IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 26 January 2024, accepted 28 February 2024, date of publication 19 March 2024, date of current version 25 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3379420

RESEARCH ARTICLE

Secure Consensus Control for Connected Vehicle Systems With Resilient Predictors Against Denial-of-Service Attacks

YONGGUI LIU[1], (Member, IEEE), ZIYUAN LI[1], QINXUE LI[2], AND XUHUAN XIE[3]

[1]Key Laboratory of Autonomous Systems and Network Control, Ministry of Education, School of Automation Science and Engineering, South China University of Technology, Guangzhou 510641, China
[2]Department of Electrical Engineering, Guangzhou Maritime University, Guangzhou 510700, China
[3]School of Mechanical and Automotive Engineering, South China University of Technology, Guangzhou 510641, China

Corresponding author: Qinxue Li (liqinxue512@foxmail.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61573153 and Grant 62006052, in part by the Natural Science Foundation of Guangdong Province under Grant 2021A1515011520, and in part by Guangdong Basic and Applied Basic Research Foundation under Grant 2022A1515110148 and Grant 2023A1515012468.

ABSTRACT This paper concentrates on the secure consensus control problem for a class of second-order connected vehicle systems (CVSs) in the presence of denial-of-service (DoS) attacks. First, the necessary and sufficient conditions for the consensus of CVSs are derived in the attack-free case. Second, in order to defend against DoS attacks, we design a novel secure consensus control protocol where resilient predictors are used to estimate the states of other vehicles during DoS attacks. Then, by using Lyapunov stability theory, matrix analysis tool, and algebraic graph theory, the convergence of CVSs with the resilient predictors against DoS attacks is achieved in the attack case. It is proved that under the designed secure consensus control protocol with resilient predictors, not only the prediction errors can be converged to a bounded range, but also the system errors can be converged. Finally, the effectiveness of the proposed novel secure consensus control protocol with resilient predictors is illustrated by some simulation results.

INDEX TERMS Connected vehicle systems (CVSs), denial-of-service (DoS) attacks, resilient predictors, secure consensus control protocol.

I. INTRODUCTION

As the application of cyber-physical systems, connected vehicle systems (CVSs) play a significant role in smart city due to its advantages in reducing traffic accidents and greenhouse gases, increasing traffic efficiency, and etc [1], [2]. In CVSs, vehicles are connected through ad-hoc networks and the control protocol is generated according to the received status information (position, velocity, etc.) of other vehicles [3]. The appropriate control protocol ensures the internal stability of CVSs, which can be implemented through cooperative adaptive cruise control (CACC) [4], [5], [6], [7]. Flocking theory [8], [9] and consensus control [10], [11], are widely adopted to implement CACC for CVSs. While in the consensus control method, vehicles exchange their state information with each other and eventually reach consensus [12]. In particular, the ‘‘look-ahead’’ type network topology (a vehicle receives the information from its ahead vehicle through wireless communication or the sensors placed in front of the vehicle) has gained increasingly interests in the consensus control for CVSs, please see e.g. [13], [14], [15], and [16] and the references therein.

Since data is exchanged between vehicles through wireless networks, cyber-attacks are one of the most critical factors that affect the stability and security of CVSs. Many cyber-attacks are designed by attackers, exploiting loopholes and security flaws to the attacked systems and endanger communication security. In recent years, cyber security incidents occur frequently all over the world, which show that cyber-attacks are becoming a critical threat and urgently

The associate editor coordinating the review of this manuscript and approving it for publication was Jiefeng Hu.

necessary to be solved. To name a few, in 2010, a replay attack virus named StuxNet used the loophole of industrial control system to invade the nuclear power plant in Iran, which resulted in the abandonment of 1/5 centrifuges [17]. In 2015, security researchers Charlie Miller and Chris Valasek showed that they can remotely hack into the Cherokee Jeep from Miller's basement to disable the brakes, take control over the steering wheel, and finally send the vehicle into a ditch. This cyber-carjacking incident caused the recall of 1.4 million cars [18]. From the perspective of real-world engineering, three typical cyber-attacks are disclosed: deception attacks [19], [20], [21], replay attacks [22], [23], [24], and denial-of-service (DoS) attacks [25], [26], [27]. In DoS attacks, the attackers generate several useless data or/and repeatedly send aggressive service requests, which make the target unable to receive and respond to external requests in a timely manner.

It is one of critical challenges for CVSs to design consensus control protocols to defend against DoS attacks, which has been received extensive attention in the open literature [28], [29], [30], [31]. In [28], the platoon control problem for CVSs suffering from DoS attacks and multiple disturbances is studied. A resilient platoon control protocol is proposed to achieve internal stability of CVSs and minimize the disturbance propagation bound. In [29], the authors investigate the distributed secure platoon control for a class of CVSs where the DoS attacks may occur at some time-varying sampling time instant. The distributed control strategy can ensure the exponential tracking performance, and the several quantitative relationships between attack parameters and system performance are revealed. Moreover, based on the idea of adaptive control, the distributed secure adaptive platoon control for CVSs in the presence of intermittent DoS attacks is further investigated in [30]. The proposed protocol can guarantee that the vehicle state estimation errors and platoon tracking errors can be regulated to reside in small neighborhoods around zero. In order to resist DoS attacks, using event-triggered method to reduce network traffic in communication channel is a possible solution. However, it is noteworthy that the event-triggered method reduces network traffic in communication channel, but the real-time performance is compromised, especially when the triggered data is lost during the active period of DoS attacks. As a consequence, the event-triggered method may not be the best solution for the CVSs which needs a lot of real-time information. For this reason, in [31], the authors develop a resilient consensus control scheme for CVSs equipped with CACC to mitigate the DoS attacks, a set of resilient predictors are designed via sliding mode theory and adaptive observer theory. Using the resilient predictor to estimate the states of other vehicles during DoS attacks is a promising way. However, in [31], the authors only investigate the convergence of the prediction errors of the resilient predictors, but the convergence of system error is not considered. The above observations motivate the research presented in this paper.

In this paper, the problem of secure consensus control for a class of second-order CVSs in the presence of DoS attacks is investigated. The main contributions can be highlighted as follows:

1) A novel secure consensus control protocol with resilient predictors is developed for the CVSs subject to DoS attacks, where the resilient predictors are added to the controller of each vehicle to estimate the states of other vehicles during DoS attacks.
2) The necessary and sufficient conditions for the consensus of CVSs are derived in the attack-free case, and the convergence of CVSs with predictors against DoS attacks is further achieved in the attack case.
3) Different from [31], under the designed secure consensus control protocol with resilient predictors, not only the prediction errors can converge to a bounded range, but the system errors can also converge.

The rest of this paper is organized as follows. In Section II, the models of CVSs and DoS attacks are introduced, and the secure consensus control protocol with resilient predictors is designed. In Section III, some important results are derived. Simulations are given in Section IV to verify the proposed strategy, and conclusions are drawn in Section V.

Notations: Notation $P = P^T > 0$ (≥ 0) means that the matrix P is real symmetric positive definite (semi-definite). Let $\mathbb{R}$ denotes the set of real numbers, and $\mathbb{R}^+$ denotes the set of positive reals. Let $Re(x)$ denotes the real part of the complex number x. Let I_n and 0_n denote the $n \times n$ identity matrix and $n \times n$ zero matrix, respectively. The 2-norm of a vector x is denoted as $\|x\|$. And $a_{i,j}$ $(i, j = 1, \dots, n)$ denote the elements of adjacency matrix of the graph, which take the value of 1 when there is a communication link from j to i and take the value of 0 otherwise. Let $L = \{l_{i,j}\}$ $(i, j = 1, \dots, n)$ denote the Laplacian matrix of the corresponding graph, where $l_{i,i} = \sum_{k=1,k\neq i}^{n} a_{i,k}$ and $l_{i,j} = -a_{i,j}$, $i \neq j$. A^T and A^{-1} denote the transpose and inverse of matrix A, respectively. For brevity, we write symmetric matrices of the form $\begin{bmatrix} A & B \\ B^T & C \end{bmatrix}$ as $\begin{bmatrix} A & B \\ * & C \end{bmatrix}$. Matrices, if not explicitly stated, are assumed to have compatible dimensions.

II. PROBLEM FORMULATION

A. CVSS MODELING

As shown in Fig. 1, this paper considers a platoon includes one lead vehicle and n followers, where the classical predecessor following (PF) network topology is used [6]. Each follower has the following second-order dynamics:

$$\begin{cases} \dot{p}_i(t) = v_i(t) \\ \dot{v}_i(t) = u_i(t), \end{cases} \tag{1}$$

where, $i = 1, 2, \cdots, n$; $p_i(t)$, $v_i(t)$ and $u_i(t)$ are position, velocity and control input of the vehicle i at time t, respectively.

The control objectives of the platoon are to achieve asymptotical stability of CVSs, which can be described: as time goes to infinite

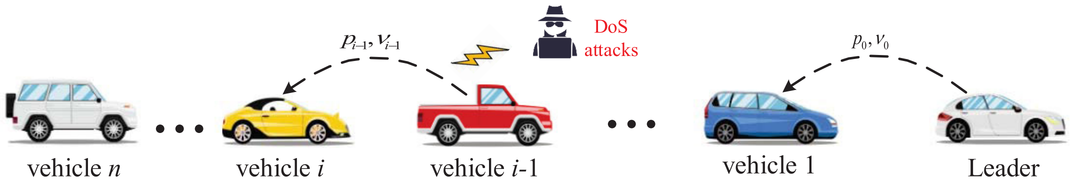


FIGURE 1. CVSs based on the PF network topology.

1) The longitudinal spacing between two adjacent vehicles is the same;
2) All followers track the lead vehicle with the same velocity.

The above control objectives are described as

$$\begin{cases} \lim_{t\to\infty} p_i(t) \to p_i^*(t) = p_0(t) + id \\ \lim_{t\to\infty} v_i(t) \to v_i^*(t) = v_0(t), \end{cases} \tag{2}$$

where $p_i^*(t)$ and $v_i^*(t)$ are the desired position and velocity of vehicle i at time t, respectively; d is the desired distance between adjacent vehicles and $d \geq d_{min}$, where d_{min} is the minimum safety distance between neighbor vehicles; $p_0(t)$ and $v_0(t)$ are the position and velocity of the lead vehicle.

In order to achieve the control objectives, letting $\bar{p}_i = p_i - p_i^*$ and $\bar{v}_i = v_i - v_i^*$, for each vehicle i $(i = 1, 2, \cdots, n)$, the following cooperative control protocol is designed:

$$u_i = -k_1(\bar{p}_i - \bar{p}_{i-1}) - k_2(\bar{v}_i - \bar{v}_{i-1}), \tag{3}$$

where k_1 and k_2 are the control parameters to be designed.

Let $x_i(t) = \left[\bar{p}_i^T(t), \bar{v}_i^T(t)\right]^T$, then vehicle i has the following dynamics:

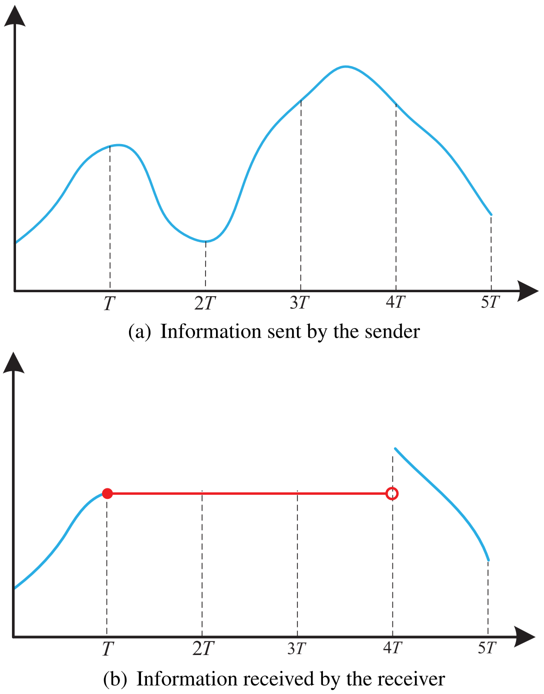
$$\dot{x}_i(t) = Ax_i(t) + Bx_{i-1}(t), \tag{4}$$

where $A = \begin{bmatrix} 0 & 1 \\ -k_1 & -k_2 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 0 \\ k_1 & k_2 \end{bmatrix}$.

B. MODELING OF DOS ATTACKS

We regard the DoS attacks as the phenomenon that prevents the information of vehicles from being transmitted at each desired time. During the DoS attacks, vehicle $i, (i = 1, 2, \ldots, n)$ is not able to receive the information from the vehicle $i - 1$. The vehicles keep the previous information of the moment before DoS attacks [31], [33]. Therefore, the DoS attacks can be modeled as a stochastic delay τ in data transmission via the network [31], [32]. Based on the fact that an attacker has the nature of concealment and limited energy, one has $\tau < \tau max$, where τmax denotes the maximum delay can be caused by DoS attacks.

Fig. 2 shows the difference between the information sent by the sender vehicle and the information received by the receiver vehicle when DoS attacks occur. The DoS attacks occur at T and end at $4T$. We can see that during the duration of DoS attacks, the sender's real-time information cannot be received by the receiver and the receiver can only hold the information at the moment before the DoS attacks occur. In addition, since CVSs share the same communication network, we assume that τmax caused by the DoS attacks is the same for each vehicle. Moreover, it is reasonable for τmax to be limited, this is in line with practical engineering.



(a) Information sent by the sender

(b) Information received by the receiver

FIGURE 2. Information update under DoS attacks.

C. DESIGN OF SECURE CONTROLLER WITH RESILIENT PREDICTORS AGAINST DOS ATTACKS

To deal with the problem that vehicle can not receive the state information of the vehicles in front of it during the DoS attacks. We add the resilient predictors in the controller of vehicle i to predict the state information of the vehicles in front of it. In the absence of DoS attacks, the controller generates control signals according to the original control protocol (3). In this case, vehicle i has the dynamics in (4).

When the controller detects a DoS attack, the controller uses the information of the resilient predictors. Let $\hat{p}_i$ and $\hat{v}_i$ denote the predictions of p_i, v_i, respectively. In this case, from (3), the control protocol of vehicle i is:

$$u_i(t) = -k_1(\bar{p}_i(t) - \hat{\bar{p}}_{i-1}(t)) - k_2(\bar{v}_i(t) - \hat{\bar{v}}_{i-1}(t)) \tag{5}$$

where $\hat{\bar{p}}_{i-1} = \hat{p}_{i-1} - p^*_{i-1}$ and $\hat{\bar{v}}_{i-1} = \hat{v}_{i-1} - v^*_{i-1}$.

Vehicle i has the following dynamics:

$$\dot{x}_i(t) = Ax_i(t) + B\hat{x}_{i-1}(t) + E(t), \tag{6}$$

where $\hat{x}_i(t) = \left[\hat{p}_i^T(t), \hat{v}_i^T(t)\right]^T$, $E(t)$ represents the errors that may be introduced due to noise disturbances or other uncertainties. Suppose $\|E(t)\|_\infty < E_{\max}$, where $E_{\max}$ is a constant.

The update rules of resilient predictors are designed as follows:

$$\dot{\hat{x}}_{i-1}(t) = A\hat{x}_{i-1}(t) + B\hat{x}_{i-2}(t) + H\tilde{x}_{i-1}(t-\tau), \tag{7}$$

where $\tilde{x}_i(t) = x_i(t) - \hat{x}_i(t)$ denotes the prediction error, H is the gain matrix, and τ $(\tau \le \tau_{max})$ is the time delay caused by DoS attacks, which can be calculated by setting a timer.

III. MAIN RESULTS

It is desired that the CVSs should be stable in the attack-free case, which is a foundation for deriving stability conditions in the attack case. Therefore, in the following analysis, we first study the stability of CVSs without DoS attacks, then based on the modeling analysis method of time-delay system, Lyapunov stability theory and estimation method, we investigate the convergence of CVSs in presence of DoS attacks.

A. CONVERGENCE ANALYSIS IN ABSENCE OF DOS ATTACKS

Lemma 1: The CVSs (1) with the control protocol (3) are stable and meet the control objectives (2) if and only if $k_1 > 0$ and $k_2 > 0$.

Proof: Let $\bar{p} = [\bar{p}_1, \bar{p}_2, \cdots, \bar{p}_n]^T$, $\bar{v} = [\bar{v}_1, \bar{v}_2, \cdots, \bar{v}_n]^T$ and $e = [\bar{p}^T, \bar{v}^T]^T$. Combining (1) and (3), the dynamic equation of the system error can be obtained as

$$\dot{e} = Ce, \tag{8}$$

where

$$C = \begin{bmatrix} 0_n & I_n \\ -k_1 L & -k_2 L \end{bmatrix},$$

and

$$L = \begin{bmatrix} 1 & & & \\ -1 & 1 & & \\ & \ddots & \ddots & \\ & & -1 & 1 \end{bmatrix}.$$

L is a variant of the Laplacian matrix of the vehicle platoon due to the lack of state of leader vehicle in e. It is easy to derive $\lambda_i = 1$ $(i = 1, 2, \ldots, n)$, where λ_i is the ith eigenvalue of L.

Let α be the eigenvalue of the matrix C, one can derive that

$$\begin{aligned} &\det(\alpha I_{2n} - C) \\ &= \det\left(\begin{bmatrix} \alpha I_n & -I_n \\ k_1 L & \alpha I_n + k_2 L \end{bmatrix}\right) \\ &= \det\left(\alpha^2 I_n + (k_2\alpha + k_1)L\right) \\ &= \prod_{i=0}^{n}[\alpha^2 + (k_2\alpha + k_1)\lambda_i]. \end{aligned} \tag{9}$$

Let the characteristic equation $\det(\alpha I_{2n} - C) = 0$, one has

$$\alpha^2 + (k_2\alpha + k_1)\lambda_i = 0. \tag{10}$$

Solving the equation (10), one obtains

$$\alpha_{i,j} = \frac{-k_2\lambda_i \pm \sqrt{k_2^2\lambda_i^2 - 4k_1\lambda_i}}{2}, \tag{11}$$

where $i = 1, 2, \cdots, n; j = 1, 2$.

The vehicle platoon is stable if and only if $Re(\alpha_{i,j}) < 0$. According to (11), when $k_2^2 \ge 4k_1$, one has $k_1 > 0$; when $k_2^2 < 4k_1$, one has $k_2 > 0$. Therefore, $k_1 > 0$ and $k_2 > 0$ can ensure that the $\alpha_{i,j}$ has two complex roots with negative real parts. The proof is completed. ■

In the following section, we first study the convergence of the prediction error.

B. CONVERGENCE ANALYSIS OF THE PREDICTION ERROR IN PRESENCE OF DOS ATTACKS

During DoS attacks, vehicle $i-1$ has the following dynamics:

$$\dot{x}_{i-1}(t) = Ax_{i-1}(t) + B\hat{x}_{i-2}(t) + E(t). \tag{12}$$

Subtracting (7) from (12), one has:

$$\dot{\tilde{x}}_i(t) = A\tilde{x}_i(t) - H\tilde{x}_i(t-\tau) + E(t). \tag{13}$$

Next, we introduce a lemma to ensure that the prediction error described in (13) is converged to a bounded range.

Lemma 2: If there exist matrices A and H such that the following matrix inequality holds:

$$\Phi = \begin{bmatrix} \phi_{11} & \phi_{12} & \mathbf{0}_2 & \phi_{13} & P_2^T \\ * & \phi_{22} & \mathbf{0}_2 & -P_3^T H & P_3^T \\ * & * & \phi_{33} & -e^{-a\tau_{max}}R & 0_2 \\ * & * & * & -2e^{-a\tau_{max}}R & 0_2 \\ * & * & * & * & -bI_2 \end{bmatrix} < 0, \tag{14}$$

where, $a > 0, b > 0$, $P = P^T > 0$, $P_2 = P_2^T > 0$, $P_3 = P_3^T > 0$, $R = R^T > 0$, $S = S^T > 0$, $\phi_{11} = A^T P_2 + P_2^T A + aP + S - e^{-a\tau_{max}}R$, $\phi_{12} = P - P_2^T + A^T P_3$, $\phi_{13} = e^{-a\tau_{max}}R - P_2^T H$, $\phi_{22} = \tau_{max}^2 R - P_3 - P_3^T$ and $\phi_{33} = -e^{-a\tau_{max}}(R + S)$,
then the prediction error described in (13) satisfies:

$$\|\tilde{x}_i(t)\|^2 < \lambda_{\min}^{-1}(P)\Big[e^{-at}\tilde{x}_{i0}^T P\tilde{x}_{i0} + (1 - e^{-at})\frac{b}{a}\|E_{\max}\|^2\Big], \tag{15}$$

where $\tilde{x}_{i0} = \tilde{x}_i(0)$ represents the initial value of the prediction error.

Proof: Take the Lyapunov-krasovskii functional as:

$$V(\tilde{x}_i, \dot{\tilde{x}}_i) = \tilde{x}_i^T(t)P\tilde{x}_i(t) + \int_{t-\tau_{max}}^{t} e^{a(s-t)}\tilde{x}_i^T(s)S\tilde{x}_i(s)ds + \tau_{\max}\int_{-\tau_{\max}}^{0}\int_{t+\theta}^{t} e^{a(s-t)}\dot{\tilde{x}}_i^T(s)R\dot{\tilde{x}}_i(s)dsd\theta. \tag{16}$$

Let $W \triangleq aV - b\|E(t)\|^2 + \dot{V}$. According to the comparison principle [34], if $W < 0$, then one has:

$$\tilde{x}_i^T(t)P\tilde{x}_i(t) \le V(\tilde{x}_i, \dot{\tilde{x}}_i) < e^{-at}V(\tilde{x}_{i0}, \dot{\tilde{x}}_{i0}) + \int_0^t e^{-a(t-s)}b\|E(s)\|^2 ds. \tag{17}$$

Combing $\lambda_{min}(P)\|\tilde{x}_i(t)\|^2 \le \tilde{x}_i^T(t)P\tilde{x}_i(t)$, equation (15) can be derived.

In the following, we show how to calculate W. First, we calculate the derivative of Lyapunov-krasovskii functional (16). In order to make the process clear, we divide the function into three parts. Let $V_1 = \tilde{x}_i^T(t)P\tilde{x}_i(t)$, $V_2 = \int_{t-\tau_{max}}^{t} e^{a(s-t)}\tilde{x}_i^T(s)S\tilde{x}_i(s)ds$ and $V_3 = \tau_{\max}\int_{-\tau_{\max}}^{0}\int_{t+\theta}^{t} e^{a(s-t)}\dot{\tilde{x}}_i^T(s)R\dot{\tilde{x}}_i(s)dsd\theta$. Taking differential for them, one has:

$$\dot{V}_1 = 2\tilde{x}_i^T(t)P\dot{\tilde{x}}_i(t). \tag{18}$$

$$\begin{aligned}\dot{V}_2 &= \frac{\partial}{\partial t}\left(e^{-at}\int_{t-\tau_{max}}^{t} e^{as}\tilde{x}_i^T(s)S\tilde{x}_i(s)ds\right)\\ &= -ae^{-at}\int_{t-\tau_{max}}^{t} e^{as}\tilde{x}_i^T(s)S\tilde{x}_i(s)ds + \tilde{x}_i^T(t)S\tilde{x}_i(t)\\ &\quad + e^{-a\tau_{max}}\tilde{x}_i^T(t-\tau_{max})S\tilde{x}_i(t-\tau_{max}).\end{aligned} \tag{19}$$

$$\begin{aligned}\dot{V}_3 = &\ \tau_{\max}\int_{-\tau_{\max}}^{0}\frac{\partial}{\partial t}\left(e^{-at}\int_{t+\theta}^{t} e^{as}\dot{\tilde{x}}_i^T(s)R\dot{\tilde{x}}_i(s)ds\right)d\theta\\ &= \tau_{\max}\int_{-\tau_{\max}}^{0}\Bigg(-ae^{-at}\int_{t+\theta}^{t} e^{as}\dot{\tilde{x}}_i^T(s)R\dot{\tilde{x}}_i(s)ds\\ &\quad + \dot{\tilde{x}}_i^T(t)R\dot{\tilde{x}}_i(t) - e^{-a\theta}\dot{\tilde{x}}_i^T(t+\theta)R\dot{\tilde{x}}_i(t+\theta)\Bigg)d\theta\\ &= -a\tau_{\max}\int_{-\tau_{\max}}^{0}\int_{t+\theta}^{t} e^{a(s-t)}\dot{\tilde{x}}_i^T(s)R\dot{\tilde{x}}_i(s)dsd\theta\\ &\quad + \tau_{\max}^2\dot{\tilde{x}}_i^T(t)R\dot{\tilde{x}}_i(t)\\ &\quad - \tau_{\max}\int_{t-\tau_{\max}}^{t} e^{-a(s-t)}\dot{\tilde{x}}_i^T(s)R\dot{\tilde{x}}_i(s)ds.\end{aligned} \tag{20}$$

Then a combination of (18)–(20), and recalling the definition of W [35], one can derive that:

$$W \le \eta^T(t)\Phi\eta(t) \le 0, \tag{21}$$

where $\eta^T(t) = [\tilde{x}_i^T(t), \dot{\tilde{x}}_i^T(t), \tilde{x}_i^T(t-\tau_{\max}), \tilde{x}_i^T(t-\tau), E^T(t)]$.

If $\Phi < 0$, then $W < 0$, which implies that (15) holds. The proof is completed. ■

Remark 1: According to Lemma 2, if matrixes A and H satisfy the requirements of the matrix inequality in (14), then the prediction error meets (15). Especially, when time goes to infinity, one has $\|\tilde{x}\|^2 < \lambda_{\min}^{-1}(P)\frac{b}{a}\|E_{\max}\|^2$. It means that the prediction error can converge to a bounded range related to the error caused by noise interference. Furthermore, when the delay estimation is accurate and there is no noise disturbance, the prediction error can converge to 0.

So far, we have proved that when DoS attacks occur, the prediction error is bounded. Can the CVSs be stable with this kind of bounded prediction error? We will give the answer in the next section.

C. STABILITY ANALYSIS OF THE CVSS IN PRESENCE OF DOS ATTACKS

Combined with the equations (1), (6) and (7), one can derive dynamics of the system error is as follows:

$$\dot{X} = CX + D\tilde{X}, \tag{22}$$

where $X = [\bar{p}^T, \bar{v}^T]^T$, $\tilde{X} = [\tilde{p}^T, \tilde{v}^T]^T$, $\tilde{p} = [\tilde{p}_1, \tilde{p}_2, \cdots, \tilde{p}_n]^T$, $\tilde{v} = [\tilde{v}_1, \tilde{v}_2, \cdots, \tilde{v}_n]^T$ and

$$D = \begin{bmatrix} \mathbf{0}_n & \mathbf{0}_n \\ -k_1(L - I_n) & -k_2(L - I_n) \end{bmatrix}.$$

First, we introduce the definition of being input-to-state stable (ISS).

Definition 1: System (22) is said to be ISS if there exist a $\mathcal{KL}$ function β and a $\mathcal{K}_\infty$ function γ such that for each $\omega_t \in \mathcal{L}_\infty(\mathbb{R}^+)$ and $x_i(0) \in \mathbb{R}^n$, the following inequality

$$\|x_i(t)\| \le \beta(\|x_i(0)\|, t) + \gamma(\|\omega_t\|_\infty) \tag{23}$$

holds for all $t \in \mathbb{R}^+$.

It can be learned from Lemma 2 that the prediction error of resilient predictors is always bounded. Let the bound be $\tilde{M}$, one has $\|\tilde{x}_i(t)\|^2 < \tilde{M}$. Then, we can obtain the following theorem:

Theorem 1: If there exist matrices A and H satisfying (14), the CVSs (22) with control protocol (5) and resilient predictors (7) under DoS attacks are ISS. Especially, when the prediction error is 0, the CVSs (22) are globally asymptotically stable (GAS).

Proof: Choose the Lyapunov function $V(X) = X^T\tilde{P}X$, then one has:

$$\alpha_1\|X(t)\|^2 \le V(X(t)) \le \alpha_2\|X(t)\|^2, \tag{24}$$

where, α_1 and α_2 are the minimum and maximum eigenvalues of $\tilde{P}$, respectively.

Then the derivation of Lyapunov function can be obtained:

$$\begin{aligned}\dot{V} &= X^T(\tilde{P} + \tilde{P}^T)(CX + D\tilde{X})\\ &= -X^TQX + 2X^T\tilde{P}D\tilde{X}\\ &\le -\gamma_1\|X\|^2 + \gamma_2\|X\|\|\tilde{X}\|,\end{aligned} \tag{25}$$

where Q is the solution of Lyapunov equation $C^T\tilde{P} + \tilde{P}C + Q = 0$, γ_1 is the minimum eigenvalue of Q and $\gamma_2 = 2\|\tilde{P}D\|$.

According to Young's inequality [36], for any positive real δ, one has:

$$2\|X\|\|\tilde{X}\| \le \frac{1}{\delta}\|X\|^2 + \delta\|\tilde{X}\|^2. \tag{26}$$

Let $\delta = \frac{\gamma_2}{\gamma_1}$ and combine with (25) and (26), one has:

$$\begin{aligned}\dot{V} &\leq (-\gamma_1 + \frac{\gamma_1}{2})\|X\|^2 + \frac{\gamma_2^2}{2\gamma_1}\|\tilde{X}\|^2 \\ &\leq -\omega_1 V + \gamma_3\|\tilde{X}\|^2, \end{aligned} \tag{27}$$

where $\omega_1 = \frac{\gamma_1}{2\alpha_2}$ and $\gamma_3 = \frac{\gamma_2^2}{2\gamma_1}$.

According to the comparison principle, one derives:

$$V \leq e^{-\omega_1 t} V(X_0) + \gamma_4 \tilde{M}, \tag{28}$$

where $\gamma_4 = \frac{\gamma_3}{\omega_1}$.

Combine with (24), one has:

$$\|X(t)\|^2 < \frac{\alpha_2}{\alpha_1} e^{-\omega_1 t}\|X_0\|^2 + \frac{\gamma_4}{\alpha_1}\tilde{M}. \tag{29}$$

For any positive real numbers f and g, there is $f^2 + g^2 \leq (f+g)^2$. So the above equation can transform into:

$$\|X(t)\| < \sqrt{\frac{\alpha_2}{\alpha_1}} e^{-\frac{\omega_1 t}{2}} \|X_0\| + \sqrt{\frac{\gamma_4}{\alpha_1}\tilde{M}}. \tag{30}$$

According to the Definition 1, the system (22) is ISS. And when $\tilde{M} \equiv 0$, the system (22) is GAS. This completes the proof. ■

Remark 2: So far, we have shown that the prediction error is bounded in presence of DoS attacks. Moreover, with this kind of bounded prediction error, we further have proved that the system error is still ISS, and the system is GAS when the prediction error comes to 0. Therefore, we can say that the CVSs with the resilient predictors in this paper can against DoS attacks.

Remark 3: Since the novel secure consensus control protocol developed in our paper takes both the convergence of prediction errors and system errors into account, it has advantages over the control protocol in [31] that only considers the convergence of prediction errors.

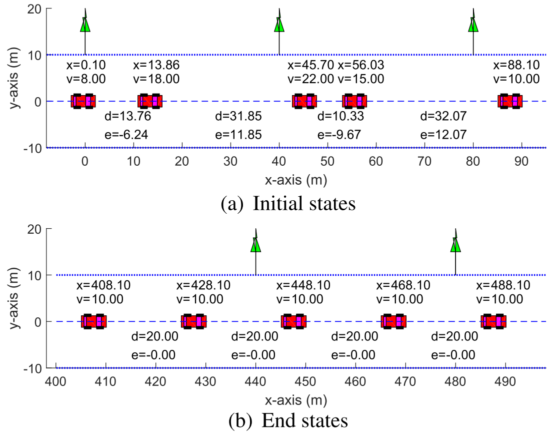
Remark 4: It can be seen from Lemma 1 and Theorem 1 that the system errors in the presence or absence of an attack are ISS and GAS, respectively. That is, 1) it can be realized that the system error in the absence of an attack is 0, and the system error in the presence of an attack is 0 only under certain circumstances; 2) a too large attack makes stability of the system error more mild.

IV. SIMULATIONS

In this section, the validity of the proposed methods is verified. Consider a vehicle platoon that includes one leader and four followers. In order to verify the convergence of proposed strategy, we conduct the following simulation research.

A. CONVERGENCE OF THE CVSS IN ABSENCE OF DOS ATTACKS

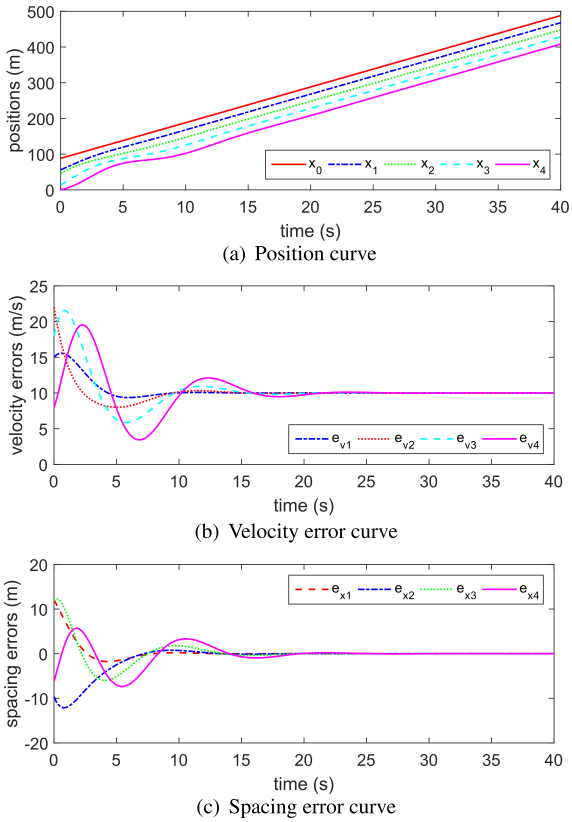
The lead vehicle runs with the constant velocity $20m/s$, while the followers start running as follows: 1) Different initial spacings selected arbitrarily based on Gauss distribution with mean of 20 and variance of 25; 2) Different velocities selected from 0m/s to 30m/s. The initial states of the CVSs are shown in Fig. 3(a). The desired spacing is set to $20m$. And for comparison, let the platoon have the same initial state in the following simulation.



(a) Initial states

(b) End states

FIGURE 3. Initial and end states of the CVSs in the absence of DoS attacks.



(a) Position curve

(b) Velocity error curve

(c) Spacing error curve

FIGURE 4. States of the CVSs in the absence of DoS attacks.

Let $k_1 = 0.5$, $k_2 = 0.8$, which meet the conditions in Lemma 1, and let CVSs run $40s$, the end states of the CVSs and the running processes are shown in Figs. 3(b) and 4, respectively.

We can see that the consensus of the platoon is reached as time goes. There is no collision during the running of

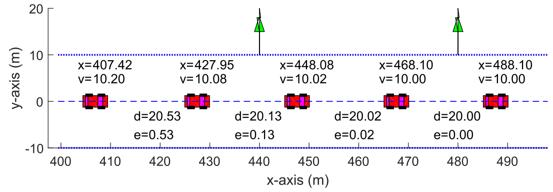
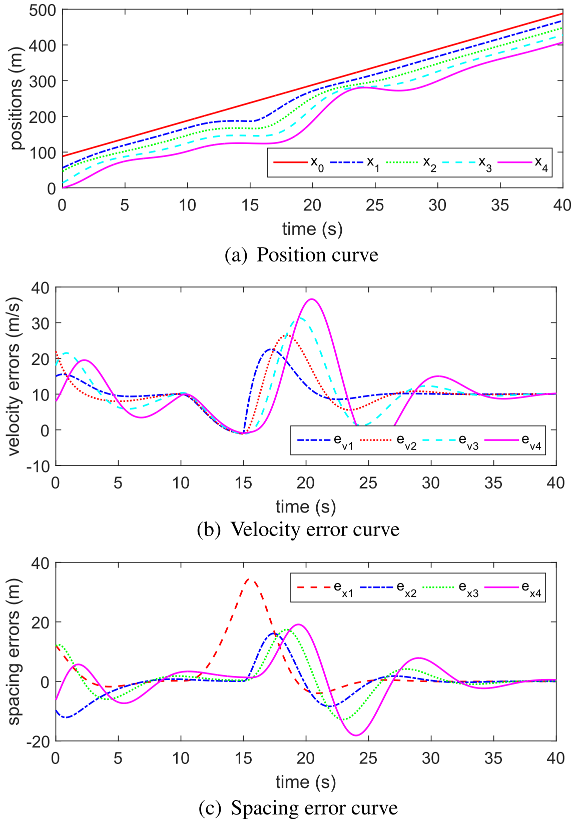


FIGURE 5. End states of the CVSs without resilient predictors in the presence of DoS attacks.



(a) Position curve

(b) Velocity error curve

(c) Spacing error curve

FIGURE 6. States of the CVSs without resilient predictors in the presence of DoS attacks.

the platoon (there is no intersection of the position curves), which can be seen in Fig. 4(a); The followers with different initial spacings and velocities reach the same velocity, and the spacing errors between adjacent vehicles converge to 0, which can be seen from Figs. 4(b) and 4(c).

B. CONVERGENCE OF THE CVSS WITHOUT RESILIENT PREDICTORS IN PRESENCE OF DOS ATTACKS

Let the CVSs have the same initial states as Fig. 3(a) and still let $k_1 = 0.5$, $k_2 = 0.8$. During the period of 10-15s, let the communication network of the CVSs be attacked by DoS attacks. The end states of the CVSs and the running processes are shown in Figs. 5 and 6, respectively.

It can be seen from Fig. 6(a) that the CVSs basically reached convergence at the end of the simulation, but vehicles 3 and 4 collided at about 23s. From Figs. 6(b) and 6(c), it can be seen that the maximum speed error and the maximum spacing error reached the 38 m/s and 36 m, respectively. As a consequence, compared with the convergence of the CVSs in Section IV-A, it is not difficult to find that the DoS attacks can greatly destroy the convergence of the CVSs.

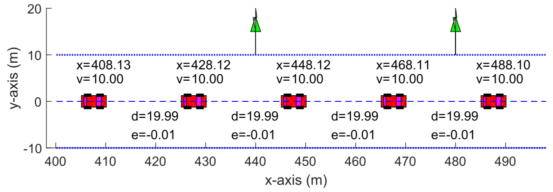
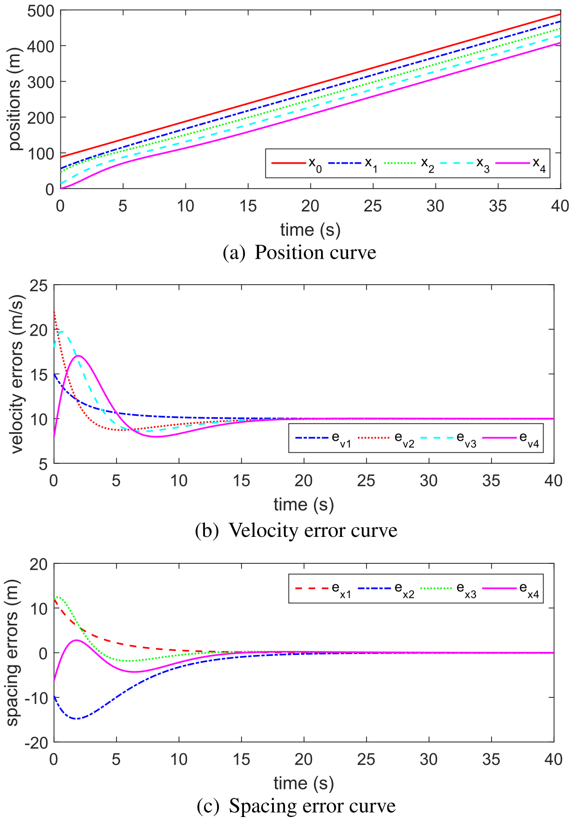


FIGURE 7. End states of the CVSs with resilient predictors in the presence of DoS attacks.



(a) Position curve

(b) Velocity error curve

(c) Spacing error curve

FIGURE 8. States of the CVSs with resilient predictors in the presence of DoS attacks.

C. CONVERGENCE OF THE CVSS WITH RESILIENT PREDICTORS IN PRESENCE OF DOS ATTACKS

Different from the simulation in Section IV-B, the resilient predictors are added to the controller of each vehicle. The $k_1 = 0.2$, $k_2 = 1$, $H = I_2$ are selected under that the requirements in Lemma 2 are satisfied. Let the CVSs run 40s, the end states of the CVSs and the running processes are shown in Figs. 7 and 8, respectively.

Fig. 8 shows that the platoon can reach consensus with both spacing errors and velocity errors converging to zero quickly and no collision occurs. Compared with the results in

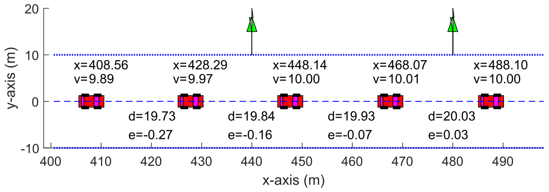
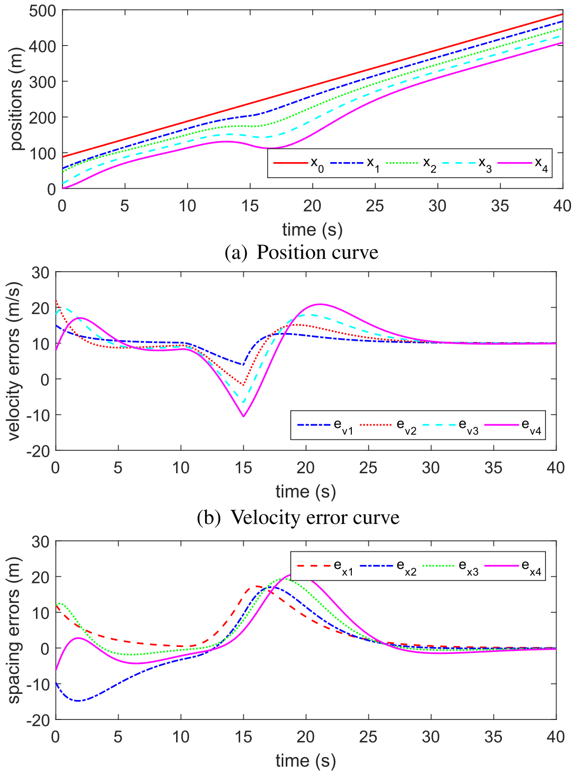


FIGURE 9. End states of the CVSs with resilient predictors in the presence of DoS attacks: the case that estimated delay error is 1ms.



(a) Position curve

(b) Velocity error curve

(c) Spacing error curve

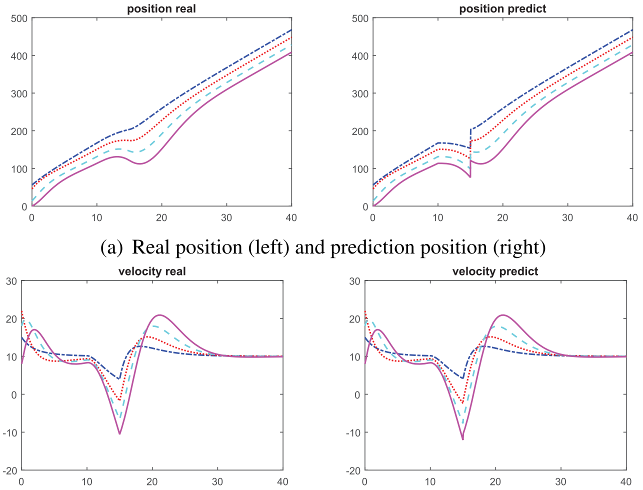
FIGURE 10. States of the CVSs with resilient predictors in the presence of DoS attacks: the case that estimated delay error is 1ms.

Section IV-B, we can find that DoS attacks have little impact on the proposed method.

D. CONVERGENCE OF THE CVSS WITH RESILIENT PREDICTORS IN PRESENCE OF DOS ATTACKS: THE CASE OF INACCURATE DELAY ESTIMATION

Since the actual CVSs have discrete sampling interval, they may cause that a slight error between the time that the CVSs detect the occurrence of DoS attacks and the time that DoS attacks actually occur. For this reason, based on the parameters designed in Section IV-C, we conduct the simulation study that the CVSs have an error of 1ms in the calculation of time delay. The end status and running processes are shown in Figs. 9 and 10, respectively.

From Fig. 9, it can be concluded that the convergence of CVSs is basically reached at the end of simulation. From Figs. 10(a)-10(c), it is clear that during the DoS attacks, the prediction for the actual states of the CVSs is poor due to the error with regarding to the delay calculation. Furthermore, the comparison between the real position and the prediction position in Fig. 11 shows that if the error with regarding to the delay calculation is not estimated accurately, then the prediction position will deviate from the real position considerably. This causes collision between vehicles. As a consequence, compared with the simulation results in Section IV-C, it is important to accurately estimate the time delay.



(a) Real position (left) and prediction position (right)

(b) Real speed (left) and prediction speed (right)

FIGURE 11. Comparison of the real states and prediction states of the CVSs: the case that estimated delay error is 1ms.

V. CONCLUSION

In this paper, we investigated the secure consensus control problem of the second-order CVSs in presence of DoS attacks. The conditions of stability of CVSs were first derived in the attack-free case. To resist DoS attacks, the resilient predictors were added into the original CVSs, and the corresponding conditions were found so that the prediction errors converge to a certain bound. Based on these, we further investigated the consensus of the overall system under DoS attacks. It shows that under the designed secure consensus control protocol with resilient predictors, not only the prediction errors can be converged to a bounded range, but also the system errors can be converged. In the future, the high-order systems with interaction network against cyber-attacks will be further investigated.

REFERENCES

[1] 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.

[2] M. Li, Z. Cao, and Z. Li, "A reinforcement learning-based vehicle platoon control strategy for reducing energy consumption in traffic oscillations," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 32, no. 12, pp. 5309–5322, Dec. 2021.

[3] H.-X. Hu, B. Tang, Y. Zhang, and W. Wang, "Vehicular ad hoc network representation learning for recommendations in Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 4, pp. 2583–2591, Apr. 2020.

[4] 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 (CACC)," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 2, pp. 491–509, Feb. 2016.

[5] 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.*, vol. 22, no. 10, pp. 6162–6174, Oct. 2021.

[6] Y. Liu and H. Gao, "Stability, scalability, speedability, and string stability of connected vehicle systems," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 52, no. 5, pp. 2819–2832, May 2022.

[7] Z. Shen, Y. Liu, Z. Li, and M. H. Nabin, "Cooperative spacing sampled control of vehicle platoon considering undirected topology and analog fading networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 10, pp. 18478–18491, Oct. 2022.

[8] F. Wang and Y. Chen, "A novel hierarchical flocking control framework for connected and automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 4801–4812, Aug. 2021.

[9] L. E. Beaver and A. A. Malikopoulos, "An overview on optimal flocking," *Annu. Rev. Control*, vol. 51, pp. 88–99, Jan. 2021.

[10] B. Wang and R. Su, "A distributed platoon control framework for connected automated vehicles in an urban traffic network," *IEEE Trans. Control Netw. Syst.*, vol. 9, no. 4, pp. 1717–1730, Dec. 2022.

[11] Z. Zhang, W. Yan, H. Li, and L. Li, "Consensus control of linear systems with optimal performance on directed topologies," *J. Franklin Inst.*, vol. 357, no. 4, pp. 2185–2202, Mar. 2020.

[12] 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.

[13] T. Liu, X. Hu, S. E. Li, and D. Cao, "Reinforcement learning optimized look-ahead energy management of a parallel hybrid electric vehicle," *IEEE/ASME Trans. Mechatronics*, vol. 22, no. 4, pp. 1497–1507, Aug. 2017.

[14] M. A. S. Kamal, K. Hashikura, T. Hayakawa, K. Yamada, and J.-I. Imura, "Look-ahead driving schemes for efficient control of automated vehicles on urban roads," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 1280–1292, Feb. 2022.

[15] C. Zhai, Y. Liu, and F. Luo, "A switched control strategy of heterogeneous vehicle platoon for multiple objectives with state constraints," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 5, pp. 1883–1896, May 2019.

[16] 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.

[17] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, Jan. 2011.

[18] M. H. Eiza and Q. Ni, "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity," *IEEE Veh. Technol. Mag.*, vol. 12, no. 2, pp. 45–51, Jun. 2017.

[19] L. Li, H. Yang, Y. Xia, and C. Zhu, "Attack detection and distributed filtering for state-saturated systems under deception attack," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 4, pp. 1918–1929, Dec. 2021.

[20] A. Kazemy, J. Lam, and X.-M. Zhang, "Event-triggered output feedback synchronization of master–slave neural networks under deception attacks," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 33, no. 3, pp. 952–961, Mar. 2022.

[21] J. Wu, C. Peng, J. Zhang, and B.-L. Zhang, "Event-triggered finite-time H_∞ filtering for networked systems under deception attacks," *J. Franklin Inst.*, vol. 357, no. 6, pp. 3792–3808, Apr. 2020.

[22] H. S. Sánchez, D. Rotondo, T. Escobet, V. Puig, J. Saludes, and J. Quevedo, "Detection of replay attacks in cyber-physical systems using a frequency-based signature," *J. Franklin Inst.*, vol. 356, no. 5, pp. 2798–2824, Mar. 2019.

[23] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Monticello, IL, USA, Sep. 2009, pp. 911–918.

[24] W. Xu, J. Kurths, G. Wen, and X. Yu, "Resilient event-triggered control strategies for second-order consensus," *IEEE Trans. Autom. Control*, vol. 67, no. 8, pp. 4226–4233, Aug. 2022.

[25] X. Xie, Y. Liu, and Q. Li, "Neural network-based adaptive event-triggered control for cyber–physical systems under resource constraints and hybrid cyberattacks," *Automatica*, vol. 152, Jun. 2023, Art. no. 110977.

[26] X. Xie, S. Hu, Y. Liu, and Q. Li, "Resilient adaptive event-triggered H_∞ fuzzy filtering for cyber-physical systems under stochastic-sampling and denial-of-service attacks," *IEEE Trans. Fuzzy Syst.*, vol. 31, no. 1, pp. 278–292, Jan. 2023.

[27] L. Zha, J. Liu, and J. Cao, "Resilient event-triggered consensus control for nonlinear muti-agent systems with DoS attacks," *J. Franklin Inst.*, vol. 356, no. 13, pp. 7071–7090, Sep. 2019.

[28] Y. Zhao, Z. Liu, and W. S. Wong, "Resilient platoon control of vehicular cyber physical systems under DoS attacks and multiple disturbances," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 10945–10956, Aug. 2022.

[29] D. Zhang, Y.-P. Shen, S.-Q. Zhou, X.-W. Dong, and L. Yu, "Distributed secure platoon control of connected vehicles subject to DoS attack: Theory and application," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 51, no. 11, pp. 7269–7278, Nov. 2021.

[30] S. Xiao, X. Ge, Q.-L. Han, and Y. Zhang, "Secure distributed adaptive platooning control of automated vehicles over vehicular ad-hoc networks under denial-of-service attacks," *IEEE Trans. Cybern.*, vol. 52, no. 11, pp. 12003–12015, Nov. 2022.

[31] Z. Abdollahi Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3893–3902, Dec. 2018.

[32] M. Long, C.-H. Wu, and J. Y. Hung, "Denial of service attacks on network-based control systems: Impact and mitigation," *IEEE Trans. Ind. Informat.*, vol. 1, no. 2, pp. 85–96, May 2005.

[33] W. B. Qin, M. M. Gomez, and G. Orosz, "Stability analysis of connected cruise control with stochastic delays," in *Proc. Amer. Control Conf.*, Portland, OR, USA, Jun. 2014, pp. 4624–4629.

[34] E. Fridman and M. Dambrine, "Control under quantization, saturation and delay: An LMI approach," *Automatica*, vol. 45, no. 10, pp. 2258–2264, Oct. 2009.

[35] E. Fridman and Y. Orlov, "Exponential stability of linear distributed parameter systems with time-varying delays," *Automatica*, vol. 45, no. 1, pp. 194–201, Jan. 2009.

[36] G. Hardy, J. Littlewood, and G. Polya, *Inequalities*. Cambridge, U.K.: Cambridge Univ. Press, 1952.

YONGGUI LIU (Member, IEEE) received the B.S. degree in electronic information engineering from Hunan University of Technology, in 2001, the M.S. degree from the School of Electronic and Information Engineering, South China University of Technology (SCUT), Guangzhou, China, in 2008, and the Ph.D. degree from the College of Automation Science and Engineering, SCUT, in 2011.

He was a Postdoctorate Fellow with Shenzhen Research Institute, The Chinese University of Hong Kong, from September 2012 to August 2014. He is currently an Associate Professor 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, networked control systems, and wireless sensor networks.

Dr. Liu is an Active Reviewer of some international journals, such as IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Vehicular Technology, IEEE Transactions on Automatic Control, IEEE Access, *IET Control Theory and Applications*, and *International Journal of Distributed Sensor Networks*.

ZIYUAN LI received the B.S. degree in automatic science and engineering from the South China University of Technology (SCUT), Guangzhou, China, in 2017, where 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.

His main research interests include autonomous vehicle control, cooperative control, network security control, and consensus of stochastic systems.

QINXUE LI received the Ph.D. degree in control theory and control engineering from the South China University of Technology, Guangzhou, China, in 2019.

She was an Associate Professor with the School of Ship and Ocean Engineering, Guangzhou Maritime University, Guangzhou. Her research interests include security of cyber physical systems, fault diagnosis, and signal processing of networked control systems.

XUHUAN XIE received the Ph.D. degree in control theory and control engineering from the South China University of Technology (SCUT), Guangzhou, China, in 2020.

He is currently a Postdoctoral Fellow with the School of Mechanical and Automotive Engineering, SCUT. His research interests include fuzzy systems and cyber security of cyber-physical systems.