Letter

Resilient Event-Triggered Control of Connected Automated Vehicles Under Cyber Attacks

Ning Zhao, Xudong Zhao, Ning Xu, and Liang Zhang

Dear Editor,

This letter contributes to designing a resilient event-triggered controller for connected automated vehicles under cyber attacks, including denial-of-service (DoS) and deception attacks. To characterize the effect of DoS attacks, the effective intervals of the attack are redivided based on the sampling period. Then, a resilient distributed event-triggering mechanism is proposed to compensate for the sabotage of DoS attacks and reduce the amount of transmitted data. Since the communication channel transmits the data only at the trigger instant, deception attacks may occur at this instant and be transmitted to each vehicle in superposition with the normal signal. Therefore, we construct stochastic models satisfying Bernoulli distribution to describe the false information injected by the attackers. Based on the above framework, an attack-resilient control strategy is proposed to resist the impact of cyber attacks. Then, sufficient conditions are established to achieve stability of vehicular platoons, and a co-design strategy regarding the control gain and triggering parameter matrices is given. Finally, the simulation results are provided to substantiate the effectiveness of the proposed method.

In recent decades, the widespread use of vehicles has put heavy pressure on transportation infrastructure, which in turn has led to a series of congestion problems and safety issues [1]. Vehicular platoon control allows autonomous vehicles to travel at a relatively safe distance and speed, which can alleviate traffic pressure and improve the carrying capacity of vehicles on the road. Since this technology can solve the traffic problems faced by modern society, the stability and the tracking performance of vehicular platoons have achieved some remarkable results [2], [3]. Guo and Yue [2] addressed sampled-based cooperative control issue of connected and automated vehicles with sensor failures. Reference [3] designed an adaptive sliding mode controller to solve platoon parametric uncertainties.

Communication between vehicles depends on network media, which makes it vulnerable to network channel congestion and cyber attacks. Since vehicle formations require large amounts of data transmission, traditional time-triggered mechanism can easily lead to network congestion. To achieve practical needs, a new trigger mechanism, namely the event-triggered mechanism, is proposed to deregulate the necessary data transmission. By designing a distributed adaptive event-triggered mechanism, an observer-based discrete-time controller was proposed to achieve all vehicles to maintain the desired asymptotic tracking performance [4]. Two typical types of cyber attacks are DoS attacks and deception attacks. In order to resist the effects of these two attacks, some existing works have designed security controllers to maintain the desired distance between autonomous vehicles. In [5], a distributed cooperative secure platooning controller was designed to ensure the platoon stability and scalability requirements for connected automated vehicles in the presence of DoS attacks. Not limited to one attack mode, [6] addressed the event-triggered security platoon control problem for second-order connected vehicle systems subject to DoS and deception attacks. However, few results solve attack-resilient sampled-data event-triggered platoon control problem. Its difficulty is that it fails to provide a unified framework for dividing the whole timeline by sampling period or attack intervals. To avoid this problem, the existing result [7] assumed that the attack start and end instants are integer multiples of the sampling period, which obviously limits the nature of the attack occurring at any one time. Solving this problem is the first research motivation of this letter. How to design control algorithms to save communication resources and resist the negative effects of multiple attacks is another research motivation.

Based on the above discussions, this letter studies the resilient event-triggered secure platoon control problem for connected automated vehicles under cyber attacks. The main contributions can be covered as: 1) Unlike the existing results [8] and [9], an attack-resilient sampled-data event-triggering control strategy is designed to resist the impact of cyber attacks and reduce the network bandwidth pressure; 2) By employing the Lyapunov functional approach and the linear matrix inequality technique, the stability conditions of the platoon error system are given, and then the controller gain and the trigger parameter matrices are presented simultaneously.

Notation: For a given matrix $\mathcal{P}$, $\mathcal{P} > 0$ (≥ 0) and $\mathcal{P} < 0$ (≤ 0) indicate that $\mathcal{P}$ is (semi-)positive definite and (semi-)negative definite. $\|\cdot\|$ denotes Euclidean norm for vectors.

Problem statement: Consider $N+1$ automated vehicles containing 1 leader marked 0 and N followers marked i. Let $q_i(t)$, $v_i(t)$ and $a_i(t)$ denote the position, velocity and acceleration of vehicle $i(\in \langle N \rangle)$. The dynamics of each vehicle can be uniformly modeled as

$$\dot{x}_i(t) = Ax_i(t) + Bu_i(t) \tag{1}$$

where $x_i(t) = [q_i(t), v_i(t), a_i(t)] \in \mathbb{R}^3$ is state vector, $u_i(t) \in \mathbb{R}$ is input vector and $u_0(t) = 0$, $A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{T} \end{bmatrix}$, $B = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{T} \end{bmatrix}$ with T being the inertial delay.

The goal of this letter is to design a resilient event-triggered controller for connected automated vehicles under DoS and deception attacks such that the safe distance $d_{i,j}$ remains between vehicles i and j, and all following vehicles maintain the same speed and acceleration with the leading vehicle, namely, $p_i(t) \to p_j(t) + d_{i,j}$, $v_i(t) \to v_0(t)$, and $a_i(t) \to a_0(t)$.

In this letter, the communication topology of the N following vehicles can be characterized by a undirected and connected graph $G = \{V, E\}$, where $V = \{1, 2, \ldots, N\}$ represents the set of vehicles, and $E \subseteq V \times V$ means the set of edges. Let $\mathcal{A} = [a_{ij}]_{N\times N}$ be the adjacency matrix with $a_{ij} \in \{0, 1\}$, where $a_{ij} = 1(0)$ implies $(i, j) \in (\notin) E$. The set of neighbor vehicles communicating with vehicle i is represented as $N_i = \{j \in V | a_{ij} = 1\}$. The degree of vehicle i is indicated as $\bar{D} = \text{diag}\{\bar{d}_1, \bar{d}_2, \ldots, \bar{d}_N\}$ with $\bar{d}_i = \sum_{j\in N_i} a_{ij}$. Then the Laplacian matrix L is expressed as $L = \bar{D} - A$. $\mathcal{B} = \text{diag}\{b_1, b_2, ..., b_N\}$ is the straight-through leader matrix, where $b_i \in \{0, 1\}$ with $b_i = 1$ denoting the following vehicle i communicating with the lead vehicle; $b_i = 0$ otherwise.

Since the vehicle-to-vehicle (V2V) communication relies on the open network, the data transmission is vulnerable to cyber attacks. A detection device based on the acknowledgment signal is used to associate event generator and controller to identify the occurrence of the valid DoS attacks. DoS attacks considered here are modeled in the following form:

$$S(t) = \begin{cases} 1, & t \in [H_n, H_n + \bar{H}_n) \\ 2, & t \in [H_n + \bar{H}_n, H_{n+1}) \end{cases} \tag{2}$$

where $[H_n, H_n + \bar{H}_n)$ is the attack interval with H_n denoting DoS on/off instant and $[H_n + \bar{H}_n, H_{n+1})$ is the attack-free interval with $H_n + \bar{H}_n$ denoting DoS off/on instant. Considering the power-constrained property of DoS attack, two assumptions need to be met in terms of the frequency $\mathcal{N}(t_1, t_2)$ and duration $\mathcal{S}(t_1, t_2)$ of the attack for the interval (t_1, t_2):

Assumption 1: There exist scalars $\mathcal{D}_1 > 0$, $\mathcal{D}_2 > 0$, $\mathcal{T}_1 > 0$, and

Corresponding author: Liang Zhang.

Citation: N. Zhao, X. D. Zhao, N. Xu, and L. Zhang, "Resilient event-triggered control of connected automated vehicles under cyber attacks," *IEEE/CAA J. Autom. Sinica*, vol. 10, no. 12, pp. 2300–2302, Dec. 2023.

N. Zhao and L. Zhang are with the College of Control Science and Engineering, Bohai University, Jinzhou 121013, and also with the Institute of Ocean Research, Bohai University, Jinzhou 121013, China (e-mail: zhaoning_hrbeu@163.com; md18638@126.com).

X. D. Zhao is with the Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, China (e-mail: xdzhaohit@gmail.com).

N. Xu is with the College of Information Science and Technology, Bohai University, Jinzhou 121013, China (e-mail: hpxuning@163.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JAS.2023.123483

$\mathcal{T}_2 \geq 1$, such that $\mathcal{N}(t_1,t_2) \leq \mathcal{D}_1 + \frac{t_2-t_1}{\mathcal{D}_2}, \mathcal{S}(t_1,t_2) \leq \mathcal{T}_1 + \frac{t_2-t_1}{\mathcal{T}_2}$.

In vehicle platoon, the vehicle i sends its own status information to the neighbor vehicle via wireless V2V communication. This faces the problems of network bandwidth limitation and cyber attacks. To solve these two problems, inspired by [7], the resilient event-triggered mechanism is applied to mitigate the network bandwidth pressure and remove the adverse effects of the attacks. Given that the communication network can only transmit discrete signals, we assume that the sampling period is h. In the absence of DoS attacks, the event-triggering instants can be decided by

$$e_i^T(t_k^i h + v^i h)\Omega_i e_i(t_k^i h + v^i h) \geq \sigma_i \bar{x}_i^T(t)\Omega_i \bar{x}_i(t) \tag{3}$$

where $t_k^i h$ denotes event-triggered instant of ith vehicle, σ_i is a predefined threshold, $e_i(t_k^i h + v^i h) = x_i(t_k^i h) - x_i(t_k^i h + v^i h)$, $v^i \in \mathbb{N}$, $\Omega > 0$ is a weighting matrix to be determined, and $\bar{x}_i(t) = \sum_{j=1}^{N} a_{ij}(x_i(t_k^i h) - x_j(t_{k^j}^j h) + D_{i,j}) + b_i(x_i(t_k^i h) - x_0(t_k^i h + v^i h) + D_{i,0})$, $D_{i,j} = [d_{i,j}, 0, 0]^T$ with $d_{i,j}$ denoting the safe distance for the vehicles i and j.

Unlike the existing result [7], the beginning and end moments of DoS attacks are not necessarily integer multiples of the sampling period. In order to characterize the real attack effective region, based on model (2), the new attack effective model can be described as

$$\hat{S}(t) = \begin{cases} 1, & t \in [\hat{H}_n, \hat{H}_n + \hat{\bar{H}}_n) \\ 2, & t \in [\hat{H}_n + \hat{\bar{H}}_n, \hat{H}_{n+1}) \end{cases}$$

where $\hat{H}_n = (\lfloor H_n/h \rfloor + 1)h$ and $\hat{H}_n + \hat{\bar{H}}_n = (\lfloor (H_n + \bar{H}_n)/h \rfloor + 1)h$. Let $\hat{\mathcal{S}}(t_1,t_2)$ be expressed as the duration of the effective attack. Then, based on Assumption 1, we can obtain $|\hat{\mathcal{S}}(t_1,t_2)| \leq |\mathcal{S}(t_1,t_2)| + h\mathcal{N}(t_1, t_2)$, which means $|\hat{\mathcal{S}}(t_1,t_2)| \leq (T_1 + D_1) + (\frac{1}{T_2} + \frac{h}{D_2})(t_2 - t_1)$.

Under the effect of DoS attacks, the resilient event-triggered mechanism is designed as follows:

$$t_{k+1}^i h \in \{t_{k^v}^i h \text{ satisfying (3)} \mid t_{k^v}^i h \in [\hat{H}_n, \hat{H}_n + \hat{\bar{H}}_n)\} \cup \{\hat{H}_n\} \tag{4}$$

where $t_{k^v}^i h$ denotes the periodic sampling instant.

In the absence of attacks, the distributed controller for vehicle i is constructed as

$$\begin{aligned} \bar{u}_i(t) = & -K \sum_{i \in \langle N \rangle} [a_{ij}(x_j(t_{k'}^j h) - x_i(t_k^i h) - D_{i,j}) \\ & + b_i(x_0(t_k^i h + v^i h) - x_i(t_k^i h) - D_{i,0})] \end{aligned} \tag{5}$$

where $K = [K_p, K_v, K_a]$ is the gain to be determined, $t_{k'}^j = \max\{t | t \in \{t_k^j,\ k \in \mathbb{N}\},\ t \leq t_k^j + v^j h\}$. Let $\eta(t) = [\eta_1(t), \eta_2(t), \ldots, \eta_N(t)]$ with $\eta_i(t) = x_i(t) - x_0(t) - d_{i,0}$, $\tau(t) = t - \ell h$, $t \in [\ell h, (\ell+1)h)$, $\ell \in \mathbb{N}$. Under deception attacks, the input of the actuator is $u_i(t) = \bar{u}_i(t) + \theta_i(t_k^i h) f_i(t_k^i h)$, where $f_i(t_k^i h)$ is defined as the deception attack and satisfies $\|f_i(t_k^i h)\|^2 \leq \|G_i x_i(t_k^i h)\|$ with G_i being a known constant matrix, and $\theta_i(t_k^i h) \in \{0,1\}$ satisfies the Bernoulli distribution, $\text{prob}\{\theta_i(t_k^i h) = 0\} = \bar{\theta}_i$, $\text{prob}\{\theta_i(t_k^i h) = 1\} = 1 - \bar{\theta}_i$. Under DoS attacks, the control input is zero, namely, $u_i(t) = 0$. Based on the effect of cyber attacks, we obtain from (1) and (5) that

$$\dot{\eta}(t) = \begin{cases} (I_N \otimes A)\eta(t) - (H \otimes BK)\eta(t - \tau(t)) \\ \quad -(H \otimes BK)e(t - \tau(t)) + (\Theta(t) \otimes B)F(t) \\ \quad t \in [\hat{H}_n, \hat{H}_n + \hat{\bar{H}}_n) \\ (I_N \otimes A)\eta(t),\ t \in [\hat{H}_n + \hat{\bar{H}}_n, \hat{H}_{n+1}) \end{cases} \tag{6}$$

where $H = L + \mathcal{B}$, $\tau(t) \in [0, h)$, $\dot{\tau}(t) = 1$ at $t \neq \ell h$, $\Theta(t) = \text{diag}\{\theta(t_{k_1}^1 h), \theta(t_{k_2}^2 h), \ldots, \theta(t_{k_N}^N h)\}$, and $F(t) = [f_1(t_{k_1}^1 h), f_2(t_{k_2}^2 h), \ldots, f_N(t_{k_N}^N h)]$.

Main results: This section provides sufficient conditions to guarantee exponential stability of the resulting system (6).

Theorem 1: Given scalars $\nu > 0$, $\sigma_i \in (0,1)$, $\bar{\theta}_i \in [0,1]$, h, $\mathcal{D}_\iota$, $\mathcal{T}_\iota$, γ_ι, κ_ι satisfying

$$\frac{\ln(\kappa_1\kappa_2)/(2\gamma_1 + 2\gamma_2)}{D_2} + \left(\frac{1}{T_2} + \frac{h}{D_2}\right) < \frac{\gamma_1}{\gamma_1 + \gamma_2} \tag{7}$$

and matrices G_i, K, system (6) under cyber attacks is exponentially stable if there exist $P_\iota > 0$, $Q_\iota > 0$, $R_\iota > 0$, and S_ι such that the following inequalities hold:

$$P_1 \leq \kappa_2 P_2, P_2 \leq \kappa_1 e^{2(\gamma_1+\gamma_2)h} P_2 \tag{8}$$

$$Q_\iota \leq \kappa_{3-\iota} Q_{3-\iota}, R_\iota \leq \kappa_{3-\iota} R_{3-\iota} \tag{9}$$

$$\begin{bmatrix} R_\iota & S_\iota \\ * & R_\iota \end{bmatrix} > 0 \tag{10}$$

$$\bar{\Gamma}^1 = \begin{bmatrix} \Gamma^1 & \Lambda_1 \\ * & \Lambda_2 \end{bmatrix} < 0,\ \bar{\Gamma}^2 = \begin{bmatrix} \Gamma^2 & \Upsilon_2^T \\ * & -R_2 \end{bmatrix} < 0 \tag{11}$$

where

$\Gamma^1 = [\Gamma_{\bar{m}\bar{n}}^1]_{5\times5}$, $\Gamma^2 = [\Gamma_{\bar{m}\bar{n}}^2]_{3\times3}$

$\Gamma_{11}^1 = I_N \otimes (2\gamma_1 P_1 + P_1 A + A^T P_1) + Q_1 - e^{-2\gamma_1 h} R_1$

$\Gamma_{12}^1 = -(H \otimes P_1 BK) + e^{-2\gamma_1 h}(R_1 + S_1),\ \Gamma_{13}^1 = -e^{-2\gamma_1 h} S_1$

$\Gamma_{14}^1 = -(H \otimes P_1 BK),\ \Gamma_{15}^1 = \bar{\Theta} \otimes P_1 B$

$\Gamma_{22}^1 = -e^{-2\gamma_1 h}(2R_1 + S_1 + S_1^T) + \bar{\sigma}\mathcal{H}^T \bar{\Omega}\mathcal{H}$

$\mathcal{H} = H \otimes I_n,\ \Gamma_{23}^1 = e^{-2\gamma_1 h}(R_1 + S_1),\ \Gamma_{24}^1 = \bar{\sigma}\bar{\Omega}\mathcal{H}$

$\Gamma_{33}^1 = -e^{-2\gamma_1 h}(Q_1 + R_1),\ \Gamma_{44}^1 = \bar{\sigma}\mathcal{H}^T \bar{\Omega}\mathcal{H} - \bar{\Omega}$

$\Gamma_{55}^1 = -\nu I_{mN},\ \Lambda_1 = [\Upsilon_{11}^T, \Upsilon_{12}^T, \Upsilon_{13}^T]$

$\Lambda_2 = \text{diag}\{-R_1, -R_1, -I_{nN}\}$, $\Upsilon_{11} = hR_1[(I_N \otimes A), -(H \otimes BK), 0_{nN}, -(H \otimes BK), (\bar{\Theta} \otimes B)]$, $\bar{\Theta} = \text{diag}\{\bar{\theta}_1, \bar{\theta}_2, \ldots, \bar{\theta}_N\}$

$\Upsilon_{12} = hR_1[0_{nN}, 0_{nN}, 0_{nN}, 0_{nN}, (\hat{\Theta} \otimes B)]$

$\Upsilon_{13} = [0_{nN}, \sqrt{\nu}\bar{G}^T, 0_{nN}, 0_{nN}, 0_{(nN,mN)}]$

$\bar{G} = \text{diag}\{G_1^T, G_2^T, \ldots, G_N^T\}$

$\bar{\Theta} = \text{diag}\{\hat{\theta}_1, \hat{\theta}_2, \ldots, \hat{\theta}_N\},\ \hat{\theta}_i = \bar{\theta}_i(1 - \bar{\theta}_i)$

$\Upsilon_2 = hR_2[(I_N \otimes A), 0_{nN}, 0_{nN}]$

$\bar{\sigma} = \max\{\sigma_1, \sigma_2, \ldots, \sigma_N\}$, $\bar{\Omega} = \text{diag}\{\Omega_1, \Omega_2, \ldots, \Omega_N\}$

$\Gamma_{11}^2 = I_N \otimes (-2\gamma_2 P_2 + P_2 A + A^T P_2) + Q_2 - R_2$

$\Gamma_{12}^2 = (R_2 + S_2),\ \Gamma_{13}^2 = -S_2,\ \Gamma_{22}^2 = -(2R_2 + S_2 + S_2^T)$

$\Gamma_{23}^2 = (R_2 + S_2),\ \Gamma_{33}^2 = -(Q_2 + R_2)$.

Proof: The proof can be finished by [7], the details are omitted. ■

Next, based on Theorem 1, the co-design scheme including the controller gain and the weighted matrices is stated as follows.

Theorem 2: Given scalars $\nu > 0$, $\sigma_i \in (0,1)$, $\bar{\theta}_i \in [0,1]$, h, $\mathcal{D}_\iota$, $\mathcal{T}_\iota$, γ_ι, κ_ι satisfying (7), and matrices G_i, system (6) under cyber attacks is exponentially stable if there exist $\hat{P}_\iota > 0$, $\hat{Q}_\iota > 0$, $\hat{R}_\iota > 0$, $\hat{S}$, $\hat{K}$ such that the following inequalities hold:

$$\begin{bmatrix} -\kappa_2 \hat{P}_2 & \hat{P}_2 \\ * & -\hat{P}_1 \end{bmatrix} \leq 0,\ \begin{bmatrix} -\kappa_1\varphi\hat{P}_1 & \hat{P}_1 \\ * & -\hat{P}_2 \end{bmatrix} \leq 0 \tag{12}$$

$$\begin{bmatrix} -\mu_{3-\iota}\hat{Q}_{(3-\iota)} & X_{(3-\iota)} \\ * & \varphi_\iota^2 \hat{Q}_\iota - 2\varphi_\iota X_\iota \end{bmatrix} \leq 0 \tag{13}$$

$$\begin{bmatrix} -\mu_{3-\iota}\hat{R}_{(3-\iota)} & X_{(3-\iota)} \\ * & \psi_\iota^2 \hat{R}_\iota - 2\psi_\iota X_\iota \end{bmatrix} \leq 0 \tag{14}$$

$$\begin{bmatrix} \hat{R}_\iota & \hat{S}_\iota \\ * & \hat{R}_\iota \end{bmatrix} > 0 \tag{15}$$

$$\begin{bmatrix} \hat{\Gamma}^1 & \hat{\Lambda}_1 \\ * & \hat{\Lambda}_2 \end{bmatrix} < 0,\ \begin{bmatrix} \hat{\Gamma}^2 & \hat{\Upsilon}_2^T \\ * & \hat{\Lambda}_3 \end{bmatrix} < 0 \tag{16}$$

where $\varphi = e^{2(\gamma_1+\gamma_2)h}$, $X_1 = I_N \otimes \hat{P}_1$, $X_2 = I_N \otimes \hat{P}_2$, $\hat{\Lambda}_1 = [\hat{\Upsilon}_{11}^T, \hat{\Upsilon}_{12}^T, \hat{\Upsilon}_{13}^T]$, $\hat{\Upsilon}_{11} = h[(I_N \otimes A\hat{P}_1), -(H \otimes B\hat{K}), 0_{nN}, -(H \otimes B\hat{K}), (\bar{\Theta} \otimes B)]$, $\hat{\Upsilon}_{12} = h[0_{nN}, 0_{nN}, 0_{nN}, 0_{nN}, (\hat{\Theta} \otimes B)]$, $\hat{\Upsilon}_{13} = [0_{nN}, \sqrt{\nu}(X_1\bar{G})^T, 0_{nN}, 0_{nN}, 0_{(nN,mN)}]$, $\hat{\Lambda}_2 = \text{diag}\{\beta_1^2\hat{R}_1 - 2\beta_1 X_1, \beta_1^2\hat{R}_1 - 2\beta_1 X_1, -I_{nN}\}$, $\hat{\Upsilon}_2 = h[(I_N \otimes A\hat{P}_2), 0_{nN}, 0_{nN}]$, $\hat{\Gamma}^1$ and $\hat{\Gamma}^2$ are obtained from Γ^1 and Γ^2, by replacing P_ι, $P_\iota A$, Q_ι, R_ι, $P_1 BK$, S_ι, $P_1 B$, $\bar{\Omega}$ with $\hat{P}_\iota$, $A\hat{P}_\iota$, $\hat{Q}_\iota$, $\hat{R}_\iota$, $B\hat{K}$, $\hat{S}_\iota$, B, $\hat{\Omega}$. Moreover, the controller gain and the weighting matrices are obtained by $K = \hat{K}\hat{P}_1^{-1}$ and $\bar{\Omega} = X_1^{-1}\hat{\Omega}X_1^{-1}$.

Proof: Let $\hat{P}_\iota = P_\iota^{-1}$, $\hat{\Omega} = X_1\bar{\Omega}X_1^T$, $\hat{Q}_\iota = \mathcal{X}_\iota Q_\iota \mathcal{X}_\iota^T$, $\hat{R}_\iota = \mathcal{X}_\iota R_\iota \mathcal{X}_\iota^T$, $\hat{S}_\iota = \mathcal{X}_\iota S_\iota \mathcal{X}_\iota^T$, $\hat{K} = K\hat{P}_1$, $J_1 = \text{diag}\{I_4 \otimes X_1, I_m, I_2 \otimes R_1^{-1}\}$, and $J_2 = I_3 \otimes X_2$. Then, pre-multiplying and post-multiplying $\bar{\Gamma}_\iota$ in (11) with J_ι and J_ι^T, and employing Schur complement lemma and $-X_\iota\hat{R}_\iota^{-1}X_\iota^T \leq \beta_\iota^2\hat{R}_\iota - 2\beta_\iota X_\iota$ with $\beta_\iota > 0$, the condition (11) is guaranteed by (16).

Next, it can be deduced that (12)–(15) ensure that (8)–(10) hold. ■

Numerical example: This section provides a simulation study with 1 leading vehicle and 3 following vehicles to substantiate the effectiveness of the proposed approach. We assume that the Laplacian matrix and the pinning matrix are $L=\begin{bmatrix}1&-1&0\\-1&1&0\\0&0&0\end{bmatrix}$, $\bar{D}=\text{diag}\{0,1,1\}$, and the desired distance between the vehicles is 20 m, namely, $d_{i,i-1}=20$ m.

Chose parameters $\kappa_1=\kappa_2=1.05$, $\varphi_1=\varphi_2=10$, $\psi_1=\psi_2=\beta_1=\beta_2=0.1$, $\sigma_1=\sigma_2=\sigma_3=0.1$, $\bar{\theta}_1=0.1$, $\bar{\theta}_2=0.15$, $\bar{\theta}_3=0.1$, $\nu=0.1$, $h=0.05$, $2\gamma_1=0.4$, $2\gamma_2=0.5$, $\mathcal{T}_2=2.5$, $\mathcal{D}_2=4$, then we can obtain that (7) holds. Based on the above parameters, by solving conditions in Theorem 2, the controller gain and event-triggered weighting matrices are obtained. Let initial conditions be $x_0(0)=[90,20,5]^T$, $x_1(0)=[62,0,0]^T$, $x_2(0)=[35,0,0]^T$, and $x_3(0)=[0,0,0]^T$, deception attacks be $f_1(t)=0.2\sin(G_1x_1(t))$ with $G_1=[1,0,0]$, $f_2(t)=0.25\sin(2G_2x_2(t))$ with $G_2=[0,1,0]$, $f_3(t)=0.3G_3x_3(t)\cos(G_3x_3(t))$ with $G_3=[0,0,1]$. Based on the above data, the designed event-triggered control strategy is applied to the vehicle platoon system, and the simulation results are shown in Figs. 1−4. The deception and DoS attacks sequences are provided in Figs. 1 and 2 (or Figs. 3 and 4) from which we know that $S_c=\{[0.7,0.9],[1.9,2],[2.6,3.1],[3.8,4.1],[4.9,5.3],[6.4,6.8],[8.5,8.95],[10,10.4],[12,12.45],[14.5,16.3],[18,18.9]\}$. The event-triggered instants are recorded in Fig. 2, from which we can see that the data is released at the end of DoS attacks, which means that the controller can immediately update to timely compensate for the impact of DoS attacks, and the amount of data sent is less than the amount of sampled data, which means that the proposed mechanism can save more communication resources. The displacement, speed and acceleration error trajectories of all following vehicles and the leading vehicle are shown in Fig. 3, from which we can see that all variables eventually converge to zeros. The displacement, speed and acceleration curves of all vehicles are depicted in Fig. 4, from which we can see that the desired distance between vehicles, and the speed and acceleration of all vehicles remain consistent. Therefore, the proposed resilient event-triggered control strategy can resist the impact of cyber attacks while realizing platoon control.

Conclusion: This letter has investigated the problem of resilient sampled-based event-triggering platoon control for automated vehicles under cyber attacks. By using a piecewise Lyapunov functional method, stability conditions for vehicular platoon systems have been formulated. Then, an efficient co-design scheme is presented regarding the controller gain and the event-triggering parameter matrices, which enables maintaining the desired distance and the common speed and acceleration between the vehicles.

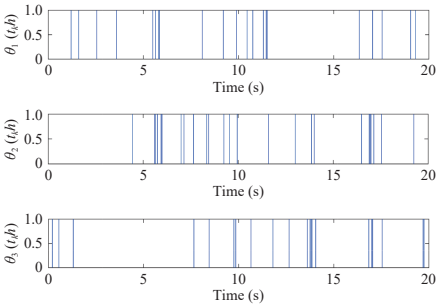

Fig. 1. Instants of deception attacks.

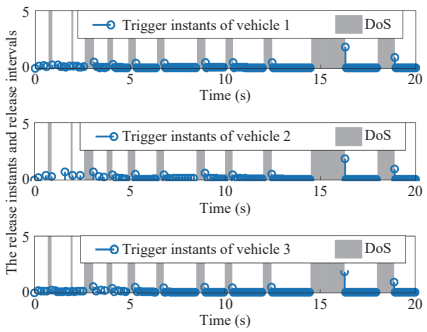

Fig. 2. The release instants.

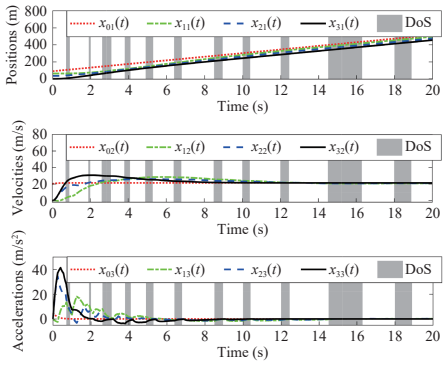

Fig. 3. Curves of system (6).

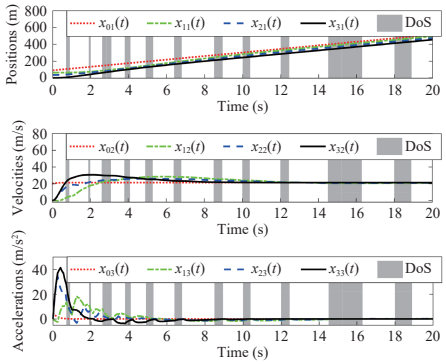

Fig. 4. Curves of system (1).

Acknowledgments: This work was supported in part by the National Natural Science Foundation of China (62203064, 62203065, 62303069) and the Open Fund of Institute of Ocean Research of Bohai University (BDHYYJY2023017).

References

[1] M. Amoozadeh, A. Raghuramu, C. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Comm. Magazine*, vol. 53, no. 6, pp. 126–132, 2015.

[2] G. Guo and W. Yue, "Sampled-data cooperative adaptive cruise control of vehicles with sensor failures," *IEEE Trans. Intelligent Transportation Syst.*, vol. 15, no. 6, pp. 2404–2418, 2014.

[3] F. Gao, X. Hu, S. E. Li, K. Li, and Q. Sun, "Distributed adaptive sliding mode control of vehicular platoon with uncertain interaction topology," *IEEE Trans. Industrial Electronics*, vol. 65, no. 8, pp. 6352–6361, 2018.

[4] H. Zhang, J. Liu, Z. Wang, H. Yan, and C. Zhang, "Distributed adaptive event-triggered control and stability analysis for vehicular platoon," *IEEE Trans. Intelligent Transportation Syst.*, vol. 22, no. 3, pp. 1627–1638, 2021.

[5] X. Ge, Q.-L. Han, Q. Wu, and X.-M. Zhang, "Resilient and safe platooning control of connected automated vehicles against intermittent denial-of-service attacks," *IEEE/CAA J. Autom. Sinica*, vol. 10, no. 5, pp. 1234–1251, May 2023.

[6] Y. Xu and G. Guo, "Event triggered control of connected vehicles under multiple cyber attacks," *Inform. Sciences*, vol. 582, pp. 778–796, 2022.

[7] N. Zhao, P. Shi, W. Xing, and J. Chambers, "Observer-based event-triggered approach for stochastic networked control systems under denial of service attacks," *IEEE Trans. Control Network Syst.*, vol. 8, no. 1, pp. 158–167, 2020.

[8] L. Ding, J. Li, M. Ye, and Y. Zhao, "Fully distributed resilient cooperative control of vehicular platoon systems under DoS attacks," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 5, pp. 937–940, 2022.

[9] 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. Cyber.*, vol. 52, no. 11, pp. 12003–12015, 2022.