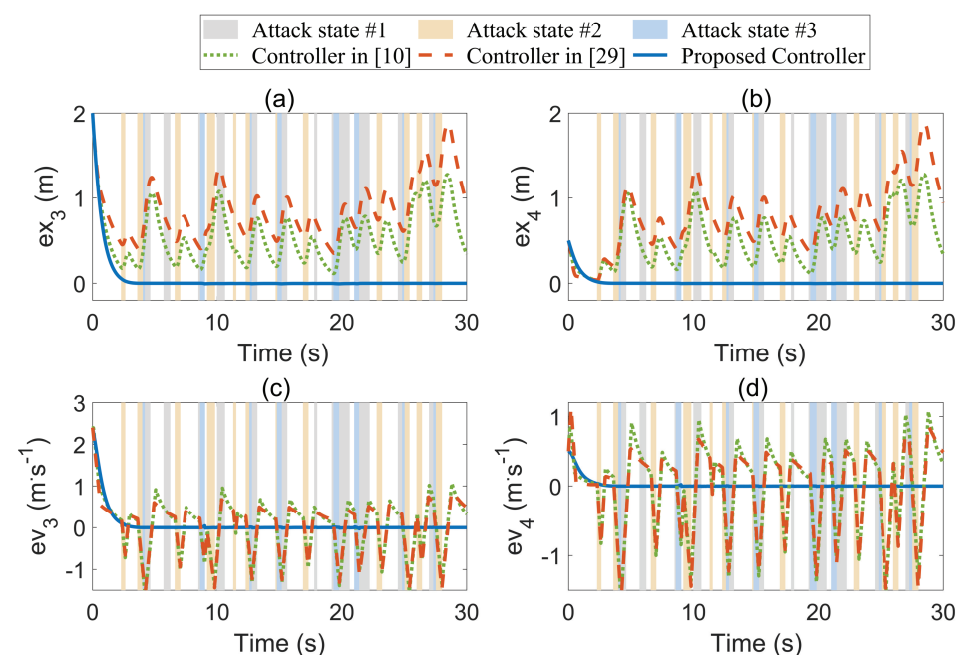


Figure 8. Tracking errors of train units #3 and #4 under DoS attacks in different control strategies. (a) Position tracking error of train unit #3; (b) Position tracking error of train unit #4; (c) Velocity tracking error of train unit #3; (d) Velocity tracking error of train unit #4.

In both [12,31], any DoS attack is bound to interfere with the communication of VCTSs due to the front-unit-following topology. Train unit #3 loses its tracking target under DoS attacks, resulting in a drastic increment in tracking errors. Conversely, the communication of train #4 is intact, enabling it to follow the incorrect operating status of train #3, which in turn impacts the control performance of the VCTS system. In addition, due to the slow error convergence of the control strategies in [12,31], the affected train units may fail to recover to the desired operating state during the dormant period of the DoS attacks. When the DoS attacks are active again, the tracking error produces new changes, and the VCTS system may fail to operate safely. With the proposed control strategy, sources for obtaining communications are flexible for train units #3 and #4. When a communication line is interrupted by DoS attacks, it is worth noting that train unit #3 can still accurately acquire tracking targets from other units. This property ensures that the tracking performance of the VCTS system remains unaffected. If the communication of train unit #3 is utterly interrupted, the locally estimated operating state of the leader unit takes over as the tracking target. Consequently, the tracking error induced by the DoS attacks is relieved. Since train

unit #4 can receive communications from other train units, the impact of inaccurate control information from train unit #3 is alleviated, protecting the overall tracking performance of the VCTS. During the inactive phase of the DoS attack, the VCTS can restore the desired operating spacing thanks to faster error convergence.

Figure 9 reflects the controller update intervals for different individual train units, and Figure 10 shows the actual number of controller updates under the designed triggering condition constraints and the ratio between the number of updates and the total number of simulation steps. The diverse operational conditions of each train unit may cause discrepancies in trigger delay errors. As a result, the timing of updates and the cumulative number of updates differ among the individual controllers. Moreover, in contrast to the time-triggered control strategy, the implemented event-triggered mechanism achieves a 70% reduction in the update frequency of the controllers, significantly alleviating the burden on the communication network of the VCTS system.

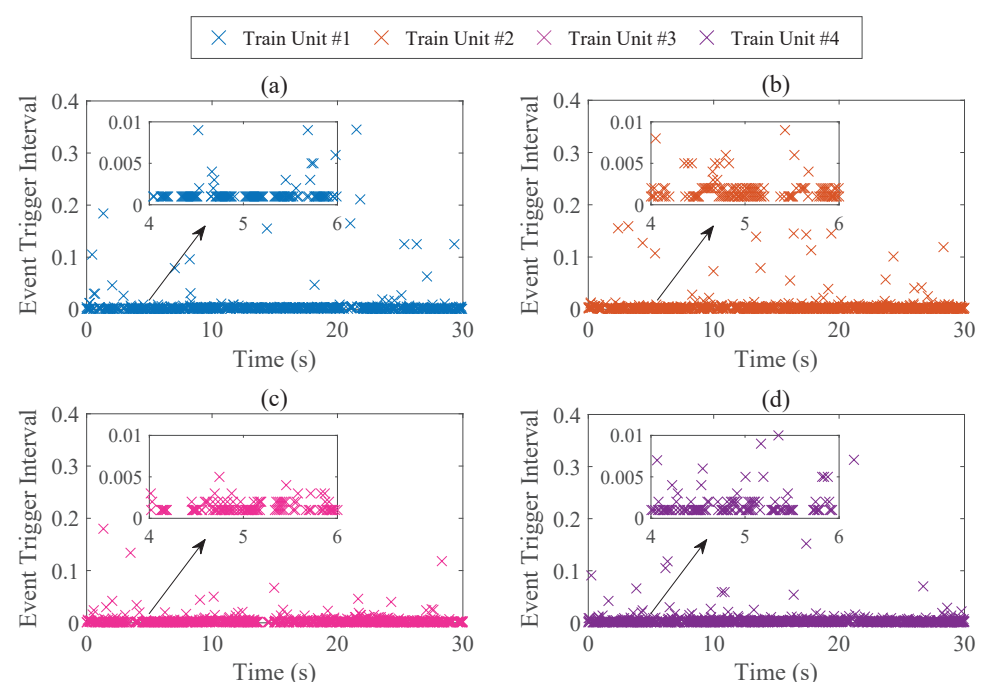


Figure 9. The controller update intervals for different individual train units. (a) Train unit #1; (b) Train unit #2; (c) Train unit #3; (d) Train unit #4.

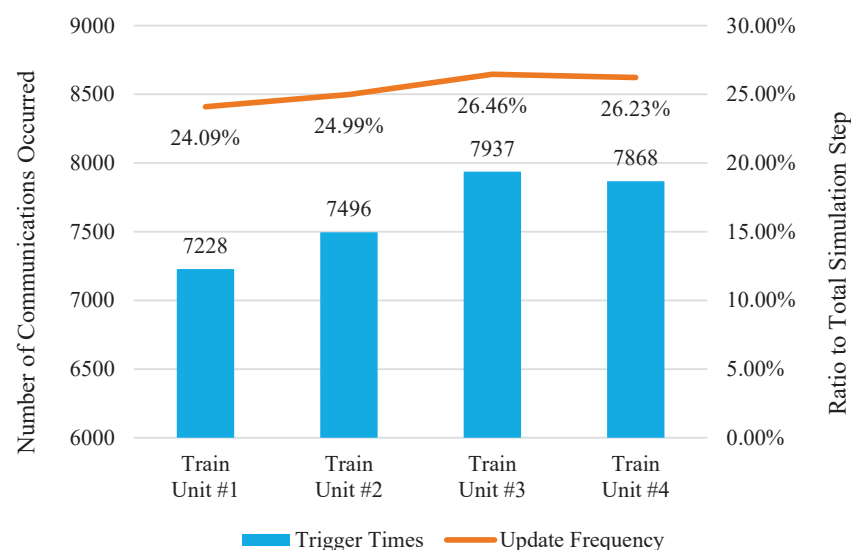


Figure 10. Number and frequency of updates to different train unit controllers.

5. Conclusions

This paper proposes a resilient event-triggered cooperative control strategy for the VCTS system, integrating multi-agent technology and finite-time theory. Through simulation analysis, the VCTS system can reliably handle malicious DoS attacks, maintain stable operations, and achieve rapid error convergence. This ensures the safe, efficient, and low-carbon operations of the urban rail transportation system. The following conclusions are drawn:

1. The proposed control strategy enhances the stability of the VCTS system against DoS attacks. By accurately estimating the leader train unit's state, the strategy ensures reliable tracking performance even when communication lines are interrupted. This resilience is crucial for maintaining operational stability and safety in urban rail transportation.
2. The control strategy improves tracking accuracy and system efficiency. The prescribed performance control strategy effectively constrains the tracking error range, ensuring rapid convergence and enhancing the overall control precision of the VCTS system. This leads to more efficient train operations and reduced energy consumption.
3. The event-triggered mechanism significantly reduces the frequency of controller updates. By intelligently triggering updates only when necessary, the mechanism decreases communication network burdens and operational energy consumption. This optimizes communication resource usage in the VCTS system and has the potential to support energy-efficient operations by mitigating unnecessary acceleration/deceleration.

From a quantitative perspective, the extensive comparative simulations validate the superiority and safety of the proposed framework. Most notably, the implemented adaptive event-triggered mechanism achieves an approximate 70% reduction in the controller update frequency compared to conventional time-triggered strategies, substantially alleviating the communication network burden. Furthermore, even under the severe DoS attack scenarios considered, the prescribed performance controller strictly limits the steady-state tracking errors within a predefined 1-m safety margin, rigorously guaranteeing collision-free operations for the VCTS system.

Despite the demonstrated resilience of the proposed control strategy against DoS attacks, this study has certain limitations regarding real-world operational constraints. Primarily, the mathematical constraints applied to the DoS attack model—such as the upper bounds of attack duration and strictly defined dormant periods—facilitate rigorous theoretical stability proofs but represent an idealized abstraction of cyber-physical threats. In a real-world urban rail transit network, DoS attacks can be highly erratic, sustained indefinitely, or compounded by physical layer jamming. Furthermore, the current dynamical model does not fully address communication delays, packet loss, actuator saturation limits, or emergency braking scenarios. In practical VCTS implementations, communication delays and packet loss could degrade synchronization accuracy, potentially causing the event-triggered mechanism to misjudge trigger conditions and reducing overall system stability. Physical actuator limits restrict the maximum acceleration and deceleration achievable by the train units, which may prolong the error convergence time during severe cyber-attacks. Additionally, emergency braking serves as a critical overriding safety measure that must be independently integrated into the control architecture to prevent collisions when safety margins are breached. Future work will focus on expanding the proposed control framework to incorporate erratic cyber-attack behaviors, heterogeneous train dynamics, and these stringent physical and communication constraints, thereby further bridging the gap between theoretical design and real-world engineering applications.

Author Contributions: Conceptualization, Y.D.; methodology, J.Y. and Y.D.; software, J.Y. and J.L.; validation, J.Y. and L.L.; formal analysis, Y.D. and S.N.; data curation, J.C.; writing—original draft preparation, Y.D. and J.Y.; writing—review and editing, Y.D. and J.Y.; supervision, Y.D. and J.L.; project administration, J.C.; funding acquisition, Y.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Zhejiang Provincial Natural Science Foundation of China, grant number LQN25E080007; Jinhua Science and Technology Plan Project, grant number 2024-4-010; and Zhejiang Provincial Philosophy and Social Sciences Planning Project, grant number 26NDJC015Z.

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

Acknowledgments: During the writing process of this work, the authors used Gemini 3.1 Pro in order to improve language only. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

Conflicts of Interest: Author Shuangfei Ni was employed by the Changzhou Jintan District Power Supply Branch, State Grid Jiangsu Electric Power Co., Ltd. The remaining authors declare that this research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Zhang, L.; U, L.H.; Zhou, M.; Li, Z. An Intelligent Train Operation Method Based on Event-Driven Deep Reinforcement Learning. *IEEE Trans. Ind. Inform.* **2022**, *18*, 6973–6980.
2. Wu, Q.; Ge, X.; Han, Q.-L.; Liu, Y. Railway Virtual Coupling: A Survey of Emerging Control Techniques. *IEEE Trans. Intell. Veh.* **2023**, *8*, 3239–3255.
3. Chai, M.; Wang, H.; Tang, T.; Chai, J.; Liu, H. A Relative Operation-Based Separation Model for Safe Distances of Virtually Coupled Trains. *IEEE Trans. Intell. Veh.* **2024**, *9*, 2031–2045.
4. Li, Y.; Huang, B.; Dai, J.; Gao, D.W.; Sun, Q.; Zhang, H. Distributed Resilient Initialization-Free Jacobi Descent Algorithm for Constrained Optimization Against DoS Attacks. *IEEE Trans. Autom. Sci. Eng.* **2024**, *21*, 3332–3343.
5. Zhu, F.; Yang, Z.; Zhao, Z.; Lin, F. Two-Stage Synthetic Optimization of Supercapacitor-Based Energy Storage Systems, Traction Power Parameters and Train Operation in Urban Rail Transit. *IEEE Trans. Veh. Technol.* **2021**, *70*, 8590–8605.
6. Zhu, L.; Lin, S.; Yu, F.R.; Li, Y. Collaborative Computing Optimization in Train-Edge-Cloud-Based Smart Train Systems Using Risk-Sensitive Reinforcement Learning. *IEEE Trans. Veh. Technol.* **2024**, *73*, 3129–3141.
7. Mihalakakou, G.; Paravantis, J.A.; Romeos, A.; Malefaki, S.; Georgiou, P.N.; Giannadakis, A. Machine Learning for Outdoor Thermal Comfort Assessment and Optimization: Methods, Applications and Perspectives. *Sustainability* **2026**, *18*, 2600.
8. Zhu, Q.; Yu, X.; Fu, H. A Decomposition-Based Deep Learning Model for Multivariate Water Quality Prediction. *Sustainability* **2026**, *18*, 4129.
9. Shang, M.; Zhou, Y.; Mei, Y.; Zhao, J.; Fujita, H. Energy-Saving Train Operation Synergy Based on Multi-Agent Deep Reinforcement Learning on Spark Cloud. *IEEE Trans. Veh. Technol.* **2023**, *72*, 214–226.
10. Wang, F.; Hu, Z.; Zhou, C.; Lin, X. Dynamic Event-Triggered Consensus Control of Multiagent Systems Under Markov Switching Topology. *IEEE Trans. Autom. Sci. Eng.* **2025**, *22*, 11163–11175.
11. Zhou, Z.; Zhu, F.; Xu, D.; Chen, B.; Guo, S.; Dai, Y. Event-Triggered Multi-Lane Fusion Control for 2-D Vehicle Platoon Systems with Distance Constraints. *IEEE Trans. Intell. Veh.* **2023**, *8*, 1498–1511.
12. Gao, S.; Peng, Z.; Liu, L.; Wang, D.; Han, Q.-L. Fixed-Time Resilient Edge-Triggered Estimation and Control of Surface Vehicles for Cooperative Target Tracking Under Attacks. *IEEE Trans. Intell. Veh.* **2023**, *8*, 547–556.
13. Ji, X.; Hao, F. Distributed Asynchronous Event-triggered Cooperative Control for Virtually Coupled Train Set Subject to Gradient Terrain and Input Saturation. *J. Frankl. Inst.* **2023**, *360*, 11809–11828.
14. Ma, S.; Wang, H.; Zhu, L.; Zhang, Q. Joint Security and Resilience Control in IIoT-Based Virtual Control Train Sets Under Jamming Attacks. *IEEE Trans. Veh. Technol.* **2023**, *72*, 11196–11212.
15. Zhu, Y.; Li, Y.; Zhu, H.; Hua, W.; Huang, G.; Yu, S.; Li, S.E.; Gao, X. Joint Sliding-Mode Controller and Observer for Vehicle Platoon Subject to Disturbance and Acceleration Failure of Neighboring Vehicles. *IEEE Trans. Intell. Veh.* **2023**, *8*, 2345–2357.
16. Wang, X.; Zhu, L.; Wang, H.; Tang, T.; Li, K. Robust Distributed Cruise Control of Multiple High-Speed Trains Based on Disturbance Observer. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 267–279.

17. Wang, Q.; Jin, S.; Hou, Z. Data-Driven Event-Triggered Cooperative Control for Multiple Subway Trains with Switching Topologies. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 14702–14711.
18. Hu, Y.; Yan, H.; Zhang, Y.; Zhang, H.; Chang, Y. Event-Triggered Prescribed Performance Fuzzy Fault-Tolerant Control for Unknown Euler-Lagrange Systems with Any Bounded Initial Values. *IEEE Trans. Fuzzy Syst.* **2023**, *31*, 2065–2075.
19. Jiang, Y.; Niu, B.; Zhao, T.; Zhao, X.; Wang, X.; Wang, H. Intelligent Consensus Asymptotic Tracking Control for Nonlinear Multiagent Systems Under Denial-of-Service Attacks. *IEEE Trans. Autom. Sci. Eng.* **2025**, *22*, 776–787.
20. Pan, Z.; Chi, R.; Hou, Z. Compensation-Based Distributed Model-Free Adaptive Control for Cyber-Attacks. *IEEE Trans. Signal Inf. Process. Over Netw.* **2023**, *9*, 84–94.
21. Zhang, Y.; Wu, Z.; Shi, P. Resilient Event-/Self-Triggering Leader-Following Consensus Control of Multiagent Systems Against DoS Attacks. *IEEE Trans. Ind. Inform.* **2023**, *19*, 5925–5934.
22. Sarrafan, N.; Zarei, J.; Razavi-Far, R.; Saif, M. Resilient Finite-Time Consensus Tracking for Nonholonomic High-Order Chained-Form Systems Against DoS Attacks. *IEEE Trans. Cybern.* **2024**, *54*, 739–751.
23. Tasooji, T.K.; Khodadadi, S.; Marquez, H.J. Event-Based Secure Consensus Control for Multirobot Systems with Cooperative Localization Against DoS Attacks. *IEEE/ASME Trans. Mechatron.* **2024**, *29*, 715–729.
24. Liang, H.; Chang, Z.; Pan, Y. Dual-Event-Triggered Intelligence Security Control for Multiagent Systems Against DoS Attacks with Applications in Mobile Robot Systems. *IEEE Trans. Artif. Intell.* **2024**, *5*, 916–924.
25. Wang, B.; Zhang, B.; Su, R. Optimal Tracking Cooperative Control for Cyber-Physical Systems: Dynamic Fault-Tolerant Control and Resilient Management. *IEEE Trans. Ind. Inform.* **2021**, *17*, 158–167.
26. Feng, Z.; Hu, G. Secure Cooperative Event-Triggered Control of Linear Multiagent Systems Under DoS Attacks. *IEEE Trans. Control Syst. Technol.* **2020**, *28*, 741–752.
27. Feng, S.; Tesi, P. Resilient Control Under Denial-of-Service: Robust Design. *Automatica* **2017**, *79*, 42–51.
28. Guo, X.; Zhang, D.; Wang, J.; Ahn, C.K. Adaptive Memory Event-Triggered Observer-Based Control for Nonlinear Multi-Agent Systems Under DoS Attacks. *IEEE/CAA J. Autom. Sin.* **2021**, *8*, 1644–1656.
29. Zhang, Y.; Wu, Z.-G. Asynchronous Control of Markov Jump Systems Under Aperiodic DoS Attacks. *IEEE Trans. Circuits Syst. II Express Briefs* **2023**, *70*, 685–689.
30. Ge, X.; Wu, Q.; Han, Q.-L.; Zhang, X.-M. Resilient Virtual Coupling Control of Automatic Train Convoys with Intermittent Communications. *IEEE Trans. Veh. Technol.* **2022**, *16*, 3658–3667.
31. Xi, W.; Hu, M.; Wang, H.; Dong, H.; Ying, Z. Formation Control for Virtual Coupling Trains With Parametric Uncertainty and Unknown Disturbances. *IEEE Trans. Circuits Syst. II Express Briefs* **2023**, *70*, 3429–3433.
32. Wang, H.; Zhao, Q.; Lin, S.; Cui, D.; Luo, C.; Zhu, L.; Wang, X.; Tang, T. A Reinforcement Learning Empowered Cooperative Control Approach for IIoT-Based Virtually Coupled Train Sets. *IEEE Trans. Ind. Inform.* **2021**, *17*, 4935–4945.
33. Basile, G.; Lui, D.G.; Petrillo, A.; Santini, S. Deep Deterministic Policy Gradient Virtual Coupling Control for the Coordination and Manoeuvring of Heterogeneous Uncertain Nonlinear High-Speed Trains. *Eng. Appl. Artif. Intell.* **2024**, *133*, 108–120.
34. Dai, Y.; Zhang, L.; Yan, K.; Chen, Q.; Zhou, Z.; Zhou, K. An Integrated Cooperative Control Strategy for EVs Accessed Community Uninterruptible Power System. *IEEE Trans. Intell. Veh.* **2023**, *8*, 2482–2493.
35. Wang, X.; Guo, J.; Tang, S.J.; Qi, S. Fixed-time Disturbance Observer Based Fixed-time Back-stepping Control for An Air-breathing Hypersonic Vehicle. *ISA Trans.* **2019**, *88*, 233–245.
36. Hou, Q.; Dong, J. Cooperative Output Regulation of MASs with a Novel Parameter Convergence Condition and Prescribed-Time Event-Triggered Observers and Its Application to Robot Formation. *IEEE Trans. Autom. Sci. Eng.* **2025**, *22*, 4168–4179.
37. Zuo, Z.; Tie, L. Distributed Robust Finite-time Nonlinear Consensus Protocols for Multi-agent Systems. *Int. J. Syst. Sci.* **2014**, *47*, 1366–1375.
38. Shtessel, Y.; Edwards, C.; Fridman, L.; Levant, A. *Sliding Mode Control and Observation*; Springer: New York, NY, USA, 2014; pp. 1743–1746.
39. Utkin, V. On Convergence Time and Disturbance Rejection of Super-twisting Control. *IEEE Trans. Autom. Control* **2013**, *58*, 2013–2017.

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.