mathematics

MDPI

Article

Secure Dynamic Event-Triggered Cluster Synchronization Control of Complex Dynamical Networks Under Random Deception Attacks

Yuncai Yu [1] and Ling Liu [2,*]

[1] School of Economics and Statistics, Guangzhou University, Guangzhou 510006, China; yyc20@gzhu.edu.cn
[2] School of Mathematics and Systems Science, Guangdong Polytechnic Normal University, Guangzhou 510665, China
* Correspondence: lgliu0@163.com

Abstract

This paper is concerned with the secure and resource-efficient cluster synchronization problem of a class of complex dynamical networks (CDNs) under random deception attacks. Each node in the CDNs is modeled by a nonlinear dynamical system with multiple time-varying delays and nonlinear couplings. The central aim is to make each cluster of nodes converge to the same reference trajectory that is distinct for each cluster regardless of the adverse effects of random deception attacks while ensuring communication efficiency for each node. Toward this aim, a distributed dynamic event-triggered mechanism is first proposed such that each node can make its own decisions to transmit or not its data of interest over the communication channel. Second, by suitably modeling the random deception attacks, secure and event-based cluster synchronization controllers are constructed, which incorporate both the effects of random deception attacks and intermittent data arrivals. Then, sufficient conditions ensuring the secure cluster synchronization of the delayed CDNs under randomly occurring deception attacks are established by constructing some appropriate Lyapunov functionals. Furthermore, tractable design criteria on the existence of desired cluster synchronization controllers are derived. Finally, an illustrative example is presented to validate the effectiveness of the main theoretical results.

Keywords: complex dynamical networks; cluster synchronization; deception attacks; dynamic event-triggered mechanism

MSC: 37M05; 37M25

Academic Editor: Zhulou Cao

Received: 14 October 2025
Revised: 18 November 2025
Accepted: 23 November 2025
Published: 26 November 2025

Citation: Yu, Y.; Liu, L. Secure Dynamic Event-Triggered Cluster Synchronization Control of Complex Dynamical Networks Under Random Deception Attacks. *Mathematics* **2025**, *13*, 3797. https://doi.org/10.3390/math13233797

1. Introduction

Complex dynamical networks (CDNs) have attracted extensive research attention in recent years due to their widespread applications in fields such as power systems, water and gas distribution systems, and transportation systems. Typically, a CDN is composed of a large number of nodes (or agents and subsystems) that interact with each other across both physical and cyber layers in such a way as to achieve some cooperative dynamical behaviors. Not surprisingly, there have been many fruitful results available on dynamical behavior analysis for CDNs, including state estimation [1], synchronization [2,3], and finite-/fixed-time control [4,5].

Synchronization, as one of the most important collective dynamical behaviors for dynamical systems, has been investigated for decades [6–8]. To analyze synchronization

performance and further design synchronization controllers, several methods have been reported, such as the master stability function method [9], the matrix measure analysis method [10], and the Lyapunov function method [11]. It is noteworthy that a large portion of existing results on synchronization of CDNs focus on complete synchronization; namely, all nodes in the CDNs share the common dynamical behavior when the time approaches infinity. However, cluster synchronization finds broader applications than complete synchronization in both nature and practical applications [12], such as during neuron discharging in the brain, multi-objective search and rescue, and military surveillance and tracking. Under a cluster synchronization setting, nodes are first split into different groups which are called clusters. Then nodes are driven to keep synchronized with their peers in the same cluster but not with those in different clusters. In the presence of multiple external reference sources, the nodes in the same cluster are then regulated to synchronize with each reference source. Up till now, a great deal of effort has been devoted to cluster synchronization of CDNs [13–17]. For example, the prescribed-time cluster synchronization issue for complex networks is studied in [14]. In [15], a pinning control strategy is presented to synchronization a class of linearly coupled CDNs into different clusters. In [16], the finite/prescribed-time cluster synchronization problem is studied for a class of CDNs with asynchronous switching. In [17], the problem of cluster synchronization is extended to deal with parameter mismatches and time-varying delays in CDNs under impulsive control. Nevertheless, it should be pointed out that the above cluster synchronization methods are based on two ideal assumptions that (1) the data transmissions/exchanges on each node are continual at every continuous time t and (2) the network environment, providing a two-way communication medium for the CDNs, is safe in a sense that all data transmissions/exchanges between sender nodes and receiver nodes are secure without any interruption or corruption.

Due to the openness and insufficient protection of most communication networks, CDNs are actually vulnerable to malicious attacks, such as denial-of service (DoS) attacks [18,19] and deception attacks [20,21]. Apparently, such malicious attacks may degrade the desired synchronization performance of CDNs or even destabilize the closed-loop CDNs. This thus calls for secure synchronization controllers against the adversarial effects of malicious attacks on CDNs. So far, several effective secure control methods have been developed in the literature of cyber-physical systems, e.g., [22–26]. Among the various attacks, deception attacks generally violate the integrity of transmitted data by injecting arbitrary and falsified information [27–29]. For example, in [27], for a class of linearly coupled complex networks under deception attacks and disturbance estimator, the synchronization issue is solved.

Apart from the security issue of CDNs aforementioned, another significant issue of synchronization control of CDNs is to preserve resource efficiency. This is because the synchronization control objective relies on the information transmission or exchange among the interacting nodes, while such an information sharing process inevitably occupies and consumes excessive resources. Event-triggered transmission mechanisms have yet shown their benefits in reducing unnecessary data transmissions and further controller updates. More specifically, compared with a conventional time-triggered mechanism where data transmissions are invoked typically at periodic times, the decisions of 'whether or not each node's data should be transmitted' are determined by some well-defined events when an event-triggered mechanism is employed. Thus, event-triggered mechanisms can effectively reduce the frequency of data transmissions and further the communication resource occupancy. Naturally, the problem of event-triggered synchronization control for CDNs has been widely explored in the last decade [30–36]. Nevertheless, it is mentioned that the above event-triggered synchronization methods all fall into the category of static triggering,

wherein the triggering conditions are based on only system available information. Recently, another strategy of dynamic triggering is proposed in [37] and has been greatly developed in the past several years. A key feature of such dynamic triggering is that some auxiliary or internal dynamic variable is introduced into the triggering conditions such that the triggering intervals can be generally prolonged. In other words, dynamic triggering can often leads to more resource efficiency than its static counterpart. Applying dynamic triggering to synchronization control problems of CDNs has also attracted great interest, see, e.g., [38–40]. To our knowledge, there have been relatively few results available on cluster synchronization of CDNs while taking into account both dynamic event-triggered mechanism and security countermeasure against deceptive attacks, which gives rise to the second motivation of this study.

In this paper, we investigate the secure cluster synchronization problem for a class of CDNs under random deception attacks. The main contributions of this paper are listed as follows. (1) A general CDN model is formulated by taking into account both nonlinear model dynamics, multiple time-varying delays, nonlinear and delayed couplings. Unlike the linear coupled CDNs [14], the CDN model researched in this paper can simulate actual nonlinear systems more accurately. (2) A unified secure cluster synchronization control framework is established to simultaneously address nonlinear dynamics, multiple time-varying delays, and random deceptive attacks. Most existing secure control works focus on denial-of-service (DoS) attacks or single-type synchronization (e.g., complete synchronization) [6–8], while this paper addresses cluster synchronization with deceptive attacks and provides explicit attack tolerance bounds, which fills the gap in heterogeneous state synchronization under data tampering. (3) Tractable stability analysis and control design criteria are derived such that the resulting closed-loop CDN achieve secure cluster synchronization while maintaining efficient resource occupancy over the communication channels. A special case of secure static event-triggered cluster synchronization control design is also presented. The controller design integrates attack compensation terms to counteract the adverse effects of data tampering, and sufficient conditions for synchronization are derived via Lyapunov-Krasovskii functionals with some integral inequalities, which are less conservative than existing delay-independent criteria [16].

The rest of this paper is organized as follows: Section 2 shows the model description. Section 3 gives the main results. In Section 4, a numerical example is presented, and concluding remarks are given in Section 5.

2. Preliminaries and Problem Formulation

2.1. Notation

Denote $\mathcal{N}$ and $\mathcal{N}^+$ as the set of natural numbers and non-negative integers, respectively. R^n and $R^{n\times m}$ stands for the set of n-dimensional real space and $n \times m$ dimensional real spaces, respectively. Denote $\mathcal{I}_n \in R^{n\times n}$ as identity matrix, $n \in \mathcal{N}^+$. $\mathcal{B} > 0$ ($\mathcal{B} < 0$) means that the matrix $\mathcal{B}$ is a positive (negative) definite matrix. The superscript 'T' indicates matrix transposition and '$\otimes$' is the Kronecker product. Matrices are all with appropriate dimensions without special description.

The interconnection topology among nodes is modeled by a digraph $\mathcal{G}(\mathcal{V}, \mathcal{E}, A)$ of order $N \in \mathcal{N}^+$ with a set of nodes $\mathcal{V} = \{1, 2, \cdots, N\}$, a set of edges $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$, and weighted adjacency matrix $A = (a_{ij})_{N\times N} \in R^{N\times N}$, where a_{ij} is the weight of the directed edge (j, i) satisfying $a_{ij} \neq 0$ if $(j, i) \in \mathcal{E}$ and $a_{ij} = 0$ otherwise. Moreover, it is assumed that $a_{ii} = 0$, $i \in \mathcal{V}$ to avoid self-loops.

Let $\mathcal{M} = 1, 2, \cdots, \bar{m}$ be a cluster set with $\bar{m} \geq 1$ and $\{\mathcal{P}_1, \cdots, \mathcal{P}_{\bar{m}}\}$ be a partition of the initial node set $\mathcal{V}$ such that $\mathcal{V} = \cup_{l=1}^{\bar{m}} \mathcal{P}_l$, and $\mathcal{P}_l \cap \mathcal{P}_k = \emptyset$ for $l \neq k, l, k \in \mathcal{M}$. Denote by $\mathcal{P}_1 = \{l_0 + 1, \cdots, l_1\}, \cdots, \mathcal{P}_k = \{l_{k-1} + 1, \cdots, l_k\}, \cdots, \mathcal{P}_{\bar{m}} = \{l_{\bar{m}-1} + 1, \cdots, l_{\bar{m}}\}$, $l_0 = 0$,

$l_{\bar{m}} = N$. Denote the total number of the nodes in the kth cluster by $n_k = \lceil \mathcal{P}_k \rfloor$, $k \in \mathcal{M}$, where $\lceil \cdot \rfloor$ represents the cardinality of the set. Other key notations can be found in the Table 1.

Table 1. Summary of Key Notations in the Paper.

Notation	Type	Definition
N	Positive integer	Total number of nodes in CDNs.
$\bar{m}$	Positive integer	Total number of clusters with $M = \{1, 2, \cdots, \bar{m}\}$.
P_k	Set	Index set of nodes belonging to the k-th cluster.
n_k	Positive integer	Number of nodes in the k-th cluster.
τ_M	Non-negative real number	Maximum delay in the CDNs.
$\alpha(t)$	Bernoulli random variable	Stochastic variable modeling random deception attacks.
$\bar{\alpha}$	Real number	Probability of deception attacks occurring.
$h(\cdot)$	Continuous function	Deceptive signal injected by attackers into the communication channel.
H	$n \times n$ positive definite matrix	Bounding matrix for the deceptive signal $h(\cdot)$.
$\bar{e}_i(t)$	n-dimensional real vector	Actual error signal received by the controller (after possible attack modification).
t_q^i	Non-negative real number	q-th event-triggering time of the i-th node.
$\eta_i(t)$	Non-negative real number	Auxiliary dynamic variable for the event-triggered mechanism.
π_i, θ_i, ζ_i, ϱ_i	Positive real numbers	Tuning parameters for the dynamic event-triggered mechanism.
Ψ_i	$n \times n$ positive definite matrix	Weighting matrix in the event-triggered condition.
K_i	$n \times n$ real matrix	Controller gain matrix for the i-th node.
Γ_{1k}, Γ_{2k}	$n \times n$ real matrices	Bounding matrices for the nonlinear function $f_k(\cdot)$.
δ_1, δ_2	Positive real numbers	Lipschitz constants for the coupling functions $g_1(\cdot)$ and $g_2(\cdot)$.
Q, R_1, R_2, R_3, R_4, M_1, M_2	Block-diagonal positive definite matrices	Weighting matrices introduced in the Lyapunov function for stability analysis.
Ξ	Real matrix	Auxiliary variable for controller gain design.

2.2. Modeling of CDNs

Consider a class of CDNs consisting of N interacting nodes, in which the dynamics of the ith node, $\forall\, i \in \mathcal{V}$, are described by the following coupling state-space equation

$$\begin{aligned} \dot{x}_i(t) =& \breve{W}_{1i} \breve{f}_i(x_i(t)) + \breve{W}_{2i} \breve{f}_i(x_i(t - \tau_1(t))) + \sum_{j=1}^{N} a_{ij} \Lambda_1 g_1(x_j(t)) \\ &+ \sum_{j=1}^{N} b_{ij} \Lambda_2 g_2(x_j(t - \tau_2(t))) + u_i(t), \end{aligned} \tag{1}$$

where $x_i(t) = (x_{i1}(t), \cdots, x_{in}(t))^T \in R^n$ is the state vector of the ith node; $\breve{W}_{1i}, \breve{W}_{2i} \in R^{n \times n}$ are the connection weight matrices; $\breve{f}_i(x_i(t)) = (\breve{f}_i(x_{i1}(t)), \cdots, \breve{f}_i(x_{in}(t)))^T$, $\breve{f}_i(x_i(t - \tau_1(t))) = (\breve{f}_i(x_{i1}(t - \tau_1(t))), \cdots, \breve{f}_i(x_{in}(t - \tau_1(t))))^T$ are continuous non-delayed and de-

layed nonlinear functions, $0 \leq \tau_1(t) \leq \tau_1$, $0 \leq \dot{\tau}_1(t) \leq \bar{\tau}_1 < 1$; $A = (a_{ij})_{N\times N} \in R^{N\times N}$ is the non-delayed output-coupling weight matrix with $a_{ii} = -\sum_{j=1,j\neq i}^{N} a_{ij}$, $a_{ii} \leq 0$, $i \in \mathcal{V}$; $\sum_{j\in\mathcal{P}_k} a_{ij} = 0$, $i \in \mathcal{P}_k$, $k \in \mathcal{M}$; $B = (b_{ij})_{N\times N} \in R^{N\times N}$ stands for the delayed output-coupling weight matrix with $b_{ii} = -\sum_{j=1,j\neq i}^{N} b_{ij}$, $b_{ii} \leq 0$, $i \in \mathcal{V}$; $\sum_{j\in\mathcal{P}_k} b_{ij} = 0$, $i \in \mathcal{P}_k$, $k \in \mathcal{M}$; $\Lambda_1 = \mathrm{diag}\{\lambda_{11}, \cdots, \lambda_{1n}\} > 0$, $\Lambda_2 = \mathrm{diag}\{\lambda_{21}, \cdots, \lambda_{2n}\} > 0$, represent the non-delayed inner-coupling matrix and delay inner-coupling matrix, respectively; $g_1(x_j(t)) = (g_{11}(x_{j1}(t)), \cdots, g_{1n}(x_{jn}(t)))^T$ means the nonlinearly non-delayed coupling vector function and $g_2(x_j(t-\tau_2(t))) = (g_{21}(x_{j1}(t-\tau_2(t))), \cdots, g_{2n}(x_{jn}(t-\tau_2(t))))^T$ means the nonlinearly delayed coupling vector function, where $j = 1, \cdots, N$, $0 \leq \tau_2(t) \leq \tau_2$, $0 \leq \dot{\tau}_2(t) \leq \bar{\tau}_2 < 1$; and $u_i(t)=(u_{i1}(t), \cdots, u_{in}(t))^T \in R^n$ is the control input of the ith node. Besides, the initial state of system (1) is defined as $x_i(r) = \xi_i(r)$, $r \in [-\tau_M, 0]$, $\tau_M = \max\{\tau_1, \tau_2\}$, $i \in \mathcal{V}$.

Our objective is to synchronize the CDN (1) of N nodes with $\bar{m}$ desired heterogeneous states, which can be $\bar{m}$ different reference trajectories, $\bar{m}$ equilibrium points, $\bar{m}$ periodic orbits or $\bar{m}$ chaotic attractors, event in the presence of deception attacks. For this purpose, we denote such $\bar{m}$ desired heterogeneous states by $s_k(t) \in R^n$, $k \in \mathcal{M}$, which are defined in accordance with the following equation:

$$\dot{s}_k(t) = W_{1k} f_k(s_k(t)) + W_{2k} f_k(s_k(t-\tau_1(t))), \tag{2}$$

where $W_{1k} = \check{W}_{1i}$, $W_{2k} = \check{W}_{2i}$, $f_k(\cdot) = \check{f}_i(\cdot)$, $i \in \mathcal{P}_k = \{l_{k-1}+1, \cdots, l_k\}$, $i \in \mathcal{V}$, $k \in \mathcal{M}$. The initial state of system (2) is defined as $s_k(r) = \hat{\xi}_k(r)$, $r \in [-\tau_1, 0]$.

Combining the CDN in (1) and the heterogeneous states in (2), the objective is to design a suitable cluster synchronization controller $u_i(t)$ for each node i belonging to the cluster $\mathcal{P}_k$ such that $x_i(t) \to s_k(t)$ for any $i \in \mathcal{P}_k$ and $k \in \mathcal{M}$. Then, it is clear that

$$\mathcal{S}(t) = (\overbrace{s_1(t), \cdots, s_1(t)}^{n_1}, \cdots, \overbrace{s_{\bar{m}}(t), \cdots, s_{\bar{m}}(t)}^{n_{\bar{m}}})$$

denotes the desired cluster synchronization pattern under the proposed synchronization controller.

Furthermore, the nonlinear functions satisfy the following mild assumption.

Assumption 1 ([1]). *There exist real constant matrices Γ_{1k} and Γ_{2k} with $\Gamma_{2k} - \Gamma_{1k} \geq 0$, $k \in \mathcal{M}$, such that for any $w, v \in R^n$, the following inequality holds*

$$(f_k(w) - f_k(v) - \Gamma_{1k}(w-v))^T (f_k(w) - f_k(v) - \Gamma_{2k}(w-v)) \leq 0. \tag{3}$$

Remark 1. *For the nonlinear function $f_k(\cdot)$ which describes the internal dynamics of nodes in cluster k, the difference between its values at two arbitrary states w and v can be 'sandwiched' between two linear functions. In other words, $f_k(\cdot)$ does not grow faster than a linear rate—this prevents unbounded nonlinearity from destabilizing the network. For example, let $f_k(x) = \tanh(x)$, we can choose $\Gamma_{1k} = 0$ and $\Gamma_{2k} = I_n$. For any w and v, $(\tanh(w) - \tanh(v))^T(\tanh(w) - \tanh(v) - I_m(w-v)) \leq 0$.*

Assumption 2. *There exist scalars δ_1, $\delta_2 > 0$ such that for any $w, v \in R^{n\times n}$, the following inequalities hold*

$$(g_1(w) - g_1(v))^T(g_1(w) - g_1(v)) \le \delta_1(w-v)^T(w-v),$$
$$(g_2(w) - g_2(v))^T(g_2(w) - g_2(v)) \le \delta_2(w-v)^T(w-v).$$

Remark 2. *For the coupling nonlinear functions $g_1(\cdot)$ and $g_2(\cdot)$ which describe interactions between nodes, the 'size' (Euclidean norm) of the difference between their values at two states w and v is at most a constant multiple of the 'size' of the state difference $w - v$. For example, let $g_1(t) = (0.3\sin(x_1), 0.4\tanh(x_2))^T$, we can choose $\delta_1 = 0.23$.*

2.3. A Dynamic Event-Triggered Transmission Mechanism

To solve the above cluster synchronization problem, the widely-adopted synchronization controller takes the following form of

$$u_i(t) = K_i e_i(t) = K_i(x_i(t) - s_k(t)), \ \ \forall\, i \in \mathcal{P}_k, k \in \mathcal{M}, \tag{4}$$

where $K_i > 0$ is the controller gain to be designed and $e_i(t)$ represents the cluster synchronization error.

It is clear that the error signal $e_i(t)$ in (4) on node $i \in \mathcal{P}_k$ has to be transmitted to the controller at every continuous time instant t. This may cause excessive usage of the limited computation and communication resources of each node and the network medium. In the following section, a dynamic event-triggered mechanism is considered under which the cluster synchronization controller in (4) can be updated in an intermittent manner.

For any $i \in \mathcal{P}_k$, let the triggering time sequence be denoted by $\{t_q^i\}_{q=1}^{+\infty}$ with $0 = t_1^i < t_2^i < \cdots < t_q^i < \cdots$. Then, the following triggering mechanism specifies how the triggering times can be recursively determined

$$\begin{aligned} t_{q+1}^i = \inf\{t > t_q^i \mid \pi_i\eta_i(t) + \theta_i[\zeta_i e_i^T(t)\Psi_i e_i(t) \\ - (e_i(t) - e_i(t_q^i))^T\Psi_i(e_i(t) - e_i(t_q^i))] > 0\}, \end{aligned} \tag{5}$$

where Ψ_i is positive define matrix, $\pi_i > 0$, $\theta_i > 0$, $\zeta_i \in (0,1)$, $i \in \mathcal{P}_k$, and $\eta_i(t)$ is an auxiliary dynamic variable satisfying

$$\dot{\eta}_i(t) = -\varrho_i\eta_i(t) + \zeta_i e_i^T(t)\Psi_i e_i(t) - (e_i(t) - e_i(t_q^i))^T\Psi_i(e_i(t) - e_i(t_q^i)), \tag{6}$$

where $\eta_i(0) = \eta_{i0} > 0$ and $\varrho_i > 0$, $i \in \mathcal{P}_k$.

Remark 3. *The triggered condition $\pi_i\eta_i(t) + \theta_i[\zeta_i e_i^T(t)\Psi_i e_i(t) - (e_i(t) - e_i(t_q^i))^T\Psi_i(e_i(t) - e_i(t_q^i))] > 0$ in (5) means that only when the current data (error) $e_i(t)$ satisfying the inequality will be triggered and released. From the sensor's perspective, this basically means that the continuous data $e_i(t)$ has no need to be persistently transmitted to the controller. Meanwhile, at the controller side, during $[t_q^i, t_{q+1}^i)$, the controller will not be updated with any new data but instead using the previously triggered data $e_i(t_q^i)$, namely, $u_i(t) = K_i e_i(t)$ for any $t \in [t_q^i, t_{q+1}^i)$. As a result, compared with the continuous-time cluster synchronization controller (4), the consumption of computation and communication resources of the sensor and controller can be significantly reduced under the above event-triggered cluster synchronization controller. On the other hand, the auxiliary dynamic variable $\eta_i(t)$ possesses an important non-negative feature which plays an important role in reducing the frequency of data transmissions. Specifically, it is easy to get that $\zeta_i e_i^T(t)\Psi_i e_i(t) - (e_i(t) - e_i(t_q^i))^T\Psi_i(e_i(t) - e_i(t_q^i)) > -\dfrac{\pi_i\eta_i(t)}{\theta_i}$ during $[t_q^i, t_{q+1}^i)$. Then, it*

follows from (6) that $\dot{\eta}_i(t) > -\varrho_i\eta_i(t) - \dfrac{\pi_i\eta_i(t)}{\theta_i}$, *which leads to* $\eta_i(t) \geq 0$ *for* $t \in [0, +\infty)$ *based on the comparison principle.*

Remark 4. π_i *and* ϱ_i *primarily suppress unnecessary triggers by adjusting the auxiliary variable's influence, while* θ_i *and* ζ_i *directly tune the sensitivity of the error-based triggering condition—properly selecting them balances communication resource savings and synchronization performance. The Table 2 shows the selection guidelines of parameters.*

Table 2. Parameter → Effect on Triggering Frequency.

Parameter	Core Effect on Triggering Frequency	Simple Selection Guidelines
π_i	Larger $\pi_i \rightarrow$ Lower frequency	Choose a moderate value (e.g., 0.1–0.5) based on resource constraints.
θ_i	Larger $\theta_i \rightarrow$Higher frequency	Set to a value that avoids excessive triggers (e.g., 1–5).
ζ_i	Larger ζ_i (within $(0,1)$) $\rightarrow$Higher frequency	Select between 0.2–0.8.
ϱ_i	Larger $\varrho_i \rightarrow$Lower frequency	Choose a value matching the system's time scale (e.g., 0.5–2).

2.4. Modeling of Random Deception Attacks

Once the data packet $(t_q^i, e_i(t_q^i))$ with its time stamp t_q^i is triggered, it will be released over certain communication network or channel. Such a released data packet is considered to be important for achieving the desired cluster synchronization objective. However, most realistic communication networks suffer from inherent security vulnerabilities due to their openness or insufficient protection against malicious cyber attacks. To make the desired cluster synchronization controller resilient and secure to malicious cyber attacks, it is thus imperative to incorporate cyber attacks into the controller design. In doing so, we first present the following random deception attack model

$$\bar{e}_i(t) = \alpha(t)h(e_i(t_q^i)) + (1-\alpha(t))e_i(t_q^i),\ t \in [t_q^i, t_{q+1}^i) \tag{7}$$

for any $\forall\, i \in \mathcal{P}_k$, $k \in \mathcal{M}$, where $\bar{e}_i(t)$ represents the actually received data at the controller side, $h(e_i(t_q^i))$ denotes the deception data or signal injected by attackers over the network or during network transmission. For simplicity and without loss of generality, it is assumed that $h(v) = (h_1(v), \cdots, h_n(v))^T$, $h_i(v)$, $i = 1, \cdots, n$, is a continuous function, and for $\forall v_1, v_2 \in R^n$, $h(\cdot)$ satisfies $(h(v_1) - h(v_2))^T\ (h(v_1) - h(v_2)) \leq (v_1 - v_2)^T H(v_1 - v_2)$, $h(0) = 0$, where $H \in R^{n\times n}$ is a known positive definite matrix. The function $h(\cdot)$ represents the adversary's falsification strategy, for example, scaling, offsetting, or distorting the original error signal $e_i(t_q^i)$ to produce the attacked signal $h(e_i(t_q^i))$. The matrix H serves as a bound on the attack's maximum allowable distortion. Such a bounding assumption on the deception signal is reasonable since (1) realistic adversaries are often energy-limited and may not be able to inject arbitrarily large data packets, and (2) arbitrarily large injection signalS may be easily detected by the existing anomaly detector via checking the data residue.

Furthermore, $\alpha(t)$ in (7) is a Bernoulli distribution variable satisfying $\Pr(\mathrm{ff(t)} = 1) = \bar{\mathrm{ff}}$ and $\Pr(\mathrm{ff(t)} = 0) = 1 - \bar{\mathrm{ff}}$, where $\bar{\alpha} \in (0,1)$ is known constant. Such a stochastic variable is introduced to model the random characteristics of real-world deception attacks. Since our focus is placed on the deception attacks occurring within the network channels or during networked data transmission, it is mild to assume a homogeneous stochastic variable $\alpha(t)$ for all the network channels. The Bernoulli-distributed attack model adopted in this paper is a simplified yet practical choice, and its rationale lies in two key aspects aligned

with real-world scenarios: First, it effectively captures the binary 'hit-or-miss' nature of deception attacks—in actual communication channels, an attacker either injects falsified data (attack occurs) or does not interfere (no attack), and the Bernoulli variable directly maps this discrete stochasticity. Second, the model's statistical property ($\mathbb{E}[\alpha(t)] = \bar{\alpha}$) enables tractable mean-square stability analysis, which is critical for deriving explicit linear matrix inequality (LMI) conditions and feasible controller gains—an essential step for validating the proposed secure synchronization framework through both theoretical proofs and numerical simulations.

Remark 5. *While recent work on deception attacks focuses on output feedback PID control or switched system resilience, our study uniquely integrates dynamic event-triggered mechanisms with cluster synchronization, addressing the under-explored challenge of secure grouping in complex networks rather than full-network consensus. Unlike the static event-triggered designs, our auxiliary variable-based triggering rule (6) adaptively adjusts to random deception attacks. Compared to works handling asynchronous DoS attacks via linear auxiliary trajectories [19], we explicitly model deception attack dynamics with a Bernoulli variable and bounded disturbance matrix H, providing verifiable guidelines for H estimation that are absent in prior LMI-based resilient control frameworks.*

2.5. The Problem to Be Addressed

Based on the dynamic event-triggered mechanism (5) and attack model (7), we are interested in constructing and design the following cluster synchronization controller

$$u_i(t) = K_i \bar{e}_i(t), \quad t \in [t_q^i, t_{q+1}^i). \tag{8}$$

From (5)–(8), for $t \in [t_q^i, t_{q+1}^i)$, the synchronization error dynamics can be written as

$$\begin{aligned}\dot{e}_i(t) =& W_{1k}\bar{f}_k(e_i(t)) + W_{2k}\bar{f}_k(e_i(t-\tau_1(t))) + \sum_{j=1}^{N} a_{ij}\Lambda_1\bar{g}_1(e_j(t)) + \sum_{j=1}^{N} b_{ij}\Lambda_2\bar{g}_2(e_j(t-\tau_2(t)))\\ &+ \alpha(t)K_i h(e_i(t_q^i)) + (1-\alpha(t))K_i e_i(t_q^i),\end{aligned} \tag{9}$$

where $\bar{f}_k(e_i(t)) = f_k(x_i(t)) - f_k(s_k(t))$, $\bar{f}_k(e_i(t-\tau_1(t))) = f_k(x_i(t-\tau(t))) - f_k(s_k(t-\tau_1(t)))$, $\bar{g}_1(e_i(t)) = g_1(x_i(t)) - g_1(s_k(t))$, $\bar{g}_2(e_i(t-\tau_2(t))) = g_2(x_i(t-\tau_2(t))) - g_2(s_k(t-\tau_2(t)))$, $i \in \mathcal{P}_k$, $k \in \mathcal{M}$, $i \in \mathcal{V}$.

Furthermore, let $\epsilon_i(t) = e_i(t) - e_i(t_q^i)$, $t \in [t_q^i, t_{q+1}^i)$, $\tilde{e}_k(t) = (e_{l_{k-1}+1}^T(t), \cdots, e_{l_k}^T(t))^T$, $k \in \mathcal{M}$. The error system can be rewritten as, for $k \in \mathcal{M}$,

$$\begin{aligned}\dot{\tilde{e}}_k(t) =& \bar{W}_{1k}\bar{F}_k(\tilde{e}_k(t)) + \bar{W}_{2k}\bar{F}_k(\tilde{e}_k(t-\tau_1(t))) + \sum_{j=1}^{\bar{m}} \tilde{A}_{kj} \otimes \Lambda_1\bar{G}_1(\tilde{e}_j(t))\\ &+ \sum_{j=1}^{\bar{m}} \tilde{B}_{kj} \otimes \Lambda_2\bar{G}_2(\tilde{e}_j(t-\tau_2(t))) + (\alpha(t)-\bar{\alpha})\tilde{K}_k\bar{H}_k(\tilde{e}_k(t) - \tilde{\epsilon}_k(t))\\ &+ \bar{\alpha}\tilde{K}_k\bar{H}_k(\tilde{e}_k(t) - \tilde{\epsilon}_k(t)) + (1-\bar{\alpha})\tilde{K}_k(\tilde{e}_k(t) - \tilde{\epsilon}_k(t)) - (\alpha(t)-\bar{\alpha})\tilde{K}_k(\tilde{e}_k(t) - \tilde{\epsilon}_k(t)),\end{aligned}$$

where

$$\begin{aligned}\bar{W}_1 = \mathrm{diag}\{\overbrace{W_{1k}, \cdots, W_{1k}}^{n_k}\}, \quad \bar{W}_2 = \mathrm{diag}\{\overbrace{W_{2k}, \cdots, W_{2k}}^{n_k}\},\\ \bar{F}_k(\tilde{e}_k(t)) = (\bar{f}_k^T(e_{l_{k-1}+1}(t)), \cdots, \bar{f}_k^T(e_{l_k}(t))^T,\\ \bar{F}_k(\tilde{e}_k(t-\tau_1(t))) = (\bar{f}_k^T(e_{l_{k-1}+1}(t-\tau_1(t))), \cdots, \bar{f}_k^T(e_{l_k}(t-\tau_1(t))))^T,\end{aligned}$$

$$\tilde{A}_{kj} = \begin{pmatrix} a_{l_{k-1}+1,l_{j-1}+1} & \cdots & a_{l_{k-1}+1,l_j} \\ \vdots & & \vdots \\ a_{l_k,l_{j-1}+1} & \cdots & a_{l_k,l_j} \end{pmatrix} \in R^{n_k \times n_j},$$

$$\bar{G}_1(\tilde{e}_j(t)) = (\bar{g}_1^T(e_{l_{j-1}+1}(t)), \cdots, \bar{g}_1^T(e_{l_j}(t)))^T,$$

$$\tilde{B}_{kj} = \begin{pmatrix} b_{l_{k-1}+1,l_{j-1}+1} & \cdots & b_{l_{k-1}+1,l_j} \\ \vdots & & \vdots \\ b_{l_k,l_{j-1}+1} & \cdots & b_{l_k,l_j} \end{pmatrix} \in R^{n_k \times n_j},$$

$$\bar{G}_2(\tilde{e}_j(t-\tau_2(t))) = (\bar{g}_2^T(e_{l_{j-1}+1}(t-\tau_2(t))), \cdots, \bar{g}_2^T(e_{l_j}(t-\tau_2(t))))^T,$$

$$\tilde{K}_k = \mathrm{diag}\{\overbrace{K_{l_{k-1}+1}, \cdots, K_{l_{k-1}+n_k}}^{n_k}\},$$

$$\tilde{\epsilon}_k(t) = (\epsilon_{l_{k-1}+1}^T(t), \cdots, \epsilon_{l_k}^T(t))^T,$$

$$\bar{H}_k(\tilde{e}_k(t) - \tilde{\epsilon}_k(t)) = (h^T(e_{l_{k-1}+1}(t) - \epsilon_{l_{k-1}+1}(t)), \cdots, h^T(e_{l_k}(t) - \epsilon_{l_k}(t)))^T.$$

The main problem to be addressed in this paper can now be stated as follows.

Problem 1. *For the CDNs in (1), we aim to design a secure dynamic event-triggered cluster synchronization controller in the form of (8) such that the desired secure cluster synchronization objective is achieved regardless of the simultaneous effects of intermittent data transmission under (5) and random deception attacks under (7), i.e.,* $E\{\sum_{i=l_{k-1}+1}^{l_k} \|e_i(t)\|\} = 0$ *as* $t \to +\infty$ *for any* $k \in \mathcal{M}$ *and initial condition.*

Before ending this section, some definitions, assumption, lemmas are recalled.

Definition 1 ([15]). *Consider* $D = (d_{ij}) \in R^{N\times N}$. *If*

(1) $d_{ij} \geq 0$, *for* $i \neq j$, *and* $d_{ii} = -\sum_{j=1,j\neq i}^{N} d_{ij} = -\sum_{j=1,j\neq i}^{N} d_{ji}$, $i = 1, 2, \cdots, N$.

(2) D is irreducible.

Then we say $D \in \mathcal{D}_1$.

Definition 2 ([15]). *For an* $N \times N$ *matrix*

$$D = \begin{pmatrix} D_{11} & D_{12} & \cdots & D_{1m} \\ D_{21} & D_{22} & \cdots & D_{2m} \\ & & \cdots & \\ D_{m1} & D_{m2} & \cdots & D_{mm} \end{pmatrix},$$

with $D_{ii} \in R^{(l_i-l_{i-1})\times(l_i-l_{i-1})}$, $D_{ij} \in R^{(l_i-l_{i-1})\times(l_j-l_{j-1})}$, $i, j = 1, 2, \cdots, m$, *if each block* D_{ij} *is a zero-row-sum matrix, then we say* $D \in \mathcal{D}_1(m)$. *Furthermore, if* $D_{ii} \in \mathcal{D}_1$, $i = 1, 2, \cdots, d$, *then we say* $D \in \mathcal{D}_2(m)$.

Assumption 3. *The coupling matrix A in (1) satisfies* $A \in \mathcal{D}_2(\bar{m})$, $B \in \mathcal{D}_2(\bar{m})$.

Remark 6. *The non-delay coupling matrix A and delayed coupling matrix B must have two properties. (1) For each cluster, the sum of coupling weights from any node in the cluster to all other nodes in the same cluster is zero which ensures internal cluster balance. (2) Each submatrix of A and B corresponding to a single cluster is 'irreducible', in other words, no isolated nodes in the*

cluster. For example, consider a CDN with 2 *clusters:* $P_1 = \{1, 2\}$, $P_2 = \{3, 4\}$. *We can choose the non-delayed coupling matrix:*

$$\begin{bmatrix} -1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & -2 & 2 \\ 0 & 0 & 2 & -2 \end{bmatrix}.$$

Lemma 1 ([41]). *For any constant positive matrix* $M \in R^{m\times m}$, *scalar* $\hat{\tau} \le \tau(t) < \bar{\tau}$ *and vector function* $\dot{e}(t) : [-\bar{\tau}, \hat{\tau}] \to R^m$ *such that the following integration is well defined, then it holds that*

$$\begin{aligned} & -(\bar{\tau} - \hat{\tau}) \int_{t-\bar{\tau}}^{t-\hat{\tau}} (\dot{e}(\vartheta))^T M \dot{e}(\vartheta) \mathrm{d}\vartheta \\ & \le \begin{bmatrix} e(t-\bar{\tau}) \\ e(t-\tau(t)) \\ e(t-\hat{\tau}) \end{bmatrix}^T \begin{bmatrix} -M & M & 0 \\ * & -2M & M \\ * & * & M \end{bmatrix} \begin{bmatrix} e(t-\bar{\tau}) \\ e(t-\tau(t)) \\ e(t-\hat{\tau}) \end{bmatrix}. \end{aligned} \tag{10}$$

Lemma 2. *(Schur Complement) Given matrices* U_1, U_2, U_3, *where* $U_1^T = U_1$, $U_3^T = U_3 > 0$, *then* $U_1 + U_2 U_3^{-1} U_2^T < 0$ *if and only if*

$$\begin{bmatrix} U_1 & U_2 \\ U_2^T & -U_3 \end{bmatrix} < 0, \quad \begin{bmatrix} -U_3 & U_2^T \\ U_2 & U_1 \end{bmatrix} < 0. \tag{11}$$

Lemma 3. *For any matrices* $\mathcal{R} > 0$, $\mathcal{Q}$ *and scalar* ι, *the following inequality holds*

$$-\mathcal{Q}\mathcal{R}^{-1}\mathcal{Q} \le \iota^2 \mathcal{R} - 2\iota\mathcal{Q}. \tag{12}$$

For the sake of simplicity, some mathematical notations are introduced as follows.

$$e(t) = \left(\tilde{e}_1^T(t), \cdots, \tilde{e}_{\bar{m}}^T(t)\right)^T, \ \epsilon(t) = \left(\tilde{\epsilon}_1^T(t), \cdots, \tilde{\epsilon}_{\bar{m}}^T(t)\right)^T,$$

$$\begin{aligned} z(t) \quad = \quad & \Big(e^T(t), e^T(t-\tau_1(t)), e^T(t-\tau_1), e^T(t-\tau_2(t)), \\ & e^T(t-\tau_2), \bar{F}^T(e(t)), \bar{F}^T(e(t-\tau_1(t))), \bar{G}_1^T(e(t)), \\ & \bar{G}_2^T(e(t-\tau_2(t))), \bar{H}^T(e(t)-\epsilon(t)), \epsilon^T(t)\Big)^T, \end{aligned}$$

$$\Phi = ((1-\bar{\alpha})\tilde{K}, 0, 0, 0, 0, \tilde{W}_1, \tilde{W}_2, \mathcal{A}, \mathcal{B}, \bar{\alpha}\tilde{K}, -(1-\bar{\alpha})\tilde{K}),$$

$$\bar{F}(e(t)) = (\bar{F}_1^T(\tilde{e}_1(t)), \cdots, \bar{F}_{\bar{m}}^T(\tilde{e}_{\bar{m}}(t))^T,$$

$$\bar{F}(e(t-\tau_1(t))) = (\bar{F}_1^T(\tilde{e}_1(t-\tau_1(t))), \cdots, \bar{F}_{\bar{m}}^T(\tilde{e}_{\bar{m}}(t-\tau_1(t))))^T,$$

$$\bar{G}_1(e(t)) = (\bar{G}_1^T(\tilde{e}_1(t)), \cdots, \bar{G}_1^T(\tilde{e}_{\bar{m}}(t)))^T,$$

$$\bar{G}_2(e(t-\tau_2(t))) = (\bar{G}_2^T(\tilde{e}_1(t-\tau_2(t))), \cdots, \bar{G}_2^T(\tilde{e}_{\bar{m}}(t-\tau_2(t))))^T,$$

$$\tilde{W}_1 = \mathrm{diag}\{\bar{W}_{11}, \cdots, \bar{W}_{1\bar{m}}\}, \tilde{W}_2 = \mathrm{diag}\{\bar{W}_{21}, \cdots, \bar{W}_{2\bar{m}}\},$$

$$\mathcal{A} = \begin{pmatrix} \tilde{A}_{11} \otimes \Lambda_1 & \cdots & \tilde{A}_{1\bar{m}} \otimes \Lambda_1 \\ \vdots & & \vdots \\ \tilde{A}_{\bar{m}1} \otimes \Lambda_1 & \cdots & \tilde{A}_{\bar{m}\bar{m}} \otimes \Lambda_1 \end{pmatrix},$$

$$\mathcal{B} = \begin{pmatrix} \tilde{B}_{11} \otimes \Lambda_2 & \cdots & \tilde{B}_{1\bar{m}} \otimes \Lambda_2 \\ \vdots & & \vdots \\ \tilde{B}_{\bar{m}1} \otimes \Lambda_2 & \cdots & \tilde{B}_{\bar{m}\bar{m}} \otimes \Lambda_2 \end{pmatrix},$$

$$\bar{H}(e(t)-\epsilon(t)) = (\bar{H}_1^T(\tilde{e}_1(t)-\tilde{\epsilon}_1(t)),\cdots,\bar{H}_{\bar{m}}^T(\tilde{e}_{\bar{m}}(t)-\tilde{\epsilon}_{\bar{m}}(t)))^T,$$
$$\epsilon(t) = (\tilde{\epsilon}_1(t),\cdots,\tilde{\epsilon}_{\bar{m}}(t))^T, \tilde{K} = \mathrm{diag}\{\tilde{K}_1,\cdots,\tilde{K}_{\bar{m}}\},$$
$$\Theta_1 = \mathrm{diag}\{\theta_1\Psi_1,\cdots,\theta_N\Psi_N\},$$
$$\Theta_2 = \mathrm{diag}\{\theta_1\zeta_1\Psi_1,\cdots,\theta_N\zeta_N\Psi_N\},$$
$$\Theta_3 = \mathrm{diag}\{\zeta_1\Psi_1,\cdots,\zeta_N\Psi_N\},$$
$$\Psi = \mathrm{diag}\{\Psi_1,\cdots,\Psi_N\},$$
$$\mathcal{H} = I_N \otimes H = \mathrm{diag}\{\overbrace{H,\cdots,H}^{N}\},$$
$$\tilde{\Gamma}_k = -\frac{\Gamma_{1k}^T+\Gamma_{2k}^T}{2},\ \bar{\Gamma}_k = \frac{\Gamma_{1k}^T\Gamma_{2k}+\Gamma_{2k}^T\Gamma_{1k}}{2},$$
$$\tilde{\Gamma} = \mathrm{diag}\{\tilde{\Gamma}_1,\cdots,\tilde{\Gamma}_1,\cdots,\tilde{\Gamma}_{\bar{m}},\cdots,\tilde{\Gamma}_{\bar{m}}\},$$
$$\bar{\Gamma} = \mathrm{diag}\{\bar{\Gamma}_1,\cdots,\bar{\Gamma}_1,\cdots,\bar{\Gamma}_{\bar{m}},\cdots,\bar{\Gamma}_{\bar{m}}\}.$$

3. Main Results

3.1. The Dynamic Event-Triggered Case

This subsection aims to deal with the secure cluster synchronization issue of CDNs (1) under dynamic event-triggered scheme and design suitable pinning controllers. Firstly, a theorem about secure cluster synchronization of CDNs under deception attacks is given.

Theorem 1. *Consider the CDNs in (1), suppose that Assumptions 1–3 hold. For given parameters* $\tau_M > 0$, $\bar{\tau}_1, \bar{\tau}_2 \in [0,1)$, $\pi_i > 0$, $\theta_i > 0$, $\zeta_i > 0$, $\eta_i(0) > 0$, $\varrho_i > 0$, $i \in \mathcal{V}$; $\bar{\alpha} \in (0,1)$, $\delta_1 > 0$, $\delta_2 > 0$, $\rho_k > 0$, $\varpi_k > 0$, $n_k, p_k \in \mathcal{N}^+$, $k \in \mathcal{M}$, $\beta > 0$, $\lambda \in (0,\beta)$, *and matrices* $H > 0$ *and* K_i, $i \in \mathcal{V}$, *if there exist scalars* $\iota_q > 0$, $q = 1,\cdots,6$, *positive define matrices* $\tilde{Q}_k$, $\tilde{R}_{1k}$, $\tilde{R}_{2k}$, $\tilde{R}_{3k}$, $\tilde{R}_{4k}$, $\tilde{M}_{1k}$, $\tilde{M}_{2k}$, $k \in \mathcal{M}$ *such that*

$$\iota_1\pi_i + \lambda - \varrho_i \le 0,\ i \in \mathcal{V}, \tag{13}$$

$$\tilde{\mathcal{D}} = \begin{bmatrix} \bar{\mathcal{D}} & \tau_1^2\Phi^T & \tau_2^2\Phi^T \\ * & -\tau_1^2\tilde{M}_1^{-1} & 0 \\ * & * & -\tau_2^2\tilde{M}_2^{-1} \end{bmatrix} < 0 \tag{14}$$

hold, where

$$\bar{\mathcal{D}} = \begin{bmatrix} \mathcal{D}_{11}+\Theta_3 & \mathcal{D}_{12} & 0 & \mathcal{D}_{14} & 0 & \mathcal{D}_{16} & \mathcal{D}_{17} & \mathcal{D}_{18} & \mathcal{D}_{19} & \mathcal{D}_{10} & \mathcal{D}_{111} \\ * & \mathcal{D}_{22} & \mathcal{D}_{23} & 0 & 0 & 0 & \mathcal{D}_{27} & 0 & 0 & 0 & 0 \\ * & * & \mathcal{D}_{33} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & \mathcal{D}_{44} & \mathcal{D}_{45} & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & \mathcal{D}_{55} & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & * & \mathcal{D}_{66} & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & * & * & \mathcal{D}_{77} & 0 & 0 & 0 & 0 \\ * & * & * & * & * & * & * & \mathcal{D}_{88} & 0 & 0 & 0 \\ * & * & * & * & * & * & * & * & \mathcal{D}_{99} & 0 & 0 \\ * & * & * & * & * & * & * & * & * & \mathcal{D}_{00} & 0 \\ * & * & * & * & * & * & * & * & * & * & \bar{\mathcal{D}}_{1111} \end{bmatrix},$$

$$\begin{aligned}
\mathcal{D}_{11} =& (1-\bar{\alpha})(\tilde{Q}\tilde{K}+\tilde{K}^T\tilde{Q})+\tilde{R}_1+\tilde{R}_3+\iota_1\Theta_2+\iota_4\delta_1 I_{nN}-\iota_2\bar{\Gamma}+\iota_6\mathcal{H}-\tilde{M}_1-\tilde{M}_2,\\
\mathcal{D}_{12} =& \tilde{M}_1,\ \mathcal{D}_{14}=\tilde{M}_2,\ \mathcal{D}_{16}=\tilde{Q}\tilde{W}_1-\iota_2\tilde{\Gamma},\mathcal{D}_{17}=\tilde{Q}\tilde{W}_2,\mathcal{D}_{18}=\tilde{Q}\mathcal{A},\ \mathcal{D}_{19}=\tilde{Q}\mathcal{B},\\
\mathcal{D}_{10} =& \bar{\alpha}\tilde{Q}\tilde{K},\ \mathcal{D}_{111}=-\iota_6\mathcal{H}-(1-\bar{\alpha})\tilde{Q}\tilde{K},\mathcal{D}_{22}=-(1-\bar{\tau}_1)\tilde{R}_1+\tilde{R}_2-\iota_2\bar{\Gamma}-2\tilde{M}_1,\\
\mathcal{D}_{23} =& \tilde{M}_1,\ \mathcal{D}_{27}=-\iota_3\tilde{\Gamma},\mathcal{D}_{33}=-\tilde{R}_2-\tilde{M}_1,\mathcal{D}_{44}=-(1-\bar{\tau}_2)\tilde{R}_3+\tilde{R}_4+\iota_5\delta_2 I_{nN}-2\tilde{M}_2,\\
\mathcal{D}_{45} =& \tilde{M}_2,\ \mathcal{D}_{55}=-\tilde{R}_4-\tilde{M}_2,\mathcal{D}_{66}=-\iota_2 I_{nN},\mathcal{D}_{77}=-\iota_3 I_{nN},\ \mathcal{D}_{88}=-\iota_4 I_{nN},\\
\mathcal{D}_{99} =& -\iota_5 I_{nN},\ \mathcal{D}_{00}=-\iota_6 I_{nN},\bar{\mathcal{D}}_{11,11}=\mathcal{D}_{11,11}-\Psi,\ \mathcal{D}_{11,11}=-\iota_1\Theta_1+\iota_6\mathcal{H},\\
\tilde{Q} =& \mathrm{diag}\{\tilde{Q}_1,\cdots,\tilde{Q}_{\bar{m}}\},\tilde{R}_1=\mathrm{diag}\{\tilde{R}_{11},\cdots,\tilde{R}_{1\bar{m}}\},\tilde{R}_2=\mathrm{diag}\{\tilde{R}_{21},\cdots,\tilde{R}_{2\bar{m}}\},\tilde{R}_3=\mathrm{diag}\{\tilde{R}_{31},\cdots,\tilde{R}_{3\bar{m}}\},\\
\tilde{R}_4 =& \mathrm{diag}\{\tilde{R}_{41},\cdots,\tilde{R}_{4\bar{m}}\},\tilde{M}_1=\mathrm{diag}\{\tilde{M}_{11},\cdots,\tilde{M}_{1\bar{m}}\},\tilde{M}_2=\mathrm{diag}\{\tilde{M}_{21},\cdots,\tilde{M}_{2\bar{m}}\},
\end{aligned}$$

then the closed-loop networks (1) under dynamic event-triggered scheme (5) satisfying (6) is secure cluster synchronization for deception attacks satisfying (7).

Proof. Construct the following piecewise Lyapunov functional candidate

$$W(t) = \exp\{-\beta t\}V(t)+\sum_{i=1}^{N}\eta_i(t), \tag{15}$$

$$V(t) = V_1(t)+V_2(t)+V_3(t), \tag{16}$$

where $\beta > 0$, and

$$\begin{aligned}
V_1(t) =& \sum_{k=1}^{\bar{m}}\tilde{e}_k^T(t)\tilde{Q}_k\tilde{e}_k(t),\\
V_2(t) =& \sum_{k=1}^{\bar{m}}\int_{t-\tau_1(t)}^{t}\tilde{e}_k^T(\nu)\tilde{R}_{1k}\tilde{e}_k(\nu)\mathrm{d}\nu+\sum_{k=1}^{\bar{m}}\int_{t-\tau_1}^{t-\tau_1(t)}\tilde{e}_k^T(\nu)\tilde{R}_{2k}\tilde{e}_k(\nu)\mathrm{d}\nu\\
&+\sum_{k=1}^{\bar{m}}\int_{t-\tau_2(t)}^{t}\tilde{e}_k^T(\nu)\tilde{R}_{3k}\tilde{e}_k(\nu)\mathrm{d}\nu+\sum_{k=1}^{\bar{m}}\int_{t-\tau_2}^{t-\tau_2(t)}\tilde{e}_k^T(\nu)\tilde{R}_{4k}\tilde{e}_k(\nu)\mathrm{d}\nu,\\
V_3(t) =& \tau_1\sum_{k=1}^{\bar{m}}\int_{-\tau_1}^{0}\int_{t+\vartheta}^{t}\dot{\tilde{e}}_k^T(\nu)\tilde{M}_{1k}\dot{\tilde{e}}_k^T(\nu)\mathrm{d}\nu\mathrm{d}\vartheta+\tau_2\sum_{k=1}^{\bar{m}}\int_{-\tau_2}^{0}\int_{t+\vartheta}^{t}\dot{\tilde{e}}_k^T(\nu)\tilde{M}_{2k}\dot{\tilde{e}}_k^T(\nu)\mathrm{d}\nu\mathrm{d}\vartheta
\end{aligned}$$

where $\tilde{Q}_k = \mathrm{diag}\{Q_{l_{k-1}+1},\cdots,Q_{l_k}\}$, $\tilde{R}_{ik} = \mathrm{diag}\{R_{i,l_{k-1}+1},\cdots,R_{i,l_k}\}$, $i = 1,2,3,4$, $\tilde{M}_{ik} = \mathrm{diag}\{M_{i,l_{k-1}+1},\cdots,M_{i,l_k}\}$, $i = 1,2$; Q_l, $R_{i,l}$, M_{1l}, M_{2l}, $i = 1,2,3$, $l = 1,\cdots,N$, are symmetric positive define matrice with appropriate dimensions.

From Remark 3 and the definition of $V(t)$, we have $W(t) > 0$. Then, we obtain

$$E\{\dot{V}_1(t)\} = E\left\{\sum_{k=1}^{\bar{m}}2\tilde{e}_k^T(t)\tilde{Q}_k\dot{\tilde{e}}_k(t)\right\}, \tag{17}$$

$$
\begin{aligned}
E\{\dot{V}_2(t)\} = E\Bigg\{ & \sum_{k=1}^{\bar{m}} \tilde{e}_k^T(t)(\tilde{R}_{1k}+\tilde{R}_{3k})\tilde{e}_k(t) - (1-\dot{\tau}_1(t))\sum_{k=1}^{\bar{m}} \tilde{e}_k^T(t-\tau_1(t))\tilde{R}_{1k}\tilde{e}_k(t-\tau_1(t)) \\
& - (1-\dot{\tau}_2(t))\sum_{k=1}^{\bar{m}} \tilde{e}_k^T(t-\tau_2(t))\tilde{R}_{3k}\tilde{e}_k(t-\tau_2(t)) \\
& + (1-\dot{\tau}_1(t))\sum_{k=1}^{\bar{m}} \tilde{e}_k^T(t-\tau_1(t))\tilde{R}_{2k}\tilde{e}_k(t-\tau_1(t)) - \sum_{k=1}^{\bar{m}} \tilde{e}_k^T(t-\tau_1)\tilde{R}_{2k}\tilde{e}_k(t-\tau_1) \\
& + (1-\dot{\tau}_2(t))\sum_{k=1}^{\bar{m}} \tilde{e}_k^T(t-\tau_2(t))\tilde{R}_{4k}\tilde{e}_k(t-\tau_2(t)) - \sum_{k=1}^{\bar{m}} \tilde{e}_k^T(t-\tau_2)\tilde{R}_{4k}\tilde{e}_k(t-\tau_2)\Bigg\},
\end{aligned} \tag{18}
$$

$$
\begin{aligned}
E\{\dot{V}_3(t)\} = & E\Bigg\{\tau_1\Bigg(\sum_{k=1}^{\bar{m}}\int_{-\tau_1}^{0} \dot{\tilde{e}}_k^T(t)\tilde{M}_{1k}\dot{\tilde{e}}_k(t)\mathrm{d}\vartheta - \sum_{k=1}^{\bar{m}}\int_{-\tau_1}^{0} \dot{\tilde{e}}_k^T(t+\vartheta)\tilde{M}_{1k}\dot{\tilde{e}}_k(t+\vartheta)\mathrm{d}\vartheta\Bigg) \\
& + \tau_2\Bigg(\sum_{k=1}^{\bar{m}}\int_{-\tau_2}^{0} \dot{\tilde{e}}_k^T(t)\tilde{M}_{2k}\dot{\tilde{e}}_k(t)\mathrm{d}\vartheta - \sum_{k=1}^{\bar{m}}\int_{-\tau_2}^{0} \dot{\tilde{e}}_k^T(t+\vartheta)\tilde{M}_{2k}\dot{\tilde{e}}_k(t+\vartheta)\mathrm{d}\vartheta\Bigg)\Bigg\} \\
= & E\Bigg\{\sum_{k=1}^{\bar{m}} \tau_1^2\dot{\tilde{e}}_k^T(t)\tilde{M}_{1k}\dot{\tilde{e}}_k(t) + \sum_{k=1}^{\bar{m}} \tau_2^2\dot{\tilde{e}}_k^T(t)\tilde{M}_{2k}\dot{\tilde{e}}_k(t) - \tau_1\sum_{k=1}^{\bar{m}}\int_{t-\tau_1}^{t} \dot{\tilde{e}}_k^T(\vartheta)\tilde{M}_{1k}\dot{\tilde{e}}_k(\vartheta)\mathrm{d}\vartheta \\
& -\tau_2\sum_{k=1}^{\bar{m}}\int_{t-\tau_2}^{t} \dot{\tilde{e}}_k^T(\vartheta)\tilde{M}_{2k}\dot{\tilde{e}}_k(\vartheta)\mathrm{d}\vartheta\Bigg\}.
\end{aligned} \tag{19}
$$

From (17)–(19) and Lemma 1, we have

$$
\begin{aligned}
E\{\dot{V}_1(t)\} \le E\Bigg\{ & \sum_{k=1}^{\bar{m}} \tilde{e}_k^T(t)\tilde{Q}_k[\bar{W}_1\bar{F}_k(\tilde{e}_k(t)) + \bar{W}_2\bar{F}_k(\tilde{e}_k(t-\tau_1(t))) + \sum_{j=1}^{\bar{m}} \tilde{A}_{kj}\otimes\Lambda_1\bar{G}_1(\tilde{e}_j(t)) \\
& + \sum_{j=1}^{\bar{m}} \tilde{B}_{kj}\otimes\Lambda_2\bar{G}_2(\tilde{e}_j(t-\tau_2(t))) + (\alpha(t)-\bar{\alpha})\tilde{K}_k\bar{H}_k(\tilde{e}_k(t)-\tilde{\epsilon}_k(t)) \\
& + \bar{\alpha}\tilde{K}_k\bar{H}_k(\tilde{e}_k(t)-\tilde{\epsilon}_k(t)) + (1-\bar{\alpha})\tilde{K}_k(\tilde{e}_k(t)-\tilde{\epsilon}_k(t)) - (\alpha(t)-\bar{\alpha})\tilde{K}_k(\tilde{e}_k(t)-\tilde{\epsilon}_k(t))]\Bigg\}
\end{aligned} \tag{20}
$$

$$
\begin{aligned}
E\{\dot{V}_2(t)\} \le E\Big\{ & e^T(t)(\tilde{R}_1+\tilde{R}_3)e(t) - e^T(t-\tau_1)\tilde{R}_2e(t-\tau_1) - e^T(t-\tau_2)\tilde{R}_4e(t-\tau_2) \\
& -e^T(t-\tau_1(t))((1-\bar{\tau}_1)\tilde{R}_1-\tilde{R}_2)e(t-\tau_1(t)) - e^T(t-\tau_2(t))((1-\bar{\tau}_2)\tilde{R}_3-\tilde{R}_4)e(t-\tau_2(t))\Big\},
\end{aligned} \tag{21}
$$

$$
\begin{aligned}
E\{\dot{V}_3(t)\} = & E\Bigg\{\sum_{k=1}^{\bar{m}} \tau_1^2\dot{\tilde{e}}_k^T(t)\tilde{M}_{1k}\dot{\tilde{e}}_k(t) + \sum_{k=1}^{\bar{m}} \tau_2^2\dot{\tilde{e}}_k^T(t)\tilde{M}_{2k}\dot{\tilde{e}}_k(t) \\
& - \tau_1\sum_{k=1}^{\bar{m}}\int_{t-\tau_1}^{t} \dot{\tilde{e}}_k^T(\nu)\tilde{M}_{1k}\dot{\tilde{e}}_k(\nu)\mathrm{d}\nu - \tau_2\sum_{k=1}^{\bar{m}}\int_{t-\tau_2}^{t} \dot{\tilde{e}}_k^T(\nu)\tilde{M}_{2k}\dot{\tilde{e}}_k(\nu)\mathrm{d}\nu\Bigg\} \\
\le & E\Bigg\{\begin{bmatrix} e(t) \\ e(t-\tau_1(t)) \\ e(t-\tau_1)\end{bmatrix}^T\begin{bmatrix} -\tilde{M}_1 & \tilde{M}_1 & 0 \\ * & -2\tilde{M}_1 & \tilde{M}_1 \\ * & * & \tilde{M}_1\end{bmatrix}\times\begin{bmatrix} e(t) \\ e(t-\tau_1(t)) \\ e(t-\tau_1)\end{bmatrix} + \begin{bmatrix} e(t) \\ e(t-\tau_2(t)) \\ e(t-\tau_2)\end{bmatrix}^T \\
& \times\begin{bmatrix} -\tilde{M}_2 & \tilde{M}_2 & 0 \\ * & -2\tilde{M}_2 & \tilde{M}_2 \\ * & * & \tilde{M}_2\end{bmatrix}\begin{bmatrix} e(t) \\ e(t-\tau_2(t)) \\ e(t-\tau_2)\end{bmatrix} + \tau_1^2z^T(t)\Phi^T\tilde{M}_1\Phi z^T(t) + \tau_2^2z^T(t)\Phi^T\tilde{M}_2\Phi z^T(t)\Bigg\}
\end{aligned} \tag{22}
$$

From Assumptions 1 and 2, we can obtain

$$
\begin{bmatrix} e(t) \\ \bar{F}(e(t))\end{bmatrix}^T\begin{bmatrix} \bar{\Gamma} & \tilde{\Gamma} \\ * & I_{nN}\end{bmatrix}\begin{bmatrix} e(t) \\ \bar{F}(t)\end{bmatrix} \le 0, \tag{23}
$$

$$
\begin{bmatrix} e(t-\tau_1(t)) \\ \bar{F}(e(t-\tau_1(t)))\end{bmatrix}^T\begin{bmatrix} \bar{\Gamma} & \tilde{\Gamma} \\ * & I_{nN}\end{bmatrix}\begin{bmatrix} e(t-\tau_1(t)) \\ \bar{F}(e(t-\tau_1(t)))\end{bmatrix} \le 0, \tag{24}
$$

$$\bar{G}_1^T(e(t))\bar{G}_1(e(t)) \le \delta_1 e^T(t)e(t), \tag{25}$$

$$\bar{G}_2^T(e(t-\tau_2(t)))\bar{G}_2(e(t-\tau_2(t))) \le \delta_2 e^T(t-\tau_2(t))e(t-\tau_2(t)). \tag{26}$$

The triggering condition in (5) can be rewritten as follows

$$\sum_{i=1}^{N} \pi_i \eta_i(t) - \epsilon^T(t)\Theta_1\epsilon(t) + e^T(t)\Theta_2 e(t) > 0. \tag{27}$$

From (20)–(27), we can further obtain

$$\begin{aligned}
E\{\dot{V}(t)\} \le{}& E\{\dot{V}_1(t) + \dot{V}_2(t) + \dot{V}_3(t)\} + \iota_1(\sum_{i=1}^{N} \pi_i\eta_i(t) - \epsilon^T(t)\Theta_1\epsilon(t) + e^T(t)\Theta_2 e(t)) \\
&- \iota_2 \begin{bmatrix} e(t) \\ \bar{F}(e(t)) \end{bmatrix}^T \begin{bmatrix} \bar{\Gamma} & \tilde{\Gamma} \\ * & I_{nN} \end{bmatrix} \begin{bmatrix} e(t) \\ \bar{F}(t) \end{bmatrix} - \iota_3 \begin{bmatrix} e(t-\tau_1(t)) \\ \bar{F}(e(t-\tau_1(t))) \end{bmatrix}^T \begin{bmatrix} \bar{\Gamma} & \tilde{\Gamma} \\ * & I_{nN} \end{bmatrix} \\
&\times \begin{bmatrix} e(t-\tau_1(t)) \\ \bar{F}(e(t-\tau_1(t))) \end{bmatrix} - \iota_4(\bar{G}_1^T(e(t))\bar{G}_1(e(t)) - \delta_1 e^T(t)e(t)) + \iota_5(\delta_2 e^T(t-\tau_2(t))e(t-\tau_2(t))) \\
&- \bar{G}_2^T(e(t-\tau_2(t)))\bar{G}_2(e(t-\tau_2(t))) - \iota_6(\bar{H}^T(e(t)-\epsilon(t))\bar{H}(e(t)-\epsilon(t)) \\
&- (e(t)-\epsilon(t))^T\mathcal{H}(e(t)-\epsilon(t))) \\
\le{}& E\Big\{\tau_1^2 z^T(t)\Phi^T\tilde{M}_1\Phi z^T(t) + \tau_2^2 z^T(t)\Phi^T\tilde{M}_2\Phi z^T(t) + z^T(t)\mathcal{D}z(t)\Big\} + \iota_1\sum_{i=1}^{N}\pi_i\eta_i(t),
\end{aligned} \tag{28}$$

where $\mathcal{D} = (D_{ij})_{10\times 10}$, ι_i, $i = 1, \cdots, 5$ are some positive constants.

Introducing a positive scalar $\lambda \in (0, \beta)$, one has from (13) that

$$\begin{aligned}
E\{\dot{W}(t) + \lambda W(t)\} &= E\{\exp\{-\beta t\}\dot{V}(t)\} + \sum_{i=1}^{N}\dot{\eta}_i(t) + \sum_{i=1}^{N}\lambda\eta_i(t) \\
&\quad - (\beta-\lambda)E\{\exp\{-\beta t\}V(t)\} \\
&\le E\Big\{\tau_1^2 z^T(t)\Phi^T\tilde{M}_1\Phi z^T(t) + \tau_2^2 z^T(t)\Phi^T\tilde{M}_2\Phi z^T(t) + z^T(t)\mathcal{D}z(t)\Big\} \\
&\quad + \iota_1\sum_{i=1}^{N}\pi_i\eta_i(t) - \epsilon^T(t)\Psi\epsilon(t) + e^T(t)\Theta_3 e(t) + \sum_{i=1}^{N}\lambda\eta_i(t) - \sum_{i=1}^{N}\varrho_i\eta_i(t) \\
&\le E\Big\{z^T(t)(\tau_1^2\Phi^T\tilde{M}_1\Phi + \tau_2^2\Phi^T\tilde{M}_2\Phi + \bar{\mathcal{D}})z^T(t)\Big\}.
\end{aligned} \tag{29}$$

By applying Schur complement, one can obtain that (14) is equivalent to

$$\tau_1^2\Phi^T\tilde{M}_1\Phi + \tau_2^2\Phi^T\tilde{M}_2\Phi + \bar{\mathcal{D}} < 0. \tag{30}$$

Then, it follows from (29) and (30) that $E\{\dot{W}(t)\} < -\lambda W(t)$, which implies $\lim_{t\to+\infty} E\{\sum_{i=l_{k-1}+1}^{l_k}\|e_i(t)\|\} = 0, k \in \mathcal{M}$. Hence, the CDNs in (1) under the proposed controller (8) achieves secure cluster synchronization. This completes the proof. □

Based on Theorem 1, the synchronization controller design in terms of the desired controller gain matrices K_i, $i \in \mathcal{V}$, can be performed. Firstly, pre- and post- multiplying the inequality (14) by $\mathrm{diag}\{I, \tilde{Q}, \tilde{Q}\}$, which yields

$$\begin{bmatrix} \bar{\mathcal{D}} & \tau_1^2\bar{\Phi}^T & \tau_2^2\bar{\Phi}^T \\ * & -\tau_1^2\tilde{Q}\tilde{M}_1^{-1}\tilde{Q} & 0 \\ * & * & -\tau_2^2\tilde{Q}\tilde{M}_2^{-1}\tilde{Q} \end{bmatrix} < 0, \tag{31}$$

where $\bar{\Phi} = ((1-\bar{\alpha})\tilde{Q}\tilde{K}, 0, 0, 0, 0, \tilde{Q}\tilde{W}_1, \tilde{Q}\tilde{W}_2, \tilde{Q}\mathcal{A}, \tilde{Q}\mathcal{B}, \bar{\alpha}\tilde{Q}\tilde{K}, -(1-\bar{\alpha})\tilde{Q}\tilde{K})$. Setting $\tilde{Q}\tilde{K} = \Xi$, then (31) can be rewritten as

$$\begin{bmatrix} \hat{\mathcal{D}} & \tau_1^2\hat{\Phi}^T & \tau_2^2\hat{\Phi}^T \\ * & -\tau_1^2\tilde{Q}\tilde{M}_1^{-1}\tilde{Q} & 0 \\ * & * & -\tau_2^2\tilde{Q}\tilde{M}_2^{-1}\tilde{Q} \end{bmatrix} < 0, \tag{32}$$

where

$$\hat{\mathcal{D}}_{11} = (1-\bar{\alpha})(\Xi + \Xi^T) + \tilde{R}_1 + \tilde{R}_3 + \iota_1\Theta_2 + \iota_4\delta_1 I_{nN} - \iota_1\bar{\Gamma} + \iota_5\mathcal{H} - \tilde{M}_1 - \tilde{M}_2 + \Theta_3,$$

$$\hat{\mathcal{D}}_{10} = \bar{\alpha}\Xi,\ \hat{\mathcal{D}}_{111} = -\iota_6\mathcal{H} - (1-\bar{\alpha})\Xi,$$

$$\hat{\Phi} = ((1-\bar{\alpha})\Xi, 0, 0, 0, 0, \tilde{Q}\tilde{W}_1, \tilde{Q}\tilde{W}_2, \tilde{Q}\mathcal{A}, \tilde{Q}\mathcal{B}, \bar{\alpha}\Xi, -(1-\bar{\alpha})\Xi)^T.$$

$$\hat{\mathcal{D}} = \begin{bmatrix} \hat{\mathcal{D}}_{11} & \mathcal{D}_{12} & 0 & \mathcal{D}_{14} & 0 & \mathcal{D}_{16} & \mathcal{D}_{17} & \mathcal{D}_{18} & \mathcal{D}_{19} & \hat{\mathcal{D}}_{10} & \hat{\mathcal{D}}_{111} \\ * & \mathcal{D}_{22} & \mathcal{D}_{23} & 0 & 0 & 0 & \mathcal{D}_{27} & 0 & 0 & 0 & 0 \\ * & * & \mathcal{D}_{33} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & \mathcal{D}_{44} & \mathcal{D}_{45} & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & \mathcal{D}_{55} & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & * & \mathcal{D}_{66} & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & * & * & \mathcal{D}_{77} & 0 & 0 & 0 & 0 \\ * & * & * & * & * & * & * & \mathcal{D}_{88} & 0 & 0 & 0 \\ * & * & * & * & * & * & * & * & \mathcal{D}_{99} & 0 & 0 \\ * & * & * & * & * & * & * & * & * & \mathcal{D}_{00} & 0 \\ * & * & * & * & * & * & * & * & * & * & \bar{\mathcal{D}}_{11,11} \end{bmatrix},$$

In light of Lemma 3, one can get

$$\begin{bmatrix} \hat{\mathcal{D}} & \tau_1^2\hat{\Phi}^T & \tau_2^2\hat{\Phi}^T \\ * & -2\tau_1^2\tilde{Q} + \tau_1^2\tilde{M}_1 & 0 \\ * & * & -2\tau_2^2\tilde{Q} + \tau_2^2\tilde{M}_2 \end{bmatrix} < 0. \tag{33}$$

Based on the formulation above, the following theorem states a sufficient condition on the existence of the desired secure cluster dynamic event-triggered synchronization controller (8).

Theorem 2. *Consider the CDNs in (1), suppose that Assumptions 1–3 hold. For given parameters* $\tau_M > 0$, $\bar{\tau}_1, \bar{\tau}_2 \in [0,1)$, $\pi_i > 0$, $\theta_i > 0$, $\zeta_i > 0$, $\eta_i(0) > 0$, $\varrho_i > 0$, $i \in \mathcal{V}$; $\bar{\alpha} \in (0,1)$, $\delta_1 > 0$, $\delta_2 > 0$, $\rho_k > 0$, $\varpi_k > 0$, $n_k, p_k \in \mathcal{N}^+$, $k \in \mathcal{M}$, $\beta > 0$, $\lambda \in (0,\beta)$, *and matrix* $H > 0$, *if there exist scalers* $\iota_q > 0$, $q = 1, \cdots, 6$, *some symmetric positive define matrices* $\tilde{Q}_k$, $\tilde{R}_{1k}$, $\tilde{R}_{2k}$, $\tilde{R}_{3k}$, $\tilde{M}_k$, $k \in \mathcal{M}$, *and* Ξ *with appropriate dimensions, such that the inequalities (13) and (33) are satisfied, then the secure cluster synchronization problem is solved under the controller gain matrix given as*

$$\tilde{K} = \tilde{Q}^{-1}\Xi. \tag{34}$$

Proof. By using Schur complement and $-\tilde{Q}\tilde{M}_1^{-1}\tilde{Q} \le -2\tilde{Q} + \tilde{M}_1$, $-\tilde{Q}\tilde{M}_2^{-1}\tilde{Q} \le -2\tilde{Q} + \tilde{M}_2$, The theorem can be conducted immediately from Theorem 1. □

Remark 7. *The LMIs (33) in Theorem 2 were solved using MATLAB R2023b with the Robust Control Toolbox (Version 6.15)—specifically, the lmilab environment and feasp function. This toolbox is widely adopted in control systems research for LMI-based design due to its compatibility*

with standard academic LMI formulations. Algorithm 1 is given to show how to solve LMI and compute controller gains.

3.2. The Static Event-Triggered Case

It is worth mentioning that the dynamic event-triggered mechanism in (5) includes the static one as a special case. In addition, the results for secure cluster synchronization of the CDNs in (1) under a static event-triggered mechanism can be developed straightforwardly from Theorem 1 by letting θ approach to $+\infty$. Such a static event-triggered mechanism can be described by

$$t_{q+1}^i = \inf\{t > t_q^i | \zeta_i(e_i(t))^T e_i(t) - (e_i(t) - e_i(t_q^i))^T \Psi_i (e_i(t) - e_i(t_q^i)) \le 0\}, \tag{35}$$

where $\zeta_i \in (0,1)$. Then the design criterion for secure cluster synchronization of the CDNs (1) under the above static event-triggered mechanism is stated as follows. The proof is omitted for concise.

Algorithm 1 LMI and Compute Controller Gains

Input: $N, \bar{m}, P = [P_1, P_2, \cdots, P_{\bar{m}}], n, \tau_1, \tau_2, \tau_M = \max(\tau_1, \tau_2), W_{1k}, W_{2k}, \Gamma_{1k}, \Gamma_{2k}, \delta_1, \delta_2, A, B, \Lambda_1, \Lambda_2, \bar{\alpha} \in (0,1), H > 0, \pi_i > 0, \theta_i > 0, \zeta_i \in (0,1), \varrho_i > 0, \eta_0 > 0), \iota_q > 0$ $(q = 1, \cdots, 6), \beta > 0, \lambda \in (0, \beta)$, tol $= 10^{-8}$, T_{sim}, $dt = 10^{-4}$.
Output: K_i $(i = 1, \cdots, N)$.

Step 1: Formulate LMI

1.1 Define block-diagonal decision matrices: Q, R_1, R_2, R_3, R_4, M_1, M_2, Ξ.
1.2 Compute auxiliary matrices for triggering and attacks: Θ_1, Θ_2, Θ_3 with $\Psi_i > 0$ (predefined positive definite matrices, e.g., $\Psi_i = I_n$).
1.3 Construct core LMI block $\overline{\mathcal{D}}$:

$$\mathcal{D}_{11} = (1-\bar{\alpha})(\Xi + \Xi^T) + R_1 + R_3 + \iota_1\Theta_2 + \iota_4\delta_1 I_{nN} - \iota_2\overline{\Gamma} + \iota_6\mathcal{H} - M_1 - M_2,$$

$$\mathcal{D}_{12} = M_1,\ \mathcal{D}_{14} = M_2,\ \mathcal{D}_{16} = Q\tilde{W}_1 - \iota_2\tilde{\Gamma},\ \mathcal{D}_{10} = \bar{\alpha}\Xi,\ \mathcal{D}_{111} = -\iota_6\mathcal{H} - (1-\bar{\alpha})\Xi,$$

and fill remaining blocks $(\mathcal{D}_{22}, \mathcal{D}_{23}, \cdots)$.
1.4 Form full LMI via Schur complement:

$$\tilde{\mathcal{D}} = \begin{bmatrix} \overline{\mathcal{D}} & \tau_1^2\Phi^T & \tau_2^2\Phi^T \\ * & -\tau_1^2 M_1^{-1} & 0 \\ * & * & -\tau_2^2 M_2^{-1} \end{bmatrix} < 0,$$

where $\Phi = [(1-\bar{\alpha})\Xi, 0, 0, 0, 0, Q\tilde{W}_1, Q\tilde{W}_2, Q\mathcal{A}, Q\mathcal{B}, \bar{\alpha}\Xi, -(1-\bar{\alpha})\Xi]^T$.
1.5 Add constraints:

$$Q > 0,\ R_1 > 0,\ R_2 > 0,\ R_3 > 0,\ R_4 > 0,\ M_1 > 0,\ M_2 > 0, \quad \iota_1\pi_i + \lambda - \varrho_i \le 0\ (\forall i).$$

Step 2: Solve LMI and Controller Gains

2.1 Call LMI solver (e.g., MATLAB `feasp`) to solve $\tilde{\mathcal{D}} < 0$ with tolerance tol.
if no feasible solution exists **then**
  Print 'LMI infeasible: Relax H, τ_1, τ_2, or ι_q' and terminate.
else
  Extract feasible matrices Q_{feas} and Ξ_{feas}.
end if
2.2 Calculate controller gains: $K = Q_{\text{feas}}^{-1}\Xi_{\text{feas}}$, and split K into per-node gains K_i based on cluster partition P.
return K_i

Theorem 3. *Consider the CDNs in (1), suppose that Assumptions 1–3 hold. For given parameters* $\tau_M > 0$, $\bar{\tau}_1, \bar{\tau}_2 \in [0,1)$, $\zeta_i \in (0,1)$, $i \in \mathcal{V}$; $\bar{\alpha} \in (0,1)$, $\delta_1 > 0$, $\delta_2 > 0$, $\rho_k > 0$, $\varpi_k > 0$, $n_k, p_k \in \mathcal{N}^+$, $k \in \mathcal{M}$, *and matrix* $H > 0$, *if there exist scalers* $\iota_q > 0$, $q = 1, \cdots, 6$, *some symmetric positive define matrices* $\tilde{Q}_k$, $\tilde{R}_{1k}$, $\tilde{R}_{2k}$, $\tilde{R}_{3k}$, $\tilde{M}_k$, $k \in \mathcal{M}$, *and* $\bar{\Xi}$ *with appropriate dimensions such that*

$$\bar{\Pi} = \begin{bmatrix} \check{\Upsilon} & \tau_1^2 \check{\Phi}^T & \tau_2^2 \check{\Phi}^T \\ * & -2\tau_1^2 \tilde{Q} + \tau_1^2 \tilde{M}_1 & 0 \\ * & * & -\tau_2^2 \tilde{Q} + \tau_2^2 \tilde{M}_2 \end{bmatrix} < 0, \tag{36}$$

where

$$\begin{aligned} \Upsilon_{11} =& (1-\bar{\alpha})(\bar{\Xi} + \bar{\Xi}^T) + \tilde{R}_1 + \tilde{R}_3 + \iota_1 \Theta_3 + \iota_4 \delta_1 I_{nN} - \iota_2 \bar{\Gamma} + \iota_6 \mathcal{H} - \tilde{M}_1 - \tilde{M}_2, \\ \Upsilon_{10} =& \bar{\alpha}\bar{\Xi},\ \Upsilon_{111} = -\iota_6 \mathcal{H} - (1-\bar{\alpha})\bar{\Xi}, \\ \check{\Phi} =& ((1-\bar{\alpha})\bar{\Xi}, 0, 0, 0, 0, \tilde{Q}\tilde{W}_1, \tilde{Q}\tilde{W}_2, \tilde{Q}\mathcal{A}, \tilde{Q}\mathcal{B}, \bar{\alpha}\bar{\Xi}, -(1-\bar{\alpha})\bar{\Xi}), \end{aligned}$$

$$\check{\Upsilon} = \begin{bmatrix} \Upsilon_{11} & \mathcal{D}_{12} & 0 & \mathcal{D}_{14} & 0 & \mathcal{D}_{16} & \mathcal{D}_{17} & \mathcal{D}_{18} & \mathcal{D}_{19} & \Upsilon_{10} & \Upsilon_{111} \\ * & \mathcal{D}_{22} & \mathcal{D}_{23} & 0 & 0 & 0 & \mathcal{D}_{27} & 0 & 0 & 0 & 0 \\ * & * & \mathcal{D}_{33} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & \mathcal{D}_{44} & \mathcal{D}_{45} & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & \mathcal{D}_{55} & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & * & \mathcal{D}_{66} & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & * & * & \mathcal{D}_{77} & 0 & 0 & 0 & 0 \\ * & * & * & * & * & * & * & \mathcal{D}_{88} & 0 & 0 & 0 \\ * & * & * & * & * & * & * & * & \mathcal{D}_{99} & 0 & 0 \\ * & * & * & * & * & * & * & * & * & \mathcal{D}_{00} & 0 \\ * & * & * & * & * & * & * & * & * & * & \check{\mathcal{D}}_{11,11} \end{bmatrix},$$

then the CDNs in (1) under the static event-triggered mechanism (35) achieves secure cluster synchronization against deception attacks satisfying (7). Furthermore, the controller gain matrix is determined as $\tilde{K} = \tilde{Q}^{-1}\bar{\Xi}$.

Remark 8. *The theoretical connection between the two mechanisms—where the static case (Theorem 3) emerges as a special case of the dynamic one when* $\theta_i \to +\infty$*—stems from the gradual 'elimination' of the auxiliary variable* $\eta_i(t)$*'s influence: as* θ_i *grows infinitely large, the dynamic triggering condition (5) simplifies to the static threshold rule (36), where only the error difference* $\zeta_i e_i^T(t)\Psi_i e_i(t) - (e_i(t) - e_i(t_q^i))^T \Psi_i (e_i(t) - e_i(t_q^i)) \leq 0$ *determines triggering (the auxiliary* $\eta_i(t)$ *term becomes negligible).*

4. An Illustrative Example

Consider a network of five nodes that are assigned into two clusters $\mathcal{P}_1 = \{1,2\}$, $\mathcal{P}_2 = \{3,4,5\}$. Moreover, the ith node described as (1) with $\Lambda_1 = \text{diag}\{0.5, 0.5\}$, $\Lambda_2 = \text{diag}\{0.2, 0.2\}$, $W_{11} = \text{diag}\{1.2, 0.8\}$, $W_{21} = \text{diag}\{0.2, 0.2\}$, $W_{12} = \text{diag}\{0.8, 0.9\}$, $W_{22} = \text{diag}\{0.2, 0.5\}$, $f_1(x_i(t)) = [0.6x_{i1}(t) - \tanh(0.3x_{i1}(t)) + 0.1x_{i2}(t),\ 0.8x_{i2}(t) - \tanh(0.5x_{i2}(t))]^T$ with $\Gamma_{11} = \left[\begin{smallmatrix} 0.6 & 0.1 \\ 0 & 0.8 \end{smallmatrix}\right]$, $\Gamma_{21} = \left[\begin{smallmatrix} 0.9 & 0.1 \\ 0 & 1.3 \end{smallmatrix}\right]$, $f_2(x_i(t)) = [-0.3x_{i1}(t) - \tanh(0.2x_{i1}(t)) + 0.2x_{i2}(t),\ 0.4x_{i2}(t) - \tanh(0.4x_{i2}(t))]$ with $\Gamma_{12} = \left[\begin{smallmatrix} -0.3 & 0.2 \\ 0 & 0.4 \end{smallmatrix}\right]$, $\Gamma_{22} =$

$\begin{bmatrix} -0.1 & 0.2 \\ 0 & 0.8 \end{bmatrix}$, $g_1(x_i(t)) = \begin{bmatrix} -0.8x_{i1}(t) \\ -0.8x_{i2}(t) \end{bmatrix}$, $g_2(x_i(t)) = \begin{bmatrix} -0.1x_{i1}(t) \\ -0.1x_{i2}(t) \end{bmatrix}$, $\tau_1(t) = 0.1\tanh(t)$, $\tau_2(t) = 0.2\tanh(t)$, and

$$A = \begin{bmatrix} -2 & 2 & 1 & 0 & -1 \\ 2 & -2 & 0 & 1 & -1 \\ 1 & -1 & -4 & 2 & 2 \\ 1 & -1 & 1.5 & -3 & 1.5 \\ 1 & -1 & 1 & 1 & -2 \end{bmatrix}, \quad B = \begin{bmatrix} -3 & 3 & 0.1 & 0.1 & -0.2 \\ 1 & -1 & 0.2 & 0.2 & -0.4 \\ 1 & -1 & -3 & 2 & 1 \\ 0.5 & -0.5 & 1 & -2 & 1 \\ 0.1 & -0.1 & 1 & 1 & -2 \end{bmatrix}.$$

Choose $\delta_1 = 0.8$, $\delta_2 = 0.1$, $\tau_1 = 0.1$, $\tau_2 = 0.2$, $\bar{\tau}_1 = 0.1$, $\bar{\tau}_2(t) = 0.1$, $\pi_1 = 0.2$, $\pi_2 = 0.1$, $\pi_3 = 0.1$, $\pi_4 = 0.2$, $\pi_5 = 0.2$, $\theta_i = 1$, $\zeta_i = 0.3$, $\varrho_i = 1$, $\eta_i(0) = 1$, $i = 1, \cdots, 5$. Via solving LMI (33), the feasible controller gains are given as $K_1 = \begin{bmatrix} -28.8471 & 0.0463 \\ * & -28.2460 \end{bmatrix}$, $K_2 = \begin{bmatrix} -28.7249 & 0.0463 \\ * & -28.1023 \end{bmatrix}$, $K_3 = \begin{bmatrix} -29.7127 & -0.0280 \\ * & -29.9920 \end{bmatrix}$, $K_4 = \begin{bmatrix} -28.9436 & -0.0745 \\ * & -29.3441 \end{bmatrix}$, $K_5 = \begin{bmatrix} -28.6145 & -0.0786 \\ * & -29.1118 \end{bmatrix}$.

Applying the designed secure cluster synchronization controller, it is found that the CDNs can be synchronized into two clusters even in the presence of the simulated stochastic deception attacks. The related simulation results are shown in Figures 1–6. Specifically, from Figure 1, it can be concluded that the nodes are not synchronized without controllers. Under the controllers, nodes in the same cluster are synchronized and not synchronized in the different cluster from Figure 2. Moreover, as shown in Figure 3, the trajectories of cluster errors $e_1^{xs}(t) = \sum_{i=1}^{2} \|x_i(t) - s_1(t)\|^2$, $e_2^{xs}(t) = \sum_{i=3}^{5} \|x_i(t) - s_2(t)\|^2$ are approaching zero, such findings illustrate that the theoretical results are effective. In Figure 4, dynamic functions $\eta_i(t)$, $i = 1, \cdots, 5$ are described and we can conclude that the trajectories of dynamic functions $\eta_i(t)$, $i = 1, \cdots, 5$ are approaching zero while $t \to +\infty$. Figure 5 show the dynamical event releasing instants and intervals of nodes in the CDNs as well as the occurring instants of the simulated stochastic deception attacks. Figure 6 show the static event releasing instants and intervals of nodes in the CDNs as well as the occurring instants of the simulated stochastic deception attacks. Figures 5 and 6 intuitively illustrate two key improvements of the dynamic event-triggered mechanism: (1) it significantly reduces the number of triggering events; (2) it maintains more stable triggering intervals which avoided frequent unnecessary triggers caused by static threshold rigidness.

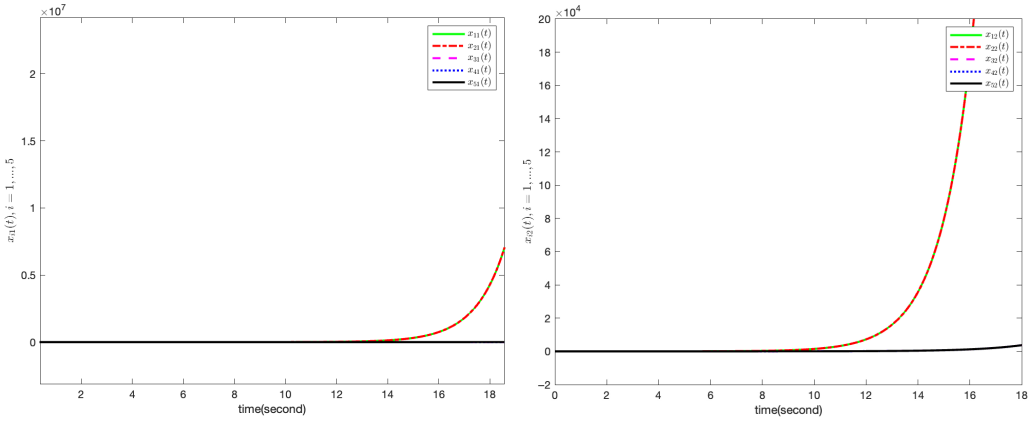

Figure 1. Trajectories of $x_{ij}(t)$ without controllers, $i = 1, \cdots, 5$, $j = 1, 2$.

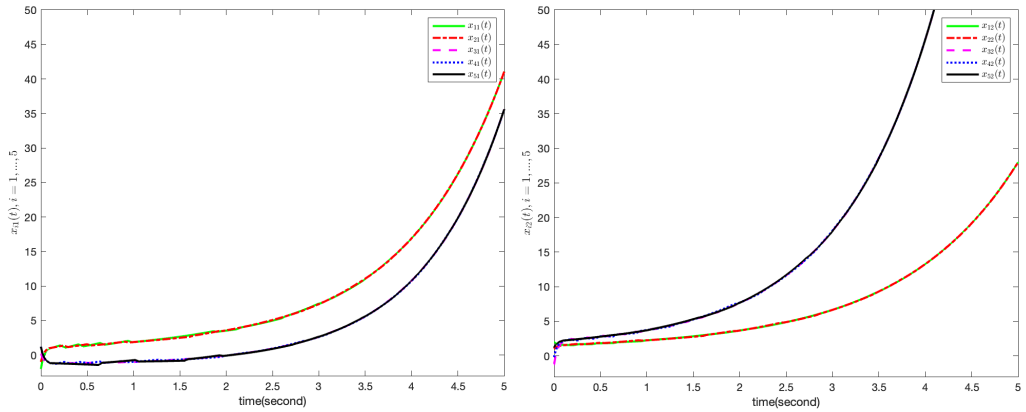

Figure 2. Trajectories of $x_{ij}(t)$ with controllers, $i = 1, \cdots, 5$, $j = 1, 2$.

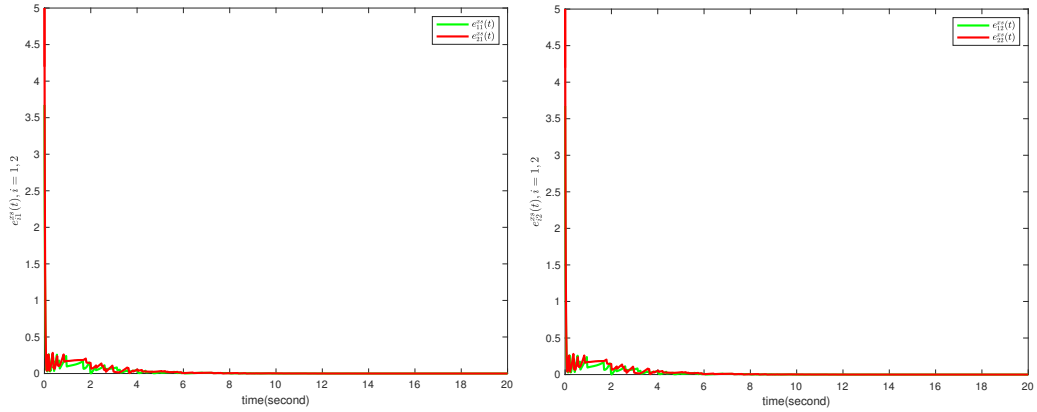

Figure 3. Trajectories of cluster errors $e_{ij}^{xs}(t)$ under controllers, $i, j = 1, 2$.

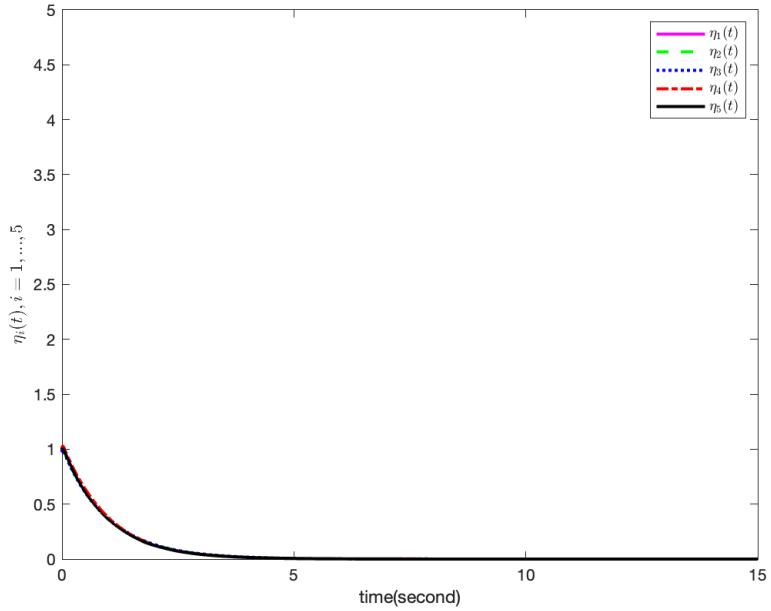

Figure 4. Trajectories of internal dynamic functions $\eta_i(t)$, $i = 1, \cdots, 5$.

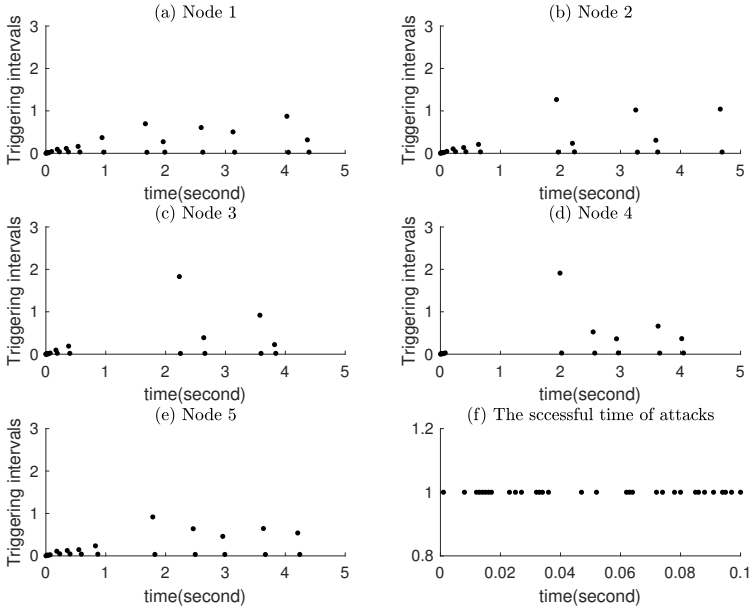

Figure 5. Dynamic event-triggered time and the attack time.

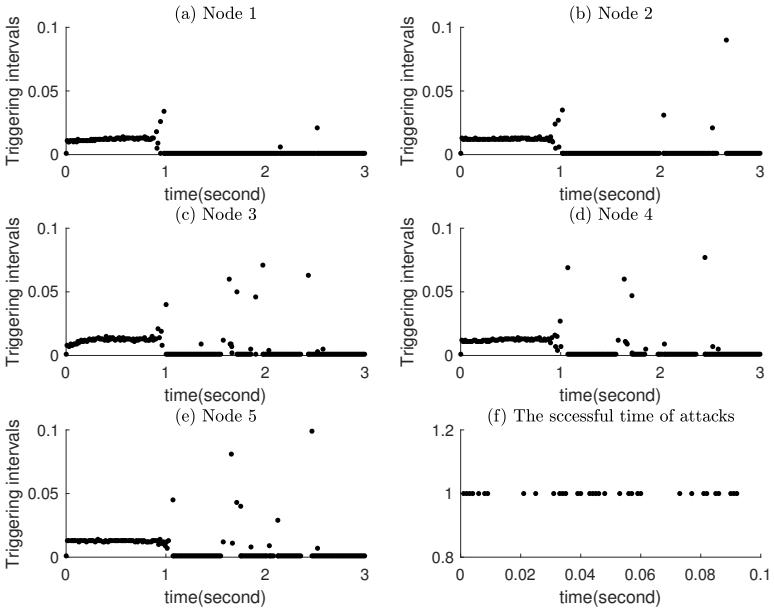

Figure 6. Static event-triggered time and the attack time.

5. Conclusions

The secure cluster synchronization problem of CDNs under deception attacks has been investigated in this chapter. By taking into account both the effects of intermittent data transmissions under the distributed dynamic event-triggered mechanism and stochastic deception attacks, some sufficient conditions on the secure cluster synchronization performance analysis and controller design are established. Then, an illustrative example is given to show the effectiveness of the proposed theoretical methods and control schemes. In future work, we plan to explore two directions: (1) Markovian jump attack models: to capture time-varying attack probabilities (e.g., attackers may increase intensity during peak network traffic, leading to transition between 'low-attack' and 'high-attack' modes); and (2) Poisson-distributed attack models: to describe the random arrival of attack sequences. These extensions will allow us to address more complex attack behaviors while maintain-

ing the core advantages of the dynamic event-triggered control framework proposed in this paper.

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

Funding: This work was funded by the Youth Doctor 'Sailing' Project of Guangzhou Basic Research Plan for Basic and Applied Basic Research grant number 1749529.

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: The authors have reviewed and edited the output and take full responsibility for the content of this publication.

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

References

1. Hu, J.; Jia, C.Q.; Liu, H.J.; Yi, X.J.; Liu, Y.R. A survey on state estimation of complex dynamical networks. *Int. J. Syst. Sci.* **2021**, *52*, 3351–3367. [CrossRef]
2. He, Z.L.; Li, C.D.; Nie, L.F. Synchronization of complex dynamical networks with saturated delayed impulsive control. *ISA Trans.* **2025**, *157*, 153–163. [CrossRef]
3. Sun, J.; Guo, Y.X.; Zhang, C. Exponential synchronization of nonlinear complex dynamic networks via intermittent pinning control on time scales. *Neurocomputing* **2024**, *578*, 127375. [CrossRef]
4. Wei, G.M.; Yuan, Z.Z.; Qi, W.H.; Cao, J.D.; Cheng, J.; Shi, K.B. Finite-time self-triggered synchronization for semi-Markov jump reaction-diffusion complex dynamical networks. *J. Frankl. Inst.* **2025**, *362*, 107765. [CrossRef]
5. Shi, J.Y.; Zhou, P.P.; Jia, Q.; Cai, S.M. Fixed-time synchronization of multilayered complex dynamic networks via quantized variable-gain saturated control. *Inf. Sci.* **2024**, *681*, 121206. [CrossRef]
6. Zhang, Y.X.; Sun, M.M.; Li, K.Z. Synchronization on complex dynamical networks via intermittently sampled-data pinning control. *Physical A* **2024**, *654*, 130109. [CrossRef]
7. Chen, W.; Wang, X.P.; Ren, F.M.; Zeng, Z.G. Quasi-synchronization for variable-order fractional complex dynamical networks with hybrid delay-dependent impulses. *Neural Netw.* **2024**, *173*, 106161.
8. Wang, L.; Liang, Q.Y.; She, Z.K.; Lv, J.H.; Wang, Q.G. A decomposition approach for synchronization of heterogeneous complex networks. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *51*, 853–863. [CrossRef]
9. Pecora, L.M.; Carroll, T.L. Master stability functions for synchronized coupled systems. *Phys. Rev. Lett.* **1998**, *80*, 2109–2112. [CrossRef]
10. Chen, M.Y. Some simple synchronization criteria for complex dynamical networks. *IEEE Trans. Circuits Syst.* **2006**, *53*, 1185–1189. [CrossRef]
11. Yao, J.; Guan, Z.H.; Hill, D.J. Passivity-based control and synchronization of general complex dynamical networks. *Automatica* **2009**, *45*, 2107–2113. [CrossRef]
12. Liao, B.; Wang, Y.; Xue, J.; Zhou, Z.; Zhang, S.; Chen, X. Dynamic Clustering-Based Time Synchronization for PLC-TWACS Integrated Multimodal Power IoT in Smart Park. *IEEE Syst. J.* **2024**, *18*, 1296–1307. [CrossRef]
13. Shi, T.T.; Hu, C.; Jiang, H.J.; Zhu, Q.X.; Huang, T.W. Fixed-time leaderless cluster synchronization of spatiotemporal community networks with coopetition interactions. *IEEE Trans. Cybern.* **2025**, *early access*. [CrossRef] [PubMed]
14. Liu, X.Y.; Ho, D.; Xie, C.L. Prescribed-time cluster synchronization of complex networks via a smooth control approach. *IEEE Trans. Cybern.* **2020**, *50*, 1771–1775. [CrossRef]
15. Wu, H.F.; Liu, S.; Wang, L.C. Cluster synchronization of complex dynamic networks under pinning control via a limited capacity communication channel. *Nonlinear Anal. Hybrid Syst.* **2025**, *55*, 101547. [CrossRef]
16. Liu, L.; Zhou, W.N.; Huang, C. Finite/prescribed-time cluster synchronization of complex dynamical networks with multi-proportional delays and asynchronous switching. *IEEE Trans. Syst. Man Cybern. Syst.* **2023**, *53*, 3683–3694. [CrossRef]
17. Wang, X.; Park, J.H.; Yang, H.L.; Zhong, S.M. An improved impulsive control approach for cluster synchronization of complex networks with parameters mismatches. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *51*, 2561–2570. [CrossRef]

18. Zhang, J.Y.; Ma, Y.C. Output feedback pinning control for complex dynamical networks subjected to multiple attacks. *Chaos Solitons Fractals* **2024**, *181*, 114625. [CrossRef]
19. Hu, T.T.; Shi, K.B. Secure synchronization control for complex dynamic networks with event-triggered communication strategy under multi-channel denial-of-service attacks. *ISA Trans.* **2025**, *158*, 50–61. [CrossRef] [PubMed]
20. Li, Y.; Song, F.Y.; Liu, J.L.; Xie, X.P.; Tian, E.G.; Fei, S.M. Round Robin-based synchronization control for discrete-time complex networks with probabilistic coupling delay and deception attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2024**, *54*, 4425–4436. [CrossRef]
21. Yang, N.; Chen, S.S.; Su, H. Adaptive event-triggered impulsive control for stochastic complex networks with delays under deception attacks. *Nonlinear Dyn.* **2025**, *113*, 2259–2276. [CrossRef]
22. Yang, N.; Fan, X.D.; Su, H. Dynamic event-triggered delayed impulsive control for stochastic T-S fuzzy complex networks under cyber attacks. *J. Frankl. Inst.* **2025**, *362*, 107863. [CrossRef]
23. Ding, D.R.; Han, Q.L.; Wang, Z.D.; Ge, X.H. Recursive filtering of distributed cyber-physical systems with attack deception. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *51*, 6466–6476. [CrossRef]
24. Rajchakit, G.; Banu, K.A.; Aparna, T.; Lim, C.P. Event-triggered secure control for Markov jump neural networks with time-varying delays and subject to cyber-attacks via state estimation fuzzy approach. *Int. J. Syst. Sci.* **2025**, *56*, 211–226. [CrossRef]
25. Javanmardi, S.; Nascita, A.; Pescapè, A.; Merlino, G.; Scarpa, M. An integration perspective of security, privacy, and resource efficiency in IoT-Fog networks: A comprehensive survey. *Comput. Netw.* **2025**, *early access*. [CrossRef]
26. Zhou, L.L.; Huang, M.Z.; Tan, F.; Zong, G.D.; Wang, Z.; Zhuang, G.M. Fixed-time discontinuous control for cluster secure synchronization of interlayer switching networks under attacks. *IEEE Trans. Autom. Sci. Eng.* **2025**, *22*, 18848–18859. [CrossRef]
27. Sakthivel, N.; Rajkumar, V.; Sabarish Kumar, V. Synchronization of a complex dynamical networks using deception attacks subject to uncertainty and disturbance estimator. *Eur. J. Control* **2025**, *83*, 101208.
28. Mi, J.; Wu, H.Q.; Cao, J.D. Finite-time secure synchronization for stochastic complex networks with delayed coupling under deception attacks: A two-step switching control scheme. *Inf. Sci.* **2025**, *691*, 121647. [CrossRef]
29. Xu, Z.L.; Yang, N.; Li, A.D.; Lu, J.Q. Input-to-state stability of switched network control systems under unknown deception attacks. *IEEE Trans. Cybern.* **2024**, *54*, 5483–5492. [CrossRef] [PubMed]
30. Wu, Y.B.; Guo, Z.R.; Xue, L.; Ahn, C.K.; Liu, J. Stabilization of complex networks under asynchronously intermittent event-triggered control. *Automatica* **2024**, *161*, 111493. [CrossRef]
31. Xu, D.S.; Wang, X.F.; Su, H. Delay event-triggered control for stability analysis of complex networks. *IEEE Trans. Circuits Syst. II Express Briefs* **2022**, *70*, 1104–1108. [CrossRef]
32. Wang, H.; Yang, X.; Xiang, Z.; Tang, R.Q.; Ning, Q. Synchronization of switched neural networks via attacked mode-dependent event-triggered control and its application in image encryption. *IEEE Trans. Cybern.* **2022**, *53*, 5994–6003. [CrossRef]
33. Yang, X.S.; Feng, G.Y.; He, C.T.; Cao, J.D. Event-triggered dynamic output quantization control of switched T-S fuzzy systems with unstable modes. *IEEE Trans. Fuzzy Syst.* **2022**, *30*, 4201–4210. [CrossRef]
34. Wang, X.L.; Ding, D.R.; Ge, X.H.; Dong, H.L.; Han, Q.L. Neural-network-based control with dynamic event-triggered mechanisms under DoS attacks and applications in load frequency control. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2022**, *69*, 5312–5324. [CrossRef]
35. Zhao, B.; Shi, G.; Liu, D. Event-triggered local control for nonlinear interconnected systems through particle swarm optimization-based adaptive dynamic programming. *IEEE Trans. Syst. Man Cybern. Syst.* **2023**, *53*, 7342–7353. [CrossRef]
36. Hu, T.T.; He, Z.; Zhang, X.J.; Zhong, S.M.; Shi, K.B.; Zhang, Y.Y. Adaptive fuzzy control for quasi-synchronization of uncertain complex dynamical networks with time-varying topology via event-triggered communication strategy. *Inf. Sci.* **2022**, *582*, 704–724. [CrossRef]
37. Girard, A. Dynamic triggering mechanisms for event-triggered control. *IEEE Trans. Automat. Control* **2015**, *60*, 1992–1997. [CrossRef]
38. Zhou, L.; Ma, Y.C.; Zou, J.H. Robust synchronization of Markovian jump complex dynamical networks under link attacks: Delay-dependent dynamic event-triggered control approach. *J. Frankl. Inst.* **2024**, *361*, 107251. [CrossRef]
39. Yang, X.T.; Li, A.J.; Zhu, Q.X. Dynamic periodic event-triggered control of stochastic complex networks with time-varying delays. *Neural Netw.* **2025**, *190*, 107659. [CrossRef]
40. Tang, W.; Sheng, Y.; Xiao, Q.; Huang, T.; Zeng, Z. Synchronization of complex dynamical networks on time scales via intermittent dynamic event-triggered control. *IEEE Trans. Syst. Man Cybern. Syst.* **2024**, *54*, 2897–2906. [CrossRef]
41. Liu, Y.R.; Wang, Z.D.; Liu, X.H. Global exponential stability of generalized recurrent neural networks with discrete and distributed delays. *Neural Netw.* **2006**, *19*, 667–675. [CrossRef] [PubMed]