Resilient Control Design of the Third-Order Discrete-Time Connected Vehicle Systems Against Cyber-Attacks

ZEMING LI¹, ZIYUAN LI², AND YONGGUI LIU² (Member, IEEE)
¹School of Mechanical and Automotive Engineering, South China University of Technology, Guangzhou 510640, China
²Key Laboratory of Autonomous Systems and Network Control, Ministry of Education, College of Automatic Science and Engineering, South China University of Technology, Guangzhou 510640, China

Corresponding author: Yonggui Liu (auygliu@scut.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61973128, in part by the Scientific Research Foundation of Central Universities under Grant 2018ZD51, and in part by the Special Application Project of Guangdong Province under Grant 2016B090927007.

ABSTRACT This paper investigates the consensus problems of the third-order discrete-time Connected Vehicle Systems (CVSs) under cyber-attacks. First, the necessary and sufficient conditions for consensus of third-order discrete-time CVSs are derived in the absence of attacks by using algebraic graph and matrix theory. Then the interaction network framework between the original CVSs in the vehicle platoon layer and a virtual system in the hidden layer is established to resist cyber-attacks. Since sufficiently large attacks can be excluded from CVSs through a threshold defense mechanism, such potential attacks considered are bounded and generated by any linear or non-linear finite L2-gain exogenous dynamics system. It is proved that the stability of CVSs can be ensured and the state errors converge to a bounded range whether the attacks exist only in the vehicle platoon layer or in the overall systems (including the vehicle platoon layer and the hidden layer) by using the Lyapunov stability method. Finally, a simulation example containing several scenarios demonstrates the effectiveness and superiority of the proposed methods.

INDEX TERMS Vehicle platoon, resilient control, consensus, cyber-attacks, interaction network.

I. INTRODUCTION
Organizing self-driving vehicles as a platoon has attracted widespread attention in recent years due to its advantages in reducing fuel consumption, improving traffic safety and increasing road efficiency [1]–[4]. Based on a distributed control protocol, each vehicle in the platoon travels utilizing local measurements and neighboring information through wireless networks (i.e., vehicle ad hoc networks (VANETs)). Owing to the interconnection and sharing of information between vehicles, such a platoon can be considered as a cyber-physical system (CPS). Considering the driver behaviors, braking control and input delays, cooperative adaptive cruise control (CACC), a typical application of CPS, is further proposed to ensure the coordination and stability of the vehicle platoon systems [5]–[7]. Flocking theory [8], [9] and consensus control [10]–[12] are widely used to analyze the information interaction between vehicles during the CACC process in CPS. Each vehicle in the platoon implements CACC and exchanges information with each other to achieve global agreement.

It has been well known that the consensus of the first-order systems can be guaranteed by analyzing and designing the eigenvalues of the Laplacian matrix corresponding to the network topology. Meanwhile, there is a growing interest in the consensus problem of the second-order or third-order systems (i.e., all agents in the systems are governed by second-order or third-order dynamics) [13]–[16]. For example, some necessary and sufficient conditions for second-order consensus in multi-agent dynamical systems have been studied in [13]. With the help of the Lyapunov-based technique, the consensus analysis method for second-order systems was extended to the case of nonlinear dynamics [14]. Besides, the consensus problem for heterogeneous multi-agent systems consisting of second-order agents and third-order agents was investigated in [15].

There are still many challenges in the research on the consensus issues of CPS. For example, the use of
communication networks in CPS is necessary and has many advantages, but it has also brought some uncertainties, such as time-delays [17], [18], packet losses [19], [20] and computational burden [21], [22]. These factors lead to poor performance in CPS. In particular, the more dangerous factor is to encounter network-induced cyber-attacks, which is becoming a critically challenging threat for CPS [23]–[25]. With a purpose to destabilize the consensus of CPS, the attacker intercepts the communication network and corrupts its local state feedback. Typical attacks can be summarized into three types: denial of service (DoS) attacks, replay attacks, and deception attacks. DoS attacks keep the network busy with forged requests, making the network unable to process legitimate requests, which can be resolved through various strategies in [26]–[29]. For example, the impact of DoS attacks was modeled as stochastic delays in the network and then an estimation scheme was added to the conventional CACC control strategy to make the platoon resilient to DoS attacks [26]. Another strategy is developing optimal control strategies with multitasking and central-tasking structures by using game theory [27]. In [28], an event-triggering based hybrid control strategy was designed for the time-varying attitude control issues of aircraft systems against DoS attacks. Besides, [29] extended the event-triggering strategy under DoS attacks to nonlinear multi-agent systems. Replay attacks intercept system data and maliciously retransmit, destroying system functionality [30]–[33]. Distributed receding-horizon control approach [30], [31] and recursive distributed Kalman fusion estimator (DKFE) [32] are effective strategies to ensure the consensus of CPS under replay attacks. Deception attacks, including data modification, data replay, and false data injection, modify messages transmitted between agents and may undermine the integrity of CPS [34]–[37]. In [34], the CPS was modeled as a stochastic linear system with the Gaussian noise, and the conditions of the system dynamics were derived to evaluate the impact of feasible stealthy deception attacks. Besides, a distributed observer and observer-based event-triggering controller were designed to obtain the consensus bound of discrete-time stochastic multiagent systems with lossy sensors and deception attacks [35]. From another perspective, a dynamic output feedback controller was proposed to guarantee the prescribed security of the discrete-time stochastic nonlinear systems under deception attacks in [36].

In addition to modeling a certain type of cyber-attacks and proposing corresponding resilient control strategies, timely system fault detection is also necessary to ensure the stability and security of CPS [38], [39]. For example, a novel cyber-attack detection method by analyzing the intersection between a prediction ellipsoid set and an estimation ellipsoid set is proposed to guarantee the security of networked control systems [38]. Furthermore, an extremely randomized trees-based scheme was proposed for stealthy cyber-attack detection, improving the security of smart grid networks [39]. Besides, Markov jumping systems (MJSs), which have been extensively investigated in state filtering [40], sliding-mode control [41], fault detection [42], and resilient asynchronous feedback controller design [43], are also promising in cyber-attack detection.

In addition to the system fault detection, the interaction network [44] implemented by software-defined networking [45] was also proposed to resist unknown cyber-attacks. Gusrialdi and his collaborators [44] extended the dynamic range of the attacks to non-linear situations, in which a virtual system without physical meaning whose number of nodes is equal to the number of followers is introduced to the original CPS. Utilizing the concept of competitive interaction, a Lyapunov-based analysis method was presented for the first-order continuous-time systems to design the interaction between the virtual networks and the original systems, giving CPS a strong resistance to cyber-attacks.

The advantages of using the interaction network to combat cyber-attacks are listed as follows: 1) During the interaction, the hidden layer will not affect the convergence of the original systems. 2) Whether before or after identifying the cyber-attacks, the interaction network can keep the stability of the systems from being compromised by attacks. 3) Even if the entire network (including the physical layer and the hidden layer) is subjected to cyber-attacks, the systems can still maintain stability. However, the existing interaction network design only applies to the first-order continuous-time systems [44]. The situation based on high-order discrete-time dynamics has not been studied, which attracts us to fill this gap.

In general, there have been many strategies and approaches to resist cyber-attacks and ensure the stability and security of CPS, but existing results have limitations on the order of systems (the first-order or high-order), attack implementation types (DoS attacks, replay attacks, or deception attacks), or network topology (undirected graph or directed graph). In this paper, the resilient consensus problem of the third-order discrete-time CVSs is investigated, where the acceleration and velocity of all vehicles reach consensus, and any two adjacent vehicles maintain the desired safety distance. To design the interaction network of the third-order systems more conveniently, we derived the iteration matrix of the system errors and designed the interaction systems based on the iterative formula, which means that the method proposed in this paper can be simply applied to the similar designs of the second-order and first-order systems. Besides, we consider the cyber-attacks generated by unknown nonlinear dynamics, providing a more universal distributed control method for multi-agent systems against multiple cyber-attacks, including false data injection, data modification, and data replay. Last but not least, the proposed network topology in this paper is applied to the undirected graph and directed graph, which means the communication cost can be reduced by optimizing the flow of information in the vehicle platoon.

Compared with the existing work, the main contributions of this paper are shown as follows:

i) We propose the cooperative interaction design method for third-order discrete-time CVSs to resist cyber-attacks...
with unknown nonlinear dynamics. The proposed method is universal and can be conveniently utilized in the resilient control design of the second-order and first-order discrete-time multi-agent systems.

ii) In addition to giving the necessary and sufficient conditions for CVSs reaching consensus asymptotically in the absence of an attack, the interaction network design method for CVSs maintaining stability whether the attacks exist only in the vehicle platoon layer or in the overall interaction systems is further developed.

iii) The expressions of system errors are derived to analyze the performance of the systems, which show that the state errors of cooperative CVSs are always bounded for unknown attacks. Moreover, a simulation example containing five cases is provided to illustrate the validity and superiority of the proposed approach.

The remaining sections of this paper are organized as follows. In section II, the recursive formula for the state errors of the third-order discrete-time CVSs with cyber-attacks is derived according to the control objectives and dynamic characteristics of vehicles. In section III, the consensus of CVSs is analyzed in the absence and presence of cyber-attacks, and conditions of controller gains and interaction matrices to stabilize the systems are given. Section IV demonstrates the effectiveness of the proposed methods through a simulation example containing several scenarios, and conclusions are given in section V.

Notation: Let $I_n$ and $0_n$ denote the $n \times n$ identity matrix and $n \times n$ zero matrix respectively. $0$ stands for an $n$-dimensional column vector where all elements are 0. The notation $\text{det}(A)$ represents the determinant of the matrix $A$. $\|A\|$ stands for the Euclidean norm of matrix $A$ or vector $A$. $\lambda_{\text{max}}(A)$ denotes the maximum eigenvalue of matrix $A$. $\text{diag}[\cdot]$ stands for a diagonal matrix. The notation $\sigma(A) \subset B(0, 1)$ describes that all the eigenvalues of the matrix $A$ lie within the unit open circle.

II. PROBLEM FORMULATION

A. DISCRETE-TIME VEHICLE PLATOON MODEL

There have been some studies on the third-order discrete-time systems [46], [47], in which the dynamic model of each agent is simplified without considering the effect of the sampling period. In this paper, the dynamic model of CVSS is derived from continuous motion equations in the sampling period. According to the dynamic characteristics of the third-order systems, it is known that the control input is the derivative of acceleration with respect to time, so the following motion equations in each sampling period can be achieved (The following symbols $u(k)$, $a(k)$, $v(k)$, and $x(k)$ represent the control input, acceleration, velocity, and position at time step $k$ respectively):

$$\begin{align*}
    v(t) & = v(k) + (t - kT) a(k) + \frac{(t - kT)^2}{2} u(k), \\
    a(t) & = a(k) + (t - kT) u(k),
\end{align*}$$

where $t \in [kT, (k + 1)T]$. Dynamic models of each vehicle can be obtained by integrating the motion equations in the sampling period $T$:

$$\begin{align*}
    v(k + 1) & = v(k) + \int_{kT}^{(k+1)T} a(t) dt \\
    & = v(k) + \int_{kT}^{(k+1)T} [a(k) + (t - kT) u(k)] dt \\
    & = v(k) + [(a(k) - kT u(k)) t + \frac{u(k)}{2} t^2] \bigg|_{kT}^{(k+1)T} \\
    & = v(k) + \frac{T^2}{2} u(k), \\
    x(k + 1) & = x(k) + \int_{kT}^{(k+1)T} v(t) dt \\
    & = x(k) + \int_{kT}^{(k+1)T} [v(k) + (t - kT) a(k)] dt \\
    & = x(k) + [(v(k) - kT a(k) + \frac{(kT)^2}{2} u(k)) t + \frac{a(k) - kT a(k)}{2} t^2 + \frac{u(k)}{6} t^3] \bigg|_{kT}^{(k+1)T} \\
    & = x(k) + T v(k) + \frac{T^2}{2} a(k) + \frac{T^3}{6} u(k).
\end{align*}$$

Consider a vehicle platoon including one lead vehicle and $n$ followers. The dynamics of vehicle $i$ in the platoon can be expressed as

$$\begin{align*}
    x_i(k + 1) & = x_i(k) + T v_i(k) + \frac{T^2}{2} a_i(k) + \frac{T^3}{6} u_i(k), \\
    v_i(k + 1) & = v_i(k) + T a_i(k) + \frac{T^2}{2} u_i(k), \\
    a_i(k + 1) & = a_i(k) + T u_i(k), \quad i = 0, 1, 2, \cdots, n,
\end{align*}$$

where $i$ means the index of the lead vehicle ($i = 0$) or the followers ($i \neq 0$), and $u_0(k)$ is assumed to be 0.

B. RECURSIVE FORMULA FOR SYSTEM ERRORS

In this paper, control objectives of the CVSSs are to design appropriate control protocol and cooperative interaction networks so that the spacings between any adjacent vehicles reach the same, and all followers follow the leading vehicle with a consensus velocity and acceleration, which can be expressed as

$$\begin{align*}
    \lim_{k \to \infty} x_i(k) & \to x_i^*(k) = x_0(k) - id, \\
    \lim_{k \to \infty} v_i(k) & \to v_i^*(k) = v_0(k), \\
    \lim_{k \to \infty} a_i(k) & \to a_i^*(k) = a_0(k), \quad i = 1, 2, \cdots, n,
\end{align*}$$

where $d$ denotes the desired spacing between adjacent vehicles, and $x_i^*(k)$, $v_i^*(k)$, $a_i^*(k)$ represent the desired position, velocity, and acceleration of the follower $i$ at time step $k$ respectively.

To express the information flow between vehicles under corresponding network topology, we define $g_{ij} = 1$ if the
vehicle $i$ can receive messages from the vehicle $j$, and $g_{ij} = 0$ otherwise ($i = 1, 2, \ldots, n, j = 0, 1, 2, \ldots, n$), so one has the Laplacian matrix $L = [l_{ij}]$; $l_{ii} = \sum_{j=0}^{n} g_{ij}$ and $l_{ij} = -g_{ij}$, $i \neq j$ ($i, j = 1, 2, \ldots, n$). Analogously, we define a diagonal matrix $L_0 \triangleq \text{diag}[g_{ii}]$ to show network topology between the leading vehicle and each follower.

Following the line in [48], one supposes each vehicle can directly or indirectly communicate with its neighbors, so there is a spanning tree. Furthermore, we assume the following network topologies: i) all followers belong to “look-ahead” type, i.e., $N'_j = \{i-h, \ldots, i-1\} \cap \{1, \ldots, n\}$, where $h$ denotes the number of the vehicles which the $i$th vehicle can communicate; ii) all followers belong to the symmetric “look-ahead” and “look-back” types, i.e., $N'_j = \{i-h, \ldots, i-1\} \cup \{i+1, \ldots, i+h\} \cap \{1, \ldots, n\}$; iii) all followers belong to the undirected ones i.e., $j \in N'_i \Leftrightarrow i \in N'_j, i,j = 1, \ldots, n$. In such cases, the eigenvalues of the Laplacian matrix of the network topologies are real numbers, moreover, one of the eigenvalues of the $L$ is zero, and the real parts of the other eigenvalues are positive known from [49]. Denote the matrix $\hat{L} \triangleq L + L_0$ and then one can obtain $\hat{\lambda}_i = \text{Re}(\hat{\lambda}_i) > 0$, where $\hat{\lambda}_i$ is the eigenvalue of the matrix $\hat{L}$.

In order to achieve the control objectives in (3), the distributed control protocol [46] is designed as:

$$u_i(k) = \sum_{j=0}^{n} g_{ij}[a[x_i(k) - x_j(k)] + (j - i)\bar{d}],$$

$$+ \beta[v_i(k) - v_j(k)] + \gamma[a_{ij}(k) - a_i(k)],$$

where $\alpha > 0$, $\beta > 0$, and $\gamma > 0$ are the control gains to be designed, and $x_i(k)$, $v_i(k)$, $a_i(k)$ represent information transmitted from the vehicle $j$ to the vehicle $i$.

Since communication between vehicles is vulnerable to cyber-attacks, feedback information can be expressed as

$$\begin{align*}
\dot{x}_i(k) &= x_i(k) + \delta_i(k) \\
\dot{v}_i(k) &= v_i(k) + \alpha_i(k),
\end{align*}$$

(5)

Let $\tilde{x}_i(k) = x_i(k) - x^*_i(k)$, $\tilde{v}_i(k) = v_i(k) - v^*_i(k)$, and $\tilde{a}_i(k) = a_i(k) - a^*_i(k)$. Denote the state error $e(k) \triangleq [\tilde{x}(k)^T, \tilde{v}(k)^T, \tilde{a}(k)^T]^T$, where $\tilde{x}(k) = [\tilde{x}_1(k), \ldots, \tilde{x}_n(k)]^T$, $\tilde{v}(k) = [\tilde{v}_1(k), \ldots, \tilde{v}_n(k)]^T$, $\tilde{a}(k) = [\tilde{a}_1(k), \ldots, \tilde{a}_n(k)]^T$, and the attack injection $\xi(k) = [0, \ldots, 0, \xi_1(k), \ldots, \xi_n(k)]^T$.

$$\begin{align*}
ex(k) &= \sum_{j=0}^{n} g_{ij}[\alpha\delta_i(k) + \beta\alpha_i(k) + \gamma\varepsilon_{ij}(k)].
\end{align*}$$

Combining (2), (3), (4) and (5), one derives

$$e(k+1) = Ge(k) + Y\xi(k),$$

where

$$G = \begin{bmatrix}
I_n - \frac{\alpha T^3}{6}L & T I_n - \frac{\beta T^3}{6}L & T^2 I_n - \frac{\gamma T^3}{2}L & \frac{\alpha T^3}{6}L \\
-\frac{\alpha T^3}{2}L & I_n - \frac{\beta T^3}{6}L & T I_n - \frac{\gamma T^3}{2}L & \frac{\alpha T^3}{6}L \\
-\frac{\alpha T^3}{2}L & I_n - \frac{\beta T^3}{6}L & T I_n - \frac{\gamma T^3}{2}L & \frac{\alpha T^3}{6}L \\
-\frac{\alpha T^3}{2}L & I_n - \frac{\beta T^3}{6}L & T I_n - \frac{\gamma T^3}{2}L & \frac{\alpha T^3}{6}L
\end{bmatrix},$$

and $Y = \begin{bmatrix} 0_n & 0_n & T^2 I_n & \frac{\alpha T^3}{6}L \\
0_n & 0_n & T^2 I_n & \frac{\alpha T^3}{6}L \\
0_n & 0_n & T^2 I_n & \frac{\alpha T^3}{6}L \\
0_n & 0_n & T^2 I_n & \frac{\alpha T^3}{6}L
\end{bmatrix}$, where $\hat{L}$ is defined before (4).

Assumption 1 (Gusrialdi [44]): The attacker aims to destabilize the vehicle platoon by inserting injection $\xi(k)$. In fact, the attacker would have a limited budget to launch the attack and any intelligent adversary would prefer to insert a bounded injection because the sufficiently large attacks can be simply excluded from CVSs through a threshold defense mechanism. Moreover, the attacks whose amplitude is close to the actual system errors are difficult to identify, so it is supposed that the attacks conform to the following general form

$$\xi(k+1) = \xi(k) + g(\xi(k), e(k)),$$

which has a finite $L_2$-gain and the expression of function $g(.)$ is unknown. The attack signal after each iteration in (7) will be limited to a reasonable bounded range, which is close to the amplitude of the actual system errors.

### III. MAIN RESULTS

The CVSs should remain stable in the ideal situation without cyber-attacks, including normal design and interaction design, which is the basis for stable driving of the vehicle platoon. Therefore, in the following analysis, we first derive the stability conditions for CVSs in the absence of an attack, and then we investigate the robustness of the systems under cyber-attacks.

### A. CONTROLLER DESIGN FOR THE VEHICLE PLATOON LAYER WITHOUT CYBER-ATTACKS

In normal design, if there are no attacks, the state error dynamics (6) is reduced to

$$e(k+1) = Ge(k).$$

The following theorem gives sufficient and necessary conditions for CVSs to reach stability in the absence of an attack.

Theorem 1: The CVSs (8) derived from (2) can achieve consensus asymptotically if and only if the controller gains in (4) satisfy

$$\begin{align*}
\alpha T^2 + 2\beta T^2 + 12\gamma T^2 &> 6T \\
m_1 &< \gamma < m_2
\end{align*}$$

with

$$m_1 = \frac{-\alpha T^2 + 3\beta T^2 + \frac{\alpha}{2\beta\min_{1 \leq i \leq n}(\lambda_i)}}{6T},$$

$$m_2 = \frac{2}{12T} + \frac{\alpha}{\text{max}_{1 \leq i \leq n}(\lambda_i)},$$

where $\hat{\lambda}$ is defined before (4).
Proof: Let $\theta$ be the eigenvalue of the matrix $G$, and one can derive the eigenvalue polynomial:

$$
\det(\theta I_n - G) = \det\left(\begin{array}{ccc}
\bar{\alpha}T^3L + \bar{\beta}I_n & \beta T^3 - TI_n \\
\alpha T^2L & \beta T^2L + \bar{\beta}I_n \\
\frac{1}{2}\alpha T & \frac{1}{2}\beta TL
\end{array}\right)
$$

$$
= \det\left(\bar{\beta}^3I_n + [(\alpha T^3/6 + \beta T^2/2 + \gamma T)\bar{\beta}^2 + (\alpha T^3 + \beta T^2\bar{\beta} + \alpha T^3]\bar{\beta}I_n \\
+ (\alpha T^3 + \beta T^2\bar{\beta} + \alpha T^3]\bar{\beta}I_n
\right)
$$

$$
= \prod_{i=1}^{n}\left(\bar{\beta}^3I_n + [(\alpha T^3/6 + \beta T^2/2 + \gamma T)\bar{\beta}^2 + (\alpha T^3 + \beta T^2\bar{\beta} + \alpha T^3]\bar{\beta}I_n \\
+ (\alpha T^3 + \beta T^2\bar{\beta} + \alpha T^3]\bar{\beta}I_n
\right) = 0,
\tag{10}
$$

where $\bar{\beta} = \theta - 1$.

Equation (10) is a polynomial of $\theta$ with the degree $3n$. $3n$ eigenvalues of the matrix $G$ can be obtained by solving this equation. It’s not difficult to find that each $\lambda_i$ corresponds to three solutions of $\theta$, so the solution for eigenvalue $\theta$ can be converted to the following formula:

$$
(\theta - 1)^3 + [(\alpha T^3/6 + \beta T^2/2 + \gamma T)(\theta - 1)^2 + (\alpha T^3 + \beta T^2)(\theta - 1) + \alpha T^3]\lambda_i = 0, \quad \forall i = 1, \ldots, n.
\tag{11}
$$

To ensure the stability of the system (8), eigenvalues $\theta$ are all in the unit open circle. Applying bilinear transformation $\theta = (s + 1)/(s - 1)$ [15, 47], one can obtain

$$
\alpha T^3\lambda_i s^3 + (-\alpha T^3 + 2\beta T^2)\lambda_i s^2 + (-\alpha T^3/3 - 2\beta T^2 + 4\gamma T)\lambda_i s + (\alpha T^3/3 - 4\gamma T)\lambda_i + 8 = 0, \quad \forall i = 1, \ldots, n.
\tag{12}
$$

It implies that the system (8) is stable if and only if $Re(s) < 0$. The controller gain $\alpha$ in (4), sampling period $T$ and eigenvalue $\lambda_i$ are all positive, then the conditions in (9) can be derived by using the Routh-Hurwitz stability criterion.

Remark 1: For the controller design in Theorem 1, firstly, an appropriate network topology can be selected according to the actual position of the vehicles and the communication cost to determine $\lambda_i$. Secondly, the sampling period $T$ of CVSSs should be decided based on the performance of the sensor networks. Finally, the controller gains $\alpha$, $\beta$ and $\gamma$ in (4) can be determined in the line with the condition (9).

B. INTERACTION NETWORK DESIGN WITHOUT CYBER-ATTACKS

To deal with potential cyber-attacks, a hidden layer with the number of nodes equal to $n$ is introduced to interact with the original vehicle platoon layer, as shown in Fig. 1 (n is assumed to be 4 in the figure). To this end, systems (8) can be rewritten as the following cooperative systems

$$
\begin{cases}
\begin{array}{l}
\dot{e}(k + 1) = Ge(k) + Kz(k) \\
\dot{z}(k + 1) = Dz(k) + Ee(k),
\end{array}
\end{cases}
\tag{13}
$$

where $K$, $D$ and $E$ are $3n \times 3n$ matrices to be designed, and $z(k) = [z_1(k), z_2(k), \ldots, z_{3n}(k)]^T$ is the state vector of the virtual system in the hidden layer.

The hidden layer can be implemented as an internal signal component at each follower of the vehicle platoon layer. For the transmission of information in the hidden layer, different communication networks can be used, such as internet technology or software-defined networking [45], which is a promising approach in network management and cloud computing.

The following lemmas are given to design the interaction matrices in (13) and guarantee the stability of the systems.

Lemma 1: Choose the appropriate matrix $D$ to ensure $\sigma(D) \subset B(0, 1)$. At the same time, the matrix $G$ designed in section III-A also meets $\sigma(G) \subset B(0, 1)$. According to the Lyapunov criterion, there exist positive symmetric matrices $P_s$ and $P_h$ satisfying $G^TP_sG - P_s < 0$ and $D^TP_hD - P_h < 0$. Then positive matrices $Q_s$ and $Q_h$ can be found to meet the following equations

$$
G^TP_sG - P_s = -Q_s,  \tag{14}
$$

$$
D^TP_hD - P_h = -Q_h.  \tag{15}
$$

Remark 2: The discrete-time Lyapunov equation $AXA^T - X + Q = 0$ can be solved by the function $X = \text{lyap}(A, Q)$ in the Matlab toolbox [50]. The description of such function in Matlab is “The solution $X$ is symmetric when $Q$ is symmetric, and positive definite when $Q$ is positive definite and $A$ has all its eigenvalues inside the unit disk.”, from which we know that when matrices $Q_s$ and $Q_h$ are determined, one obtains $P_s$ and $P_h$.

Lemma 2: Given the matrix $G$ ($D$), $P_s$ ($P_h$) in Lemma 1 increases with $Q_s$ ($Q_h$), where increasing means that all elements in the matrix change in the same proportion. To ensure that matrix $Q_s$ ($Q_h$) is positive definite, the scale factor can only be the positive real number.

Proof: From (14) one can obtain

$$
G^TP_sG - P_s = -Q_s,  \tag{14}
$$

$$
(G^2)^TP_sG^2 - G^TP_sG = -G^TQ_sG,  \tag{15}
$$
\[(G^3)^T P_s G^3 - (G^2)^T P_s G^2 = -(G^2)^T Q_s G^2, \]
\[\vdots\]
\[(G^{n+1})^T P_s G^{n+1} - (G^n)^T P_s G^n = -(G^n)^T Q_s G^n. \quad (16)\]
Adding the above formulas, one obtains \((G^{n+1})^T P_s G^{n+1} - P_s = -\sum_{k=0}^{n} (G^k)^T Q_s G^k\). According to \(\sigma(G) \in B(0, 1)\), one can know that \(\lim_{n \to \infty} (G^{n+1})^T P_s G^{n+1} = 0\), so we have
\[P_s = \sum_{k=0}^{\infty} (G^k)^T Q_s G^k. \quad (17)\]
When all elements in matrix \(Q_s\) are multiplied by the same scale factor, all elements in \(P_s\) also change accordingly. To this end, the relationship between \(P_s\) and \(Q_s\) in Lemma 2 is proved, which is also suitable for \(P_h\) and \(Q_h\).

**Lemma 3:** Consider the overall vehicle platoon systems (13) with an interaction network. The systems can achieve consensus asymptotically if (i) matrix \(G\) satisfies the Lyapunov equation (14), (ii) matrix \(D\) satisfies equation (15), (iii) matrix \(E\) satisfies
\[E = -P_h^{-1} D^{-T} K^T P_s G, \quad (18)\]
and (iv) \(Q_h\) is chosen to be sufficiently large and \(Q_s\) is taken small (i.e., The absolute value of each non-zero element in \(Q_h\) is large enough (small enough)).

**Proof:** Select the Lyapunov function candidate as
\[V_{\xi}(k) = e(k)^T P_s e(k) + z(k)^T P_h z(k). \quad (19)\]
Combining (14) and (15), one can obtain
\[\Delta V_{\xi}(k) = V_{\xi}(k + 1) - V_{\xi}(k) = [G e(k) + K z(k)]^T P_h [G e(k) + K z(k)]
+ [D z(k) + E e(k)]^T P_h [D z(k) + E e(k)]
- e(k)^T P_s e(k) - z(k)^T P_h z(k).
\]
Define the error vectors \(\bar{e}(k) \triangleq e(k) - e'(k), \bar{z}(k) \triangleq z(k) - z'(k), and \bar{\xi}(k) \triangleq \xi(k) - \xi'(k).\)
Combining (22) and (24), one obtains
\[\bar{e}(k + 1) = G \bar{e}(k) + K \bar{z}(k) + Y \bar{\xi}(k) = e''(k)
\]
\[\bar{z}(k + 1) = D \bar{z}(k) + E e''(k) = z''(k)
\]
\[\bar{\xi}(k + 1) = \bar{\xi}(k) + g(\bar{\xi}(k), e(k)). \quad (24)\]
Define the error vectors \(\bar{e}(k) \triangleq e(k) - e'(k), \bar{z}(k) \triangleq z(k) - z'(k), and \bar{\xi}(k) \triangleq \xi(k) - \xi'(k).\)
Combining (22) and (24), one obtains
\[\bar{e}(k + 1) = G \bar{e}(k) + K \bar{z}(k) + Y \bar{\xi}(k)
\]
\[\bar{z}(k + 1) = D \bar{z}(k) + E e''(k)
\]
\[\bar{\xi}(k + 1) = \bar{\xi}(k) + g(\bar{\xi}(k), e(k)). \quad (25)\]

According to the converse Lyapunov theorem [44], there exists a Lyapunov function \(V_{\bar{\xi}}(k)\) related to \(\bar{\xi}(k)\) with the following property
\[\Delta V_{\bar{\xi}}(k) < -v \|\bar{\xi}(k)\|^2, \quad (26)\]
where \(v\) is a positive constant. To verify that the interactive error systems (25) are asymptotically stable under cyber-attacks, one selects a Lyapunov function candidate as
\[V_{\bar{\epsilon}, \bar{z}, \bar{\xi}}(k) = \bar{e}(k)^T P_h \bar{e}(k) + \bar{z}(k)^T P_h \bar{z}(k) + \eta V_{\bar{\xi}}(k), \quad (27)\]
where \(\eta\) is the positive real number. Similar to (20), one can achieve
\[\Delta V_{\bar{\epsilon}, \bar{z}, \bar{\xi}}(k) = V_{\bar{\epsilon}, \bar{z}, \bar{\xi}}(k + 1) - V_{\bar{\epsilon}, \bar{z}, \bar{\xi}}(k)
\]
\[= \bar{e}(k)^T (G^T P_s G + E^T P_h E - P_s) \bar{e}(k)
\]
According to Lemma 2, \(P_h\) increases with \(Q_h\), and \(P_s\) decreases with \(Q_s\), so the first, second and third terms in the final form of equation (21) can be forced to converge to an arbitrarily small range by increasing \(Q_h\) and taking small
\(Q_s\), meanwhile, the fourth term increases with \(Q_h\), thus (21) is negative with sufficiently large \(Q_h\) and small \(Q_s\). So far, \(\Delta V_{\bar{\epsilon}, \bar{z}}(k) < 0\) can be guaranteed, simultaneously Lemma 3 is obtained.

**C. RESILIENT CONTROL DESIGN WITH CYBER-ATTACKS IN THE VEHICLE PLATOON LAYER**
Considering that the vehicle platoon layer is subject to attacks satisfying Assumption 1, systems (13) can be rewritten as:
\[\begin{align*}
    e(k + 1) &= Ge(k) + Kz(k) + Y\xi(k) \\
    z(k + 1) &= Dz(k) + Ee(k) \\
    \xi(k + 1) &= \xi(k) + g(\xi(k), e(k)).
\end{align*} \quad (22)\]

The following theorem shows the stable conditions of interactive systems (22).

**Theorem 2:** Consider the interactive systems subject to cyber-attacks in the vehicle platoon layer (i.e., the systems (22)). The systems are bounded for any injection satisfying (7) if the conditions in Lemma 3 hold. Moreover, the system errors satisfy
\[\lim_{k \to \infty} e(k) = -[(G - I_{3n}) - K(D - I_{3n})^{-1}E]^{-1}Y\xi, \quad (23)\]
where \(\xi\) is the steady state of the injection \(\xi\).

**Proof:** Let the equilibrium of \(e(k), z(k), and \xi(k)\) be \(e'(k), z'(k), and \xi'(k), respectively. One can derive
\[\begin{align*}
e''(k + 1) &= Ge''(k) + Kz''(k) + Y\xi(k) = e''(k) \\
    z''(k + 1) &= Dz''(k) + Ee''(k) = z''(k) \\
    \xi''(k + 1) &= \xi'(k) + g(\xi'(k), e'(k)).
\end{align*} \quad (24)\]

Define the error vectors \(\bar{e}(k) \triangleq e(k) - e'(k), \bar{z}(k) \triangleq z(k) - z'(k), and \bar{\xi}(k) \triangleq \xi(k) - \xi'(k).\) Combining (22) and (24), one obtains
\[\begin{align*}
    \bar{e}(k + 1) &= G \bar{e}(k) + K \bar{z}(k) + Y \bar{\xi}(k) \\
    \bar{z}(k + 1) &= D \bar{z}(k) + E \bar{e}(k) \\
    \bar{\xi}(k + 1) &= \bar{\xi}(k) + g(\bar{\xi}(k), e(k)).
\end{align*} \quad (25)\]

According to the converse Lyapunov theorem [44], there exists a Lyapunov function \(V_{\bar{\xi}}(k)\) related to \(\bar{\xi}(k)\) with the following property
\[\Delta V_{\bar{\xi}}(k) < -v \|\bar{\xi}(k)\|^2, \quad (26)\]
where \(v\) is a positive constant. To verify that the interactive error systems (25) are asymptotically stable under cyber-attacks, one selects a Lyapunov function candidate as
\[V_{\bar{\epsilon}, \bar{z}, \bar{\xi}}(k) = \bar{e}(k)^T P_h \bar{e}(k) + \bar{z}(k)^T P_h \bar{z}(k) + \eta V_{\bar{\xi}}(k), \quad (27)\]
where \(\eta\) is the positive real number. Similar to (20), one can achieve
\[\Delta V_{\bar{\epsilon}, \bar{z}, \bar{\xi}}(k) = V_{\bar{\epsilon}, \bar{z}, \bar{\xi}}(k + 1) - V_{\bar{\epsilon}, \bar{z}, \bar{\xi}}(k)
\]
obtains by selecting (22). Then, (29) can be guaranteed to be negative can be easily computed based on (18). For $3\xi^T k Y^T P_s Y \xi + \eta \Delta V_{\xi}(k)$, combining (26) one obtains

$$3\xi^T k Y^T P_s Y \xi + \eta \Delta V_{\xi}(k) < 3\lambda_{\max}(P_s) \| Y \|_2^2 \| \xi(k) \|^2 + 3\lambda_{\max}(P_s) \| Y \|_2^2 \| \xi(k) \|^2 \leq 3\lambda_{\max}(P_s) \| Y \|_2^2 \| \xi(k) \|^2.$$ (29)

Note that $\eta$ in (29) is a parameter of the Lyapunov function candidate (27), so the change of $\eta$ only means the variation of the selected Lyapunov function, and does not affect the matrix selection of (22). Then, (29) can be guaranteed to be negative by selecting $\eta > 3\lambda_{\max}(P_s) \| Y \|_2^2 / \nu$. Besides,

$$\xi^T k \{ 2G^T P_s G + E^T P_s E - P_s \} \xi $$

$$+ \xi^T k \{ 2K^T P_s K + D^T P_s D - P_s \} \xi $$

$$= [G \xi(k)]^T P_s [G \xi(k)] + [K \xi(k)]^T P_s [G \xi(k)]$$

$$- \xi^T k Q \xi - \xi^T k Q \xi $$

$$= [D^T K^T P_s G \xi(k)]^T P_s^{-1} [D^T K^T P_s G \xi(k)]$$

$$+ [G \xi(k)]^T P_s [G \xi(k)] + [K \xi(k)]^T P_s [K \xi(k)]$$

$$- \xi^T k Q \xi - \xi^T k Q \xi .$$ (30)

Similar to the negative judgment of (21), (30) is negative by increasing $Q_h$ and taking small $Q_s$. So far, $\Delta V_{\xi}(k) < 0$ can be guaranteed, thus the error systems (25) will eventually converge to 0 (i.e., $\lim e(k) = e^e(k)$). Let $\lim \xi^e(k) = \xi^e$, and one can achieve the expression of the system errors (23) by combining the first and second formulas in (24). Theorem 2 is proved.

Remark 3: Theorem 2 gives the conditions of the interaction matrices for CVSs to resist cyber-attacks in the vehicle platoon layer. Specifically, to design such a resilient system, firstly, the conditions of the controller gains in Theorem 1 must be satisfied, which helps to design the matrix $G$ and ensure that the Lyapunov equation (14) holds. Secondly, an appropriate matrix $D$ should be selected to guarantee the establishment of the equation (15). Thirdly, the matrix $K$ is determined and sufficiently large $Q_h$ and small $Q_s$ are selected, simultaneously, one obtains the matrices $P_s$ and $P_s$. As described in Remark 2. Finally, the interaction matrix $E$ can be easily computed based on (18).

Remark 4: From (23) one knows the system errors $e(k)$ cannot converge to 0 because $\xi^e \neq 0$ when there exists a cyber-attack. Besides, it is known from Lemma 2 that when increasing $Q_h$ and taking small $Q_s$ (i.e., all elements in $Q_h$, $Q_s$ increase (decrease) in the same proportion) to stabilize the interactive systems (22), the absolute value of each non-zero element in $P_h$ will become larger and that in $P_s$ gets smaller, concurrently $-K(D-I_{3n})^{-1}E = K(D-I_{3n})^{-1}P_h^{-1}D^T K^T P_s G$ in (23) can be forced to converge to an arbitrarily small neighborhood around $0_{3n}$. In this case, the system errors can be rewritten as $\lim e(k) = -(G-I_{3n})^{-1}Y \xi^e$, which is bounded for any injection $\xi$ satisfying (7). Note that in this case $-[(G-I_{3n})-K(D-I_{3n})^{-1}E]$ is not the optimal matrix that minimizes the system errors (23), so when we take infinitely large $Q_h$ and make $Q_s$ infinitely close to $0_{3n}$, (23) converges to a bounded range but not a minimum range. As a special case, the system errors converge to 0 accurately when there are no cyber-attacks.

D. ROBUSTNESS ANALYSIS WITH CYBER-ATTACKS IN THE OVERALL SYSTEMS

Next, one considers the case that the virtual system in the hidden layer, designed in section III-B to enhance the robustness of the systems, is also disturbed by cyber-attacks. To this end, the overall systems subject to cyber-attacks can be considered as

$$\begin{align*}
\xi(k+1) &= \xi(k) + \xi^e(k) + \xi^v(k) + \xi^f(k) \\
\xi^e(k+1) &= \xi^e(k) + g(\xi^e(k), e(k)) \\
\xi^v(k+1) &= \xi^v(k) + g'(\xi^e(k), z(k)).
\end{align*}$$ (31)

where $\xi^e(k)$ also satisfies Assumption 1. Then the following theorem is given to show the boundary and stabilization properties of systems (31).

Theorem 3: Consider the interactive CVSs subject to cyber-attacks in the overall systems (31). The systems are bounded for any injection $\xi$ and $\xi^v$ satisfying (7) if the conditions (i), (ii) and (iv) in Lemma 3 hold and $\sigma(\sqrt{2} D) \subset B(0,1)$. Moreover, the system errors of (31) satisfy

$$\lim_{k \to \infty} e(k) = [(G-I_{3n})-K(D-I_{3n})^{-1}E]^{-1} \times (K(D-I_{3n})^{-1}Y \xi^v - Y \xi^e) ,$$ (32)

where $\xi^v$ and $\xi^e$ are the steady states of the injections $\xi$ and $\xi^v$, respectively.

Proof: Equilibria of the systems (31) satisfies

$$\begin{align*}
\xi^e(k+1) &= Ge^e(k) + Kz^e(k) + Yz^e(k) = e^e(k) \\
z^e(k+1) &= Dz^e(k) + Ee^e(k) + Yz^v(k) = z^e(k) \\
\xi^v(k+1) &= \xi^v(k) + g(\xi^e(k), e^e(k)) = \xi^v(k) \\
\xi^e(k+1) &= \xi^e(k) + g'(\xi^e(k), z(k)) = \xi^v(k).
\end{align*}$$ (33)

Similar to the proof of Theorem 2, we have the error system for (31) as

$$\begin{align*}
\xi(k+1) &= G\xi(k) + Kz(k) + Y\xi(k) \\
z(k+1) &= Dz(k) + E\xi(k) + Y\xi(k) \\
\xi^e(k+1) &= \xi^e(k) + g(\xi^e(k), e(k)) \\
\xi^v(k+1) &= \xi^v(k) + g'(\xi^e(k), z(k)).
\end{align*}$$ (34)
A Lyapunov function candidate $V_{\xi}^{'}(k)$ related to $\xi^{'}(k)$ can be found with the following property
\begin{equation}
\Delta V_{\xi}^{'}(k) < -v^{'}\|\xi^{'}(k)\|^2, \tag{35}
\end{equation}
where $v^{'}$ is a positive constant. Select the Lyapunov function candidate as
\begin{equation}
V_{\bar{e},\bar{e},\bar{\xi},\bar{\xi}}^{'}(k) = \bar{e}(k)^T P_{\bar{e}} \bar{e}(k) + \bar{\xi}(k)^T P_{\bar{\xi}} \bar{\xi}(k) + \eta V_{\bar{z}}^{'}(k) + \eta' V_{\bar{z}}^{'}(k), \tag{36}
\end{equation}
where $\eta'$ is the positive real number. Then one can achieve
\begin{equation}
\Delta V_{\bar{e},\bar{e},\bar{\xi},\bar{\xi}}^{'}(k) = V_{\bar{e},\bar{e},\bar{\xi},\bar{\xi}}^{'}(k+1) - V_{\bar{e},\bar{e},\bar{\xi},\bar{\xi}}^{'}(k) = \bar{e}(k)^T (2G^T P_s G + 2ET P_{\bar{e}} E - P_{\bar{e}}) \bar{e}(k) + \bar{\xi}(k)^T (2K^T P_s K + 2D^T P_{\bar{\xi}} D - P_{\bar{\xi}}) \bar{\xi}(k) - \bar{e}(k) P_{\bar{e}} \bar{e}(k) - \bar{\xi}(k) P_{\bar{\xi}} \bar{\xi}(k) - \bar{e}(k)^T P_{\bar{e}} \bar{\xi}(k) - \bar{\xi}(k)^T P_{\bar{\xi}} \bar{e}(k) - \eta V_{\bar{z}}^{'}(k) - \eta' V_{\bar{z}}^{'}(k).
\end{equation}
For $3\bar{e}(k)^T Y^T P_s Y \bar{e}(k) + \eta' \Delta V_{\bar{z}}^{'}(k)$, similar to (29), by choosing $\eta' > 3\lambda_{\text{max}}(P_s)\|Y\|^2/v'$, a negative value can be determined.

If the condition $\sigma(\sqrt{D}) \subset B(0, 1)$ in Theorem 3 holds, the following Lyapunov equation similar to (15) can be found
\begin{equation}
2D^T P_{\bar{\xi}} - P_{\bar{\xi}} = -Q_{\bar{\xi}}. \tag{38}
\end{equation}

Then one can obtain
\begin{equation}
\bar{e}(k)^T (2G^T P_s G + 2ET P_{\bar{e}} E - P_{\bar{e}}) \bar{e}(k) + \bar{\xi}(k)^T (2K^T P_s K + 2D^T P_{\bar{\xi}} D - P_{\bar{\xi}}) \bar{\xi}(k) - \bar{e}(k)^T P_{\bar{e}} \bar{e}(k) - \bar{\xi}(k)^T P_{\bar{\xi}} \bar{\xi}(k) - \bar{e}(k)^T P_{\bar{e}} \bar{\xi}(k) - \bar{\xi}(k)^T P_{\bar{\xi}} \bar{e}(k) - \eta V_{\bar{z}}^{'}(k) - \eta' V_{\bar{z}}^{'}(k).
\end{equation}

Referring to the negative judgment of (30) and (28) in Theorem 2, (39) and (37) can be made negative by increasing $Q_{\bar{\xi}}$ and taking small $Q_{\bar{e}}$, so the error system (34) will eventually converge to 0. Similar to the derivation of (23), it is not difficult to achieve the system errors (32). The proof is completed.

Remark 5: Theorem 3 develops the conditions of the interaction matrices that enable the cooperative CVSs resistant to attacks in the overall system. The design of such resilient CVSs is similar to the process described in Remark 3. The only difference is that the constraint on the matrix $D$ is $\sigma(\sqrt{D}) \subset B(0, 1)$ in Theorem 3 and $\sigma(D) \subset B(0, 1)$ in Theorem 2 (The constraint on matrix $D$ in Theorem 2 is the same as that in Lemmas 1 and 3). Both of these constraints should be satisfied because CVSs are supposed to remain stable in all four design cases in section III

Remark 6: Similar to the analysis in Remark 4, it can be known from (32) that the system errors of (31) can also converge to a bounded range for any injection $\xi$ and $\xi^{'}$ satisfying (7). Therefore, the stabilization of cooperative CVSs can be guaranteed even if the overall systems are under cyber-attacks.

Remark 7: It can be known from Theorems 2 and 3 that CVSs can reach a global consensus under any attacks satisfying Assumption 1. The dynamics (i.e., the function $g(.)$ in (7)) of such attacks is unknown for CVSs, which means the injection inserted by the attacker in (5) can be multiple types, including false data injection, data modification, and data replay.

Remark 8: The proposed method is different from the existing works [44], [46], [47]. The existing consensus analysis methods for the third-order discrete-time systems ignored the sampling period $T$ of the dynamic model [46], [47], which means Theorem 1 in this paper provides more rigorous guidelines for the consensus design of the third-order discrete-time multi-agent systems in the absence of cyber-attacks. Besides, this paper proposes new Lyapunov analysis methods (seen in section III B-D) for the cooperative interaction design of the discrete-time systems, which are obviously different from the design methods for the continuous-time systems [44]. Moreover, we only need a matrix $G$ satisfying $\sigma(G) \subset B(0, 1)$ to design the resilient systems, so the proposed method can be easily applied to the second-order or first-order discrete-time systems.

IV. SIMULATIONS

Consider a vehicle platoon consisting of a leader and four followers ($n = 4$) that travels straight at a constant speed of $v_0$, where the expected distance between adjacent vehicles is $d = 20m$. To verify the convergence of the vehicle platoon systems with or without attacks, we consider that each follower has a different initial state. Set initial position, velocity, and acceleration vectors as $[x_0(0), \ldots, x_4(0)]^T = [100, 90, 65, 10, -5]^T$, $[v_0(0), \ldots, v_4(0)]^T = [20, 15, 5, 35, 30]^T$, and $[a_0(0), \ldots, a_4(0)]^T = [0, -10, 20, -15, 10]^T$ respectively. The design method of the controller gains in (4) was illustrated in Remark 1. Firstly, note that the proposed network topology in this paper is applicable to the undirected graph and directed graph. Taking directed graph as an example, considering the physical distance and communication cost, we suppose that vehicle $i$ can only receive the messages from the vehicle $i-1$ ($i = 1, \ldots, n$). Correspondingly, matrix $L$ and matrix $L_0$ in section II-B are determined, which are
\begin{equation}
L = \begin{bmatrix}
0 & 0 & 0 & 0 \\
-1 & 1 & 0 & 0 \\
0 & -1 & 1 & 0 \\
0 & 0 & -1 & 1
\end{bmatrix}
\end{equation}
and
\begin{equation}
L_0 = \text{diag}[1 \ 0 \ 0 \ 0].
\end{equation}
Then, we assume the sampling period $T = 0.03s$, which is affordable for most
sensor networks. Finally, we set the controller gains $\alpha = 2$, $\beta = 3$, and $\gamma = 4$ to meet Theorem 1. Next, simulation results in several different scenarios would be given to demonstrate the validity of the proposed methods.

**A. THE CASE WITHOUT THE HIDDEN LAYER AND IN THE ABSENCE OF CYBER-ATTACKS**

In the case without the hidden layer and in the absence of cyber-attacks (i.e., the systems (8)), the vehicle platoon is allowed to travel for 18 seconds under the control protocol (4). The trajectories of position $x_i$, position error $e_{xi}$, velocity error $e_{vi}$, and acceleration error $e_{ai}$ of vehicle $i$ are shown in Fig. 2. As can be seen in Fig. 2(a), no collision occurred during the driving process (The curves do not intersect). Besides, the control objectives in (3) can be reached eventually, i.e., the state errors converge to 0 (see Fig. 2(b), Fig. 2(c) and Fig. 2(d)).

**B. THE CASE WITH THE HIDDEN LAYER AND IN THE ABSENCE OF CYBER-ATTACKS**

For comparison, we add a hidden layer except for the lead vehicle while retaining the parameters used in section IV-A (i.e., the parameters designed at the beginning of section IV). The design method for such interaction systems (i.e., the systems (13)) was mentioned in Remark 3 and Remark 5, which would be demonstrated below. To satisfy the constraint on the matrix $D$ in Lemma 1, let $D = 0.6I_{12}$. Besides, the other parameters are set as follows: $K = 0.25I_{12}$, $Q_s = 0.01I_{12}$ and $Q_h = 8Q_s$. Then one has the solutions of the equations (14) and (15), which are $P_s = dlyap(G^T, Q_s)$ and $P_h = dlyap(D^T, Q_h)$. Until now, it is easy to compute the interaction matrix $E$ based on (18) in Lemma 3. After 6 seconds of similar running, the state change curves are shown in Fig. 3. It can be seen from Fig. 3(a) that no collision occurs when adjusting the vehicle platoon (The hidden layer does not affect the convergence of the original systems). Besides, the hidden layer accelerates the convergence speed of the spacing error, velocity error, and acceleration error (see Fig. 3(b), Fig. 3(c), and Fig. 3(d)). It takes more than 10s for CVSs without a hidden layer to reach stability (as shown in Fig. 2), but the convergence time is reduced to within 1s after adding the hidden layer (see Fig. 3). By comparing the simulation in section IV-A and section IV-B, we can see that the interactive design improves the stability of the vehicle platoon in the absence of cyber-attacks.

**C. THE CASE WITHOUT THE HIDDEN LAYER AND IN THE PRESENCE OF CYBER-ATTACKS**

In this simulation, the parameters used in section IV-A are retained and the vehicle platoon (i.e., the systems (8)) is exposed to cyber-attacks. Since the attack is unknown to the interactive systems, it is assumed that $\xi(k) = [0, \cdots, 0, \xi_1(k), \xi_2(k), \xi_3(k), \xi_4(k)]$, where $\|\xi(k)\| < 50$.

The amplitude of such attack signals is close to the maximum of the actual position error, speed error, and acceleration.
error, so it is difficult to identify them through the threshold defense mechanism. The simulation results in Fig. 4 show that without protection (i.e., without the hidden layer), attacks will destabilize the vehicle platoon. As can be seen in Fig. 4(a), collisions occurred in the driving process. Besides, the system errors cannot converge to the ideal range (see Fig. 4(b), Fig. 4(c) and Fig. 4(d)).

D. THE CASE AGAINST CYBER-ATTACKS IN THE VEHICLE PLATOON LAYER

Based on the simulation in section IV-C, we make the systems robust against the attacks by connecting the vehicle platoon systems to the same hidden layer as in IV-B (i.e., the systems (22)). After 6 seconds of similar running, the simulation results are shown in Fig. 5. Compared with the simulation results shown in Fig. 4, it can be seen that the robustness of the vehicle platoon has been significantly improved (No collision occurred during platoon adjustment (see Fig. 5(a)) and state errors converged to the ideal bounded range (see Fig. 5(b), Fig. 5(c) and Fig. 5(d)).

E. THE CASE AGAINST CYBER-ATTACKS IN THE VEHICLE PLATOON LAYER AND THE HIDDEN LAYER

In this section, we assume that the virtual system (hidden network) is also attacked as described in (31), where \( \xi'(k) \) is considered to have the same limitation as \( \xi(k) \) in IV-C, and the hidden network used is identical with it in IV-D. As shown in Fig. 6, the stability of the vehicle platoon is still guaranteed despite of the attacks on both networks.

According to the above simulation, we can know that the robustness of the CVSs has been significantly improved by adding the hidden network. The results show that the
interaction design gives the vehicle platoon strong resistance to cyber-attacks. 

Remark 9: As demonstrated above, the cooperative systems with the hidden network can guarantee the resilient consensus of CVSs under cyber-attacks. In practical applications, virtual nodes that have no physical meaning can be added to each agent of CPS to form the hidden network (as shown in Fig. 1), and then the control strategy in this paper could be applied to design the interaction matrices. After determining the interaction matrices, it is not difficult to achieve the entire cooperative interaction network topology with the physical layer and the hidden layer through software-defined networking [45]. Therefore, the approach proposed in this paper can not only be used for resilient control of vehicle platoon but also can be utilized to ensure the stability of other discrete-time multi-agent systems under cyber-attacks.

V. CONCLUSION

In this paper, the resilient consensus of third-order discrete-time CVSs subject to cyber-attacks with unknown non-linear dynamics has been studied. In the absence of an attack, the necessary and sufficient conditions for CVSs to reach stability have been first derived. Based on the Lyapunov-based method proposed to design the cooperative interaction CVSs that have a strong resistance to attacks. It has been proved that the system errors of cooperative CVSs can be controlled within a bounded range under all possible attacks. In the end, simulations have been made to verify the feasibility of the theoretical method. The proposed approach has superior performance and is also suitable for resilient control of other multi-agent systems based on first-order or high-order discrete-time dynamics. However, this paper does not give the design method of interaction matrices that can minimize the system errors of CVSs under attacks. In our future work, the optimal control framework would be utilized to design the optimal interaction matrices. Besides, the control performance of cooperative interaction systems under low communication rates will be investigated to reduce communication consumption and computational burden.

REFERENCES

[1] L. Xu, L. Y. Wang, G. Yin, and H. Zhang, “Communication information structures and contents for enhanced safety of highway vehicle platoons,” IEEE Trans. Veh. Technol., vol. 63, no. 9, pp. 4206–4220, Nov. 2014.

[2] A. Alam, B. Besselink, V. Turri, J. Mårtensson, and K. H. Johansson, “Heavy-duty vehicle platooning for sustainable freight transportation: A cooperative method to enhance safety and efficiency,” IEEE Control Syst. Mag., vol. 35, no. 6, pp. 34–56, Dec. 2015.

[3] W. Wang, B. Han, Y. Guo, X. Luo, and M. Yuan, “Fault-tolerant platoon control of autonomous vehicles based on event-triggered control strategy,” IEEE Access, vol. 8, pp. 25122–25134, 2020.

[4] H. Qi, R. Dai, Q. Tang, and X. Hu, “Coordinated intersection signal design for mixed traffic flow of human-driven and connected and autonomous vehicles,” IEEE Access, vol. 8, pp. 26067–26084, 2020.

[5] K. C. Dey, L. Yan, X. Wang, Y. Wang, H. Shen, M. Chowdhury, L. Yu, C. Qiu, and V. Soundararaj, “A review of communication, driver characteristics, and controls aspects of cooperative adaptive cruise control (CAAC),” IEEE Trans. Intell. Transp. Syst., vol. 17, no. 2, pp. 491–509, Feb. 2016.

[6] Y. Liu, B. Xu, and Y. Ding, “Convergence analysis of cooperative braking control for interconnected vehicle systems,” IEEE Trans. Intell. Transp. Syst., vol. 18, no. 7, pp. 1894–1906, Jul. 2017.

[7] Y. Liu, C. Pan, H. Gao, and G. Guo, “Cooperative spacing control for interconnected vehicle systems with input delays,” IEEE Trans. Veh. Technol., vol. 66, no. 12, pp. 10692–10704, Dec. 2017.

[8] R. Olfati-Saber, “Flocking for multi-agent dynamic systems: Algorithms and theory,” IEEE Trans. Autom. Control, vol. 51, no. 3, pp. 404–420, Mar. 2006.

[9] Y. Liu and B. Xu, “Improved protocols and stability analysis for multivehicle cooperative autonomous systems,” IEEE Trans. Intell. Transp. Syst., vol. 16, no. 5, pp. 2700–2710, Oct. 2015.

[10] R. Olfati-Saber and R. M. Murray, “Consensus problems in networks of agents with switching topology and time-delays,” IEEE Trans. Autom. Control, vol. 49, no. 9, pp. 1520–1533, Sep. 2004.

[11] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W.-C. Hong, “A survey on decentralized consensus mechanisms for cyber physical systems,” IEEE Access, vol. 8, pp. 54371–54401, 2020.

[12] Y. Zheng, S. Eben Li, J. Wang, D. Cao, and K. Li, “Stability and scalability of homogeneous vehicular platoon: Study on the influence of information flow topologies,” IEEE Trans. Intell. Transp. Syst., vol. 17, no. 1, pp. 14–26, Jan. 2016.

[13] W. Yu, G. Chen, and M. Cao, “Some necessary and sufficient conditions for second-order consensus in multi-agent dynamical systems,” Automatica, vol. 46, no. 6, pp. 1089–1095, Jun. 2010.

[14] Y. Zhang and Y. Liu, “Nonlinear second-order multi-agent systems subject to antagonistic interactions without velocity constraints,” Appl. Math. Comput., vol. 364, Jan. 2020, Art. no. 124667.

[15] H. Zhao and S. Fei, “The consensus for discrete-time heterogeneous networked systems consisting of second-order agents and third-order agents,” IEEE Access, vol. 6, pp. 14204–14211, 2018.

[16] C. Huang, G. Zhai, and G. Xu, “Necessary and sufficient conditions for consensus in third-order multi-agent systems,” IEEE/CAA J. Automatica Sinica, vol. 5, no. 6, pp. 1044–1053, Nov. 2018.

[17] X. Lyu, Q. Ai, Z. Yan, S. He, X. Luan, and F. Liu, “Finite-time asynchronous resilient observer design of a class of non-linear switched systems with time-delays and uncertainties,” IET Control Theory Appl., vol. 14, no. 7, pp. 952–963, Apr. 2020.

[18] S. He, Q. Ai, C. Ren, J. Dong, and F. Liu, “Finite-time resilient controller design of a class of uncertain nonlinear systems with time-delays under asynchronous switching,” IEEE Trans. Syst., Man, Cybern., Syst., vol. 49, no. 2, pp. 281–286, Feb. 2019.

[19] W. Cui, Y. Tang, J.-A. Fang, and J. Kurths, “Consensus analysis of second-order multi-agent networks with sampled data and packet losses,” IEEE Access, vol. 4, pp. 8127–8137, 2016.

[20] B. Zhang, C. Dou, D. Yue, Z. Zhang, and T. Zhang, “A packet loss-dependent event-triggered cyber-physical cooperative control strategy for isolated microgrid,” IEEE Trans. Cybern., early access, Dec. 13, 2020, doi: 10.1109/TCYB.2019.2954181.

[21] X. Xie, D. Yue, H. Zhang, and C. Peng, “Control synthesis of discrete-time T–S fuzzy systems: Reducing the conservatism whilst alleviating the computational burden,” IEEE Trans. Cybern., vol. 47, no. 9, pp. 2480–2491, Sep. 2017.

[22] X. Xie, D. Yue, and J. H. Park, “Enhanced switching stabilization of discrete-time Takagi–Sugeno fuzzy systems: Reducing the conservatism and alleviating the on-line computational burden,” IEEE Trans. Fuzzy Syst., early access, Apr. 13, 2020, doi: 10.1109/TFUZZ.2020.2986670.

[23] J. Duan and M.-Y. Chow, “A novel data integrity attack on consensus-based distributed energy management algorithm using local information,” IEEE Trans. Ind. Informat., vol. 15, no. 3, pp. 1544–1553, Mar. 2019.

[24] Z. Shi, R. Sun, R. Lu, L. Chen, J. Chen, and X. S. Shen, “Diverse grouping-based aggregation protocol with error detection for smart grid communications,” IEEE Trans. Smart Grid, vol. 6, no. 6, pp. 2856–2868, Nov. 2015.

[25] C. Zhao, J. He, and J. Chen, “Resilient consensus with mobile detectors against malicious attacks,” IEEE Trans. Signal Inf. Process. Netw., vol. 4, no. 1, pp. 60–69, Mar. 2018.

[26] Z. A. Biron, S. Dey, and P. Psu, “Resilient control strategy under denial of service in connected vehicles,” in Proc. Amer. Control Conf. (ACC), May 2017, p. 4971.

[27] Y. Yuan, H. Yuan, L. Guo, H. Yang, and S. Sun, “Resilient control of networked control system under DoS attacks: A unified game approach,” IEEE Trans. Ind. Inform., vol. 12, no. 5, pp. 1786–1794, Oct. 2016.
[28] Y. Tang, D. Zhang, X. Jin, D. Yao, and F. Qian, “Resilient attitude tracking algorithm for mechanical systems,” IEEE/ASME Trans. Mechatronics, vol. 24, no. 6, pp. 2550–2561, Dec. 2019.

[29] Y. Tang, D. Zhang, P. Shi, W. Zhang, and F. Qian, “Event-based formation control for multi-agent systems under DoS attacks,” IEEE Trans. Autom. Control, early access, Mar. 10, 2020, doi: 10.1109/TAC.2020.2979936.

[30] M. Zhu and S. Martinez, “On the performance analysis of resilient networked control systems under replay attacks,” IEEE Trans. Autom. Control, vol. 59, no. 3, pp. 804–808, Mar. 2014.

[31] G. Franzé, F. Tedesco, and W. Lucia, “Resilient control for cyber-physical systems subject to replay attacks,” IEEE Contr. Syst. Lett., vol. 3, no. 4, pp. 984–989, Oct. 2019.

[32] B. Chen, D. W. C. Ho, G. Hu, and L. Yu, “Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks,” IEEE Trans. Cybern., vol. 48, no. 6, pp. 1862–1876, Jun. 2018.

[33] Y. Mo and B. Sinopoli, “Secure control against replay attacks,” in Proc. 47th Ann. Allerton Conf. Commun., Control, Comput. (Allerton), Sep./Oct. 2009, pp. 911–918.

[34] C. Kwon, W. Liu, and I. Hwang, “Security analysis for cyber-physical systems against stealthy deception attacks,” in Proc. Amer. Control Conf., Washington, DC, USA, Jun. 2013, pp. 3344–3349.

[35] D. Ding, Z. Wang, D. W. C. Ho, and G. Wei, “Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks,” IEEE Trans. Cybern., vol. 47, no. 8, pp. 1936–1947, Aug. 2017.

[36] D. Ding, Z. Wang, Q.-L. Han, and G. Wei, “Security control for discrete-time stochastic nonlinear systems subject to deception attacks,” IEEE Trans. Syst., Man, Cybern., Syst., vol. 48, no. 5, pp. 779–789, May 2018.

[37] W. Fu, J. Qin, Y. Shi, W. X. Zheng, and Y. Kang, “Resilient consensus of discrete-time complex cyber-physical networks under deception attacks,” IEEE Trans. Ind. Informat., vol. 16, no. 7, pp. 4868–4877, Jul. 2020.

[38] E. Mousavinejad, F. Yang, Q.-L. Han, and V. Vlacic, “A novel cyber attack detection method in networked control systems,” IEEE Trans. Cybern., vol. 48, no. 11, pp. 3254–3264, Nov. 2018.

[39] M. R. Camana Acosta, S. Ahmed, C. E. Garcia, and I. Koo, “Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks,” IEEE Access, vol. 8, pp. 19921–19933, 2020.

[40] J. Wang, L. Shen, J. Xia, Z. Wang, and X. Chen, “Asynchronous dissipative filtering for nonlinear jumping systems subject to fading channels,” J. Franklin Inst., vol. 357, no. 1, pp. 589–605, Jan. 2020.

[41] J. Wang, C. Yang, H. Shen, J. Cao, and L. Rutkowski, “Sliding-mode control for slow-sampling singularly perturbed systems subject to Markov jump parameters,” IEEE Trans. Syst., Man, Cybern., Syst., early access, Mar. 24, 2020, doi: 10.1109/TSMC.2020.2979860.

[42] P. Cheng, J. Wang, S. He, X. Luan, and F. Liu, “Observer-based asynchronous fault detection for conic-type nonlinear jumping systems and its application to separately excited DC motor,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 67, no. 3, pp. 951–962, Mar. 2020.

[43] P. Cheng, S. He, J. Cheng, X. Luan, and F. Liu, “Asynchronous output feedback control for a class of conic-type nonlinear hidden Markov jump systems within a finite-time interval,” IEEE Trans. Syst., Man, Cybern., Syst., early access, Mar. 25, 2020, doi: 10.1109/TSMC.2020.2980312.

[44] A. Gusrialdi, Z. Qu, and M. A. Simaan, “Competitive interaction design of cooperative systems against attacks,” IEEE Trans. Autom. Control, vol. 63, no. 9, pp. 3159–3166, Sep. 2018.

[45] D. Jin, Z. Li, C. Hannon, C. Chen, J. Wang, M. Shahidehpour, and C. W. Lee, “Toward a cyber resilient and secure microgrid using software-defined networking,” IEEE Trans. Smart Grid, vol. 8, no. 5, pp. 2494–2504, Sep. 2017.

[46] Y. Cao and Y. Sun, “Consensus of discrete-time third-order multi-agent systems in directed networks,” Neurocomputing, vol. 177, pp. 394–400, Feb. 2016.

[47] Y. Cao, Y. Sun, and X.-J. Xie, “Explicit condition for consensus of third-order discrete-time multi-agent systems without accelerated velocity measurements,” J. Franklin Inst., vol. 354, no. 12, pp. 5056–5066, Aug. 2017.

[48] Y. Liu, H. Gao, C. Zhai, and W. Xie, “Internal stability and string stability of connected vehicle systems with time delays,” IEEE Trans. Intell. Transp. Syst., early access, May 4, 2020, doi: 10.1109/TITS.2020.2988401.

[49] Y. Zheng, S. E. Li, K. Li, and L.-Y. Wang, “Stability margin improvement of vehicular platoon considering undirected topology and asymmetric control,” IEEE Trans. Control Syst. Technol., vol. 24, no. 4, pp. 1253–1265, Jul. 2016.

[50] A. Barraud, “A numerical algorithm to solve $A^T X A − X = Q$,” IEEE Trans. Autom. Control, vol. 22, no. 5, pp. 883–885, Oct. 1977.

ZEMING LI is currently pursuing the B.E. degree in mechanical engineering with the School of Mechanical and Automotive Engineering, South China University of Technology, Guangzhou, China. His current research interests include autonomous vehicle control, robust control, and sensor networks.

ZIYUAN LI received the B.S. degree in automatic science and engineering from the South China University of Technology, in 2017. He is currently pursuing the master’s degree with the Key Laboratory of Autonomous Systems and Network Control, Ministry of Education, College of Automatic Science and Engineering, SCUT, Guangzhou, China. His main research interests include autonomous vehicle control, cooperative control, network security control, and consensus of stochastic systems.

YONGGUI LIU (Member, IEEE) received the B.S. degree in electronic information engineering from the Hunan University of Technology, in 2001, the M.S. degree from School of Electronic and Information Engineering, South China University of Technology (SCUT), Guangzhou, China, and the Ph.D. degree from the College of Automation Science and Engineering, SCUT, in 2011. He worked as a Postdoctoral Fellow with the Shenzhen Research Institute, Chinese University of Hong Kong, from September 2012 to August 2014. He is currently an Associate Professor and working with the Key Laboratory of Autonomous Systems and Network Control, Ministry of Education, College of Automatic Science and Engineering, SCUT. His main research interests include autonomous vehicle control, cooperative control, and networked control systems.