ISA Transactions 131 (2022) 367–376

Contents lists available at ScienceDirect

ISA Transactions

journal homepage: www.elsevier.com/locate/isatrans

Research article

A resource-aware control approach to vehicle platoons under false data injection attacks

Fan Yang [a,*], Zhou Gu [a], Lingzhi Hua [b], Shen Yan [a]

[a] College of Mechanical & Electronics Engineering, Nanjing Forestry University, Nanjing, 210037, PR China
[b] Graduate School, Nanjing University of Finance and Economics, Nanjing, 210023, PR China

ARTICLE INFO

Article history:
Received 30 April 2021
Received in revised form 28 April 2022
Accepted 28 April 2022
Available online 5 May 2022

Keywords:
Vehicle platoon
String stability
Cooperative adaptive cruise control
Event-triggered mechanism
Cyber attack

ABSTRACT

Wireless vehicle-to-vehicle communication brings inevitable imperfections. This work simultaneously addresses the resource utilization and security issues for a vehicle platoon. Inspired by the modeling of denial of service attacks, a novel queuing model is constructed to depict false data injection attacks. A switched event-triggered mechanism is proposed to optimize network resources. The transmission rate can be actively reduced when the system is under malicious attacks. Then, a unified error system is established, where string stability is interpreted as global exponential stability. By using a proper Lyapunov function, a co-design approach is developed for closed-loop controllers and event-triggering parameters, with which the vehicle platoon can maintain a small safety distance and resist the negative impacts of cyber attacks. Finally, the proposed methods are verified by a virtual vehicle platoon.

1. Introduction

Intelligent transportation systems devote to solving the issues of traffic congestion, traffic safety and energy consumption while the connected vehicle system is one of the most promising development tendency [1]. Owing to inter-vehicle communication, vehicles can share all local information with surrounding ones. As such, vehicles in a platoon are tightly coupled, which contributes to efficient and accurate traffic control. In this circumstance, cooperative adaptive cruise control (CACC) systems have attracted significant attentions over the years [2]. The main objective of CACC is to maintain a desired inter-vehicle distance while resist the disturbances added to the string of vehicles. There are mainly two types of spacing schemes, that is, the constant spacing policy and constant time policy. [3] pointed out that the former was more commonly used in control applications although the latter seemed more rational. Another research hotspot lies in the control stability [4]. Since the disturbances can be amplified step by step, the vehicle platoon may be unstable even if every individual vehicle is guaranteed to be stable. It is mainly referred to as string stability, which is an essential requirement for vehicle platoons, see, e.g., [5–7]. In addition, Lyapunov approaches are employed to deal with the stability issues of vehicle platoons [8], where string stability is interpreted as asymptotic stability.

Wireless vehicle-to-vehicle communication is the basic ingredient to implement the advantages of CACC. However, it brings inevitable imperfections such as transmission delays and packet losses, see [9–11] and the references therein. In CACC, data exchanges among vehicles are usually implemented by a dedicated short range communication (DSRC) network, which is short of high level of security mechanisms and vulnerable to cyber attacks [12]. Cyber attacks have called for significant attentions due to their severe consequences. To name a few of the preliminary outcomes, [13] designed a set of observers for connected vehicle systems to detect the occurrence of cyber attacks using an adaptive estimation theory; An adaptive sliding mode observer was developed to estimate the longitudinal position, velocity and acceleration of the preceding vehicle for CACC [14]; In [15], a partial differential equation model was employed to diagnose a specific type of cyber attack called "false data injection (FDI)" attack in the vehicle platoon system; A novel resilient distributed state estimator was proposed to counteract the negative impact of cyber attacks, such as denial of service (DoS) or FDI attacks [16]. From the above approaches, existing researches primarily stay at the network layer rather than from a control-oriented perspective. In fact, vehicle platoons can be considered as networked control systems [17,18]. FDI attacks, a type of deception attacks aiming to interpolate inter-vehicle information, are mostly modeled as stochastic approaches in the existing literature, which rely unduly on priori knowledges of cyber attacks. However, it is not entirely realistic to catch the real intentions of attackers in advance. For the vehicle-to-vehicle network, the research work for designing resilient and precise controllers subject to specific cyber attacks is still largely open, which inspires one motivation of this study.

* Corresponding author.
E-mail address: yfan0510@sina.cn (F. Yang).

https://doi.org/10.1016/j.isatra.2022.04.046
0019-0578/

To achieve all the advantages of CACC, it is critical to overcome another network-induced imperfection, that is, excessive occupancy of DSRC network resources. Considering the digital nature of DSRC, most existing results of vehicle platoon control belong to a time-triggered communication scheme [19]. The scheduling of released data is purely based on a fixed sampling period but not on the actual control requirements. Such a resource-aware control scheme can refer to event-triggered mechanisms (ETMs) [20,21], in which data transmissions are permitted only when predefined triggering conditions are satisfied. Compared with time-triggered mechanisms, more network resources can be saved through ETMs. Especially in the case subject to cyber attacks, high transmission rates might degrade the control performance on the contrary as more polluted data are brought in. The event-triggered strategy can take full consideration of attacks, which yields specific triggering conditions. In fact, ETMs have been well researched and applied to certain fields [22]. In [23], an adaptive event-triggered scheme was designed for networked nonlinear interconnected systems, in which the triggering threshold varied with the error of the system state. [24] investigated an event-triggered control issue of a DC microgrid with multiple nonlinear constant power loads. In [25], a novel memory-based ETM was proposed for cloud-aided active suspension systems, then a better suspension performance was gained under deception attacks. Considering the efficient use of scarce network resources, two dynamic event-triggered control strategies were designed, and the dynamic ETM could obtain a larger inter-execution time than static ones [26]. In [27], a dynamic triggering threshold was designed by an adaptive rule, which relied on the current system state. This idea yields a larger threshold to reduce trigger frequency when the state approaches the equilibrium state. From the literature above, it is indicated that great efforts have been made to perfect the event-triggered communication scheme according to specific systems' requirements. When it comes to the control issue of vehicle platoons, a few research results are available, including [28–32]. Event-triggered communication schemes were established for a platoon system [28] and a CACC system [29], where the issue of time-varying transmission delays was investigated. [30] proposed a dynamic ETM, with which the frequency of sampled-data transmission could be significantly reduced. [31] was concerned with the design of distributed event-triggered observers, where collision avoidance and limited communication source of each vehicle were simultaneously considered. Nevertheless, in terms of the ETM itself, few improved ETMs have been developed for vehicle platoons. And how to design specific and optimized ETMs for vehicle platoons still remains a challenging work, especially in the network environment with attacks, which inspires another motivation of present work.

In this paper, we address the resource utilization and security issues for a vehicle platoon simultaneously. Suppose that the vehicle-to-vehicle communication suffers from FDI attacks. Inspired by the modeling of DoS attacks in [33], FDI attacks are to be modeled in terms of queuing approaches, which are composed of alternant sleeping time intervals and active time intervals. Such stealth attack behaviors are more in line with the attackers' intentions. An event-triggered strategy is adopted to reduce the releasing rate of sampled data. Unlike the static one in [20], an improved ETM is to be designed. To sum up, the highlights can be listed as follows:

(1) A new queuing model is developed to depict the nature of FDI attacks. To the best knowledge of the authors, it is the first attempt to construct such a queuing model.

(2) A novel switched event-triggered communication scheme is proposed. Compared with the existing improved approaches [23–27], this novel scheme takes full consideration of the negative effects of FDI attacks. By introducing an attack energy related triggering parameter, it can adaptively reduce the transmission rate. The larger the attack energy is, the less data will be released.

(3) Through Lyapunov functional approaches, a co-design method is developed for closed-loop controllers and ETM parameters, which guarantee the concerned system to be exponentially stable.

(4) The proposed method is applied to a virtual vehicle platoon composed of five vehicles, in which a targeted experiment of vehicle tracing is designed.

Notations: In this work, I_N is a N-dimensional identity matrix. For a matrix Q, Q^{-1} and Q^T denote its inverse and transpose, respectively. For a symmetric matrix Q, $\lambda_{min}(Q)$ and $\lambda_{max}(Q)$ are defined as the minimum and maximal eigenvalue of Q. For a real number n, $\lfloor n \rfloor$ represents the largest integer no more than n. Without special declarations, matrices are assumed to have compatible dimensions.

2. Problem formulation

2.1. Vehicle model

Consider a vehicle platoon as shown in Fig. 1, which is composed of a leading vehicle and N followers. We denote p_i, v_i and a_i as the ith vehicle's position, velocity and acceleration. Each follower is capable of measuring the relative distance with respect to its preceding vehicle by onboard sensors. Meanwhile, each vehicle shares its information of velocity and acceleration to its follower through DSRC network. It is worth pointing out that not all the sampled data are transmitted while an event trigger is equipped to determine a process of transmission on demand. During data exchange processes, network-induced delays and package losses are assumed to be out of scope of this work. Note that the $i-1$th vehicle's information is used during the design of ith vehicle's controller and event trigger.

The main control objective of the vehicle platoon is to maintain a certain safety distance between two adjacent vehicles. Suppose that the constant distance spacing policy is adopted [3], the spacing error can be defined as

$$e_i^p(t) = p_i - p_{i-1} + L + r_d \tag{1}$$

where L is the vehicle length and r_d represents the desired safety distance.

Although vehicle systems belong to strong nonlinear systems, a simple linear model is wildly used by linearization techniques [34]. The dynamics of the ith vehicle can be expressed as

$$\begin{cases} \dot{p}_i(t) = v_i(t) \\ \dot{v}_i(t) = a_i(t) \\ \dot{a}_i(t) = -a_i(t)/\pi_i + u_i(t)/\pi_i \end{cases} \tag{2}$$

where π_i is a time constant relevant to engine's dynamics.

To maintain the safety distance mentioned above, it is critical to make the follower match the velocity of the preceding one. Define an error vector $e_i(t) = \left[e_i^p(t) \quad e_i^v(t) \quad e_i^a(t)\right]^T$, where $e_i^v(t) = v_i(t) - v_{i-1}(t)$, $e_i^a(t) = a_i(t) - a_{i-1}(t)$, then we consider a control law of the following form:

$$u_i(t) = K_i e_i(t) \tag{3}$$

where $K_i = \left[k_i^p \quad k_i^v \quad k_i^a\right]^T$ is the controller gain to be designed.

In this work, the vehicle platoon including N+1 vehicles will be integrated into an extended error system. According to (2), the individual error system can be written as

$$\dot{e}_i(t) = A_i e_i(t) + B_i u_i(t) - B_{i-1} u_{i-1}(t) \tag{4}$$

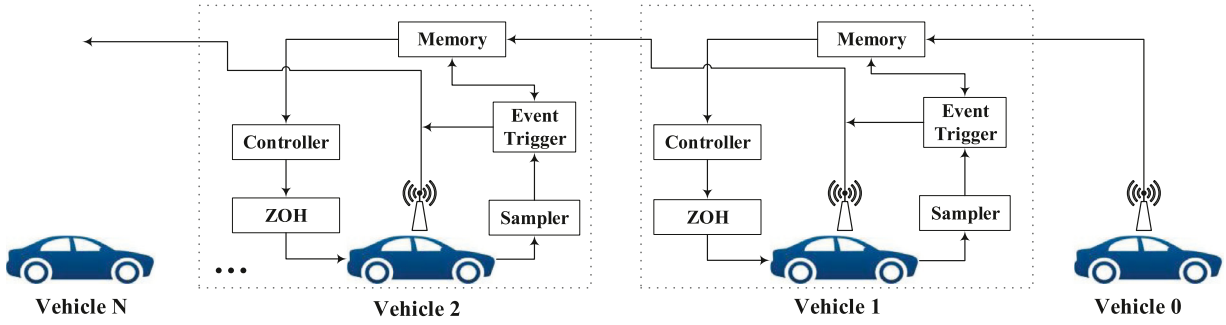

Fig. 1. Vehicle model.

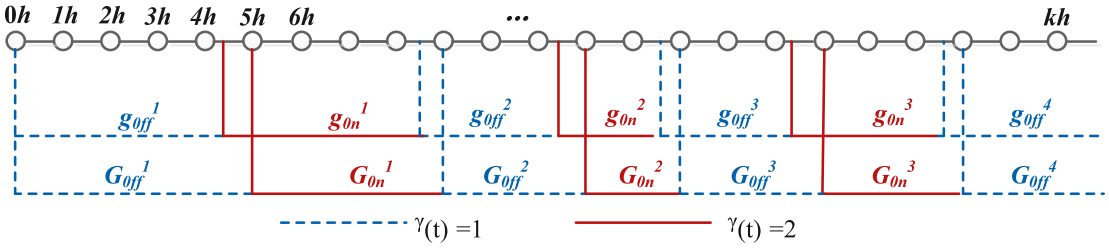

Fig. 2. Time sequence of intermittent FDI attacks.

where

$$A_i = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -1/\pi_i \end{bmatrix}, B_i = \begin{bmatrix} 0 \\ 0 \\ 1/\pi_i \end{bmatrix}.$$

Define $e(t) = [e_1^T(t), e_2^T(t), \ldots, e_N^T(t)]^T$ and $u(t) = [u_1(t), u_2(t), \ldots, u_N(t)]^T$ as the extended error vector and input vector, respectively. Combining Eqs. (2) and (4), we gain the extended error system as

$$\dot{e}(t) = Ae(t) + Bu(t) \tag{5}$$

in which

$$A = \begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & A_N \end{bmatrix},$$

$$B = \begin{bmatrix} B_1 & 0 & \cdots & 0 \\ -B_1 & B_2 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & -B_{N-1} & B_N \end{bmatrix}.$$

2.2. Modeling of false data injection attacks

The error information in (5) relies on data transmission via DSRC network. However, the network is vulnerable to cyber attacks and a queuing model is to be developed for FDI attacks.

Consider an intermittent attack signal:

$$\gamma(t) = \begin{cases} 1, & t \in [g^n, g^n + g_{off}^n) \\ 2, & t \in [g^n + g_{off}^n, g^{n+1}) \end{cases} \tag{6}$$

where $0 \le g^n < g^n + g_{off}^n < g^{n+1}$ for $n \in \mathbb{N}$. Fig. 2 shows a random example, and $\gamma(t)$ is used to identify two different attack modes. When $\gamma(t) = 1$, the concerned system is healthy and $[g^n, g^n + g_{off}^n)$ is called the nth sleeping time interval; when $\gamma(t) = 2$, FDI attacks are acting on the system and $[g^n + g_{off}^n, g^{n+1})$ is defined as the nth active time interval.

Remark 2.1. Deception attacks are usually modeled as stochastic approaches, which heavily depend on aforehand estimations of attackers' intentions. In contrast, $\gamma(t)$ represents a kind of real-time detection signal. On this basis, it gives rise to the potential of more precise controllers. Of course this assumes that the cyber attack is detectable.

Considering the periodic event-triggered strategy in Fig. 1, the attack signal can be rewritten as

$$\gamma(t) = \begin{cases} 1, & t \in [G^n, G^n + G_{off}^n) \\ 2, & t \in [G^n + G_{off}^n, G^{n+1}) \end{cases} \tag{7}$$

where $G^n = (\lfloor g^n/h \rfloor + 1)h$, $G_{off}^n = \{\lfloor (g^n + g_{off}^n)/h \rfloor + 1\}h - G^n$. We define $\Lambda_n^1 \triangleq [G^n, G^n + G_{off}^n)$ and $\Lambda_n^2 \triangleq [G^n + G_{off}^n, G^{n+1})$.

Remark 2.2. In the framework of event-triggered communication schemes, the sampling instants are the meaningful moments when the sampled data is considered to be released or not. That is, effective attack behaviors begin right from the sampling instants. For example, as shown in Fig. 2, the first attack arrives between the 4th and 5th sampling instant. Through the equivalent disposal in (7), the 5th sampling instant is considered as the beginning point.

Considering that cyber attacks are usually power-constrained, the following assumption can be made:

Assumption 2.1. The active time interval Λ_n^2 is always constrained by a scalar $G_{max} > 0$ while the sleep time interval Λ_n^1 is constrained by a scalar $G_{min} > 0$.

$$\inf_{n \in \mathbb{N}} \{G_{off}^n\} \ge G_{min} \tag{8}$$

$$\sup_{n \in \mathbb{N}} \{G_{on}^n\} \le G_{max} \tag{9}$$

where $G_{on}^n = G^{n+1} - G^n - G_{off}^n$.

Let $x_i(t) = \begin{bmatrix} 0 & v_i(t) & a_i(t) \end{bmatrix}^T$ denote the state to be transmitted to the $i+1$th vehicle and $x_i'(t) = \begin{bmatrix} e_i^p(t) & 0 & 0 \end{bmatrix}^T$ denote the

local information. Under false data injection attacks, the $i+1$th vehicle receives the contaminated data as

$$\hat{x}_i = x_i(t) + f_i(t) \tag{10}$$

where $f_i(t)$ is the injected false data. It is a bounded signal and Assumption 2.2 gives the related description.

Assumption 2.2. The injected false data $f_i(t)$ satisfies the following constraints:

$$\|f_i(t)\|_2 \leqslant \epsilon \|x_i(t) - x_{i-1}(t)\|_2 \tag{11}$$

Remark 2.3. FDI attacks belong to a type of deception attack. The attackers need to gain the information of the target system while they try to elude network security mechanisms. Besides, for the security mechanism of a vehicle platoon, the emphasis will be placed on the error information $x_i(t) - x_{i-1}(t)$. Hence, Assumption 2.2 takes a full consideration of the attackers' intentions and security strategies.

2.3. Design of switched event-triggered mechanism

To optimize the efficiency of network resources, an event-triggered strategy is employed in this work. Considering the intermittent behaviors of FDI attacks, a novel switched event-triggered mechanism (SETM) is proposed:

$$\begin{aligned} t_{n,s_i+1}^{i,\gamma(t)}h =& t_{n,s_i}^{i,\gamma(t)}h + \min_{l_i\geq 0, l_i\in\mathbb{N}} \Big\{ l_i h \mid \Delta_i^T \Omega_{\gamma(t)} \Delta_i \\ & - \sigma_i(t) \Theta_i^T \Omega_{\gamma(t)} \Theta_i \geq 0 \Big\} \end{aligned} \tag{12}$$

in which

$$\begin{aligned} &\sigma_i(t) = \sigma_0 + \omega\epsilon(\gamma(t)-1), \\ &\Delta_i \triangleq \Delta_i(t_{n,s_i}^{i,\gamma(t)}h + l_i h) = x_i(t_{n,s_i}^{i,\gamma(t)}h + l_i h) - x_i(t_{n,s_i}^{i,\gamma(t)}h), \\ &\Theta_i \triangleq \Theta_i(t_{n,s_i}^{i,\gamma(t)}h + l_i h) = x_i(t_{n,s_i}^{i,\gamma(t)}h) - \hat{x}_{i-1}(t_{n,\hat{s}_{i-1}}^{i-1,\gamma(t)}h), \\ &\hat{s}_{i-1} = \arg\min_{q\in\mathbb{N}} \left\{ t_{n,s_i}^{i,\gamma(t)} + l_i - t_{n,q}^{i-1,\gamma(t)} \mid t_{n,s_i}^{i,\gamma(t)} + l_i > t_{n,q}^{i-1,\gamma(t)} \right\}, \\ &t_{n,0}^{i,1}h \triangleq G^n,\ t_{n,0}^{i,2}h \triangleq G^n + G_{off}^n. \end{aligned}$$

where $\{t_{n,s_i}^{i,\gamma(t)}h\}$ are the releasing instants of the ith vehicle during the nth sleeping time interval or active time interval, $\sigma_0 > 0$ and $\omega > 0$ are prespecified constants, $\Omega_{\gamma(t)}$ are weighting matrices.

Remark 2.4. From the SETM (12), we can see that the triggering condition is adaptive for different attack modes. When $\gamma(t) = 1$, no attack is acting on the system and the SETM degenerates to the static one as in [33]; when $\gamma(t) = 2$, the system is suffering from malicious attacks. In fact, polluted data has a negative effect on the system performance. In particular, the higher level the attack is, the less data is expected to be transmitted. $\sigma_i(t) = \sigma_i + \omega\epsilon$ contributes to realizing this idea, that is, it yields a longer inter-execution time. Moreover, the larger the energy coefficient ϵ is, the larger the triggering parameter $\sigma_i(t)$ is, and the less data will be released.

Remark 2.5. The error information of the $i-1$th and ith vehicle's state is brought into the triggering condition. Not only the variation of an individual is considered, but also the relative relations of two adjacent vehicles have an effect on the triggering behaviors. Owing to the memory cell in Fig. 1, the last triggered data of the $i-1$th vehicle is utilized instead of the real-time sampling data.

Remark 2.6. As a switched event-triggered mechanism is proposed, it is worth mentioning its physical implementation. A specific software program can be designed by comparing the queuing of cyber attacks with the sampling sequence as shown in Fig. 2. Once pre-defined conditions are met, the switchings of local event triggers and controllers will be executed synchronously. From the definitions of $t_{n,0}^{i,1}h$ and $t_{n,0}^{i,2}h$, it can be inferred that whenever off/on or on/off transitions of attack modes occur, the system is forced to release the current data.

2.4. The resultant model

Based on the FDI attack model and design of switched event-triggered mechanism, we are now in a position to construct the resultant system.

For $t \in [kh, (k+1)h)$, we can always find a set of time instants $\{t_{n,m_i(t)}^{i,\gamma(t)}h\}$, which yields $[kh, (k+1)h) \in [t_{n,m_i(t)}^{i,\gamma(t)}h, t_{n,m_i(t)+1}^{i,\gamma(t)}h)$. Here, $m_i(t)$ is set as

$$m_i(t) = \arg\min_{q\in\mathbb{N}} \left\{ t - t_{n,q}^{i,\gamma(t)} \mid t > t_{n,q}^{i,\gamma(t)} \right\}$$

Then, we can rewrite Δ_i and Θ_i in (12) as

$$\Delta_i(kh) = x_i(kh) - x_i(t_{n,m_i(t)}^{i,\gamma(t)}h) \tag{13}$$

$$\Theta_i(kh) = x_i(t_{n,m_i(t)}^{i,\gamma(t)}h) - \hat{x}_{i-1}(t_{n,m_{i-1}(t)}^{i-1,\gamma(t)}h) \tag{14}$$

According to the SETM (12) and the ZOH in Fig. 1, the actual control input of the ith vehicle can be expressed as

$$\begin{aligned} u_i(t) &= K_{i,\gamma(t)}(x_i'(kh) + x_i(t_{n,m_i(t)}^{i,\gamma(t)}h) - \hat{x}_{i-1}(t_{n,m_{i-1}(t)}^{i-1,\gamma(t)}h)) \\ &= K_{i,\gamma(t)}(e_i(kh) + \Delta_{i-1}(kh) - \Delta_i(kh) \\ &\quad + (\gamma(t)-1)f_i(t)),\ t \in [kh, (k+1)h) \end{aligned} \tag{15}$$

Defining $\eta(t) = t - kh$ yields

$$\begin{aligned} u_i(t) =& K_{i,\gamma(t)}(e_i(t-\eta(t)) + \Delta_{i-1}(t-\eta(t)) - \Delta_i(t-\eta(t)) \\ & + (\gamma(t)-1)f_i(t)) \end{aligned} \tag{16}$$

in which $0 \leq \eta(t) < h$.

Remark 2.7. For the ith vehicle, its memory cell as shown in Fig. 1 stores the last triggered information of both the $i-1$th and ith vehicle with respect to the current moment. The components of $u_i(t)$ produced by $e_i^v(t)$ and $e_i^a(t)$ keep until next event trigger occurs. Meanwhile, $u_i(t)$ updates itself along with the local information of $e_i^p(t)$ at every sampling instant.

Without loss of generality, let $\Delta(t) = [\Delta_1^T(t), \Delta_2^T(t), \ldots, \Delta_N^T(t)]^T$, $F(t) = [f_1^T(t), f_2^T(t), \ldots, f_N^T(t)]^T$ and $K_{\gamma(t)} = diag\left\{K_{1,\gamma(t)}, K_{2,\gamma(t)}, \ldots, K_{N,\gamma(t)}\right\}$. Considering the definition of $u(t)$ and Eq. (16), one has

$$u(t) = K_{\gamma(t)}[e(t-\eta(t)) + \Psi(t-\eta(t)) + (\gamma(t)-1)F(t)] \tag{17}$$

where $\Psi(t) = (L \otimes I_3)\Delta(t)$, and $L = \begin{bmatrix} -1 & 0 & \cdots & 0 \\ 1 & -1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & -1 \end{bmatrix}$.

Substituting Eq. (17) into Eq. (5), we gain the resultant error system as

$$\begin{cases} \dot{e}(t) = Ae(t) + BK_{\gamma(t)}[e(t-\eta(t)) \\ \qquad + \Psi(t-\eta(t)) + (\gamma(t)-1)F(t)],\ t \in \Lambda_n^{\gamma(t)} \\ e(t) = \varphi(t), \qquad t \in [-h, 0] \end{cases} \tag{18}$$

Before proceeding further, we give the following definition about system stability.

Definition 2.1. The resultant error system (18) is called global exponential stability (GES), if there exist $\varrho > 0$ and $\varpi > 0$ satisfying $\|e(t)\| \leq \varpi e^{-\varrho t}\|\psi_0\|_h$, in which $\|\psi_0\|_h \triangleq sup_{-h\leq\theta\leq 0}\{\|e(\theta)\|, \|\dot{e}(\theta)\|\}$ and ϱ is called the decay rate.

For the vehicle platoon, the main control issue is to determine the controller gains $\{K_{i,\gamma(t)}\}$ and the critical parameters in the SETM (12) such that the resultant error system (18) is GES under the power-constrained attack signal (7).

3. Main results

The stability analysis for the system (18) with the attack signal (7) and the SETM (12) is formulated in the following theorem.

Theorem 3.1. *For given scalars $\sigma_0 \in (0,1)$, $\omega > 0$, $\epsilon > 0$, $\alpha_1 > 0$, $\alpha_2 > 0$, $\mu_1 \in (1,\infty)$, $\mu_2 \in (1,\infty)$, $G_{min} > 0$, $G_{max} > 0$, $\tau_a > 0$, $h > 0$, and prescribed matrices $S = diag\{0,1,1\}$, $\Sigma_1 = diag\{\sigma_{11},\sigma_{21},\ldots,\sigma_{N1}\}$, $\Sigma_2 = diag\{\sigma_{12},\sigma_{22},\ldots,\sigma_{N2}\}$ with $\sigma_{i1} = \sigma_0$, $\sigma_{i2} = \sigma_0 + \omega\epsilon$, $i = 1,2,\ldots,N$, satisfying*

$$\begin{aligned}\varrho = &(2\alpha_1 G_{min} - 2(\alpha_1+\alpha_2)h\\ &-2\alpha_2 G_{max} - \ln(\mu_1\mu_2))/\tau_a > 0\end{aligned} \tag{19}$$

The resultant error system (18) is GES with given controller gains K_m, if there exist $P_m > 0$, $Q_m > 0$, $R_m > 0$, $\Omega_m > 0$, and N_{ml}, M_{ml}, $m \in \{1,2\}$, $l \in \{1,2\}$ with appropriate dimensions such that

$$\begin{cases} P_1 \leq \mu_2 P_2,\ P_2 \leq \beta_0\mu_1 P_1 \\ Q_1 \leq \mu_2 Q_2,\ Q_2 \leq \mu_1 Q_1 \\ R_1 \leq \mu_2 R_2,\ R_2 \leq \mu_1 R_1 \end{cases} \tag{20}$$

$$\Pi^1 = \begin{bmatrix} \Pi^1_{11} & * & * \\ \Pi^1_{21} & \Pi^1_{22} & * \\ \Pi^1_{31} & 0 & \Pi^1_{33} \end{bmatrix} < 0, \tag{21}$$

$$\Pi^2 = \begin{bmatrix} \Pi^2_{11} & * & * \\ \Pi^2_{21} & \Pi^2_{22} & * \\ \Pi^2_{31} & 0 & \Pi^2_{33} \end{bmatrix} < 0, \tag{22}$$

$$\Pi^1_{11} = \begin{bmatrix} \Xi_1 & * & * & * \\ 0 & \Xi_2 & * & * \\ K_1^T B^T P_1 & 0 & \Xi_3 & * \\ \Xi_4 & N_{11}^T - N_{12} & \Xi_5 & \Xi_6 \end{bmatrix},$$

$$\Pi^1_{21} = \begin{bmatrix} \sqrt{h}A & 0 & BK_1 & BK_1 \end{bmatrix},$$

$$\Pi^1_{22} = -1/hR_1^{-1},$$

$$\Pi^1_{31} = \begin{bmatrix} M_{11}^T & 0 & 0 & M_{12}^T \\ 0 & N_{11}^T & 0 & N_{12}^T \end{bmatrix},$$

$$\Pi^1_{33} = diag\left\{-1/he^{-2\alpha_1 h}R_1, -1/he^{-2\alpha_1 h}R_1\right\},$$

$$\Pi^2_{11} = \begin{bmatrix} \Xi_7 & * & * & * & * \\ 0 & \Xi_8 & * & * & * \\ K_2^T B^T P_2 & 0 & \Xi_9 & * & * \\ \Xi_{10} & N_{11}^T - N_{12} & \Xi_{11} & \Xi_{12} & * \\ K_2^T B^T P_2 & 0 & \Xi_{13} & \Xi_{14} & \Xi_{15} \end{bmatrix},$$

$$\Pi^2_{21} = \begin{bmatrix} \sqrt{h}A & 0 & BK_2 & BK_2 & BK_2 \end{bmatrix},$$

$$\Pi^2_{22} = -1/hR_2^{-1},$$

$$\Pi^2_{31} = \begin{bmatrix} 0 & 0 & \sqrt{\epsilon} & \sqrt{\epsilon}(I_N\otimes S) & 0 \\ M_{21}^T & 0 & 0 & M_{22}^T & 0 \\ 0 & N_{21}^T & 0 & N_{22}^T & 0 \end{bmatrix},$$

$$\Pi^2_{33} = diag\left\{-I_{3N}, -1/hR_2, -1/hR_2\right\},$$

$$\Xi_1 = 2\alpha_1 P_1 + A^T P_1 + P_1 A + Q_1 + M_{11} + M_{11}^T,$$

$$\Xi_2 = -e^{-2\alpha_1 h}Q_1 - N_{11} - N_{11}^T,$$

$$\Xi_3 = (\Sigma_1\otimes\Omega_1) - ((L\otimes I_3)^{-1})^T(I_N\otimes\Omega_1)((L\otimes I_3)^{-1}),$$

$$\Xi_4 = K_1^T B^T P_1 - M_{11}^T + M_{12},$$

$$\Xi_5 = (I_N\otimes S)^T(\Sigma_1\otimes\Omega_1),$$

$$\Xi_6 = (I_N\otimes S)^T(\Sigma_1\otimes\Omega_1)(I_N\otimes S) - M_{12} - M_{12}^T + N_{12} + N_{12}^T,$$

$$\Xi_7 = -2\alpha_2 P_2 + A^T P_2 + P_2 A + Q_2 + M_{21} + M_{21}^T,$$

$$\Xi_8 = -e^{2\alpha_2 h}Q_2 - N_{21} - N_{21}^T,$$

$$\Xi_9 = (\Sigma_2\otimes\Omega_2) - ((L\otimes I_3)^{-1})^T(I_N\otimes\Omega_2)((L\otimes I_3)^{-1}),$$

$$\Xi_{10} = K_2^T B^T P_2 - M_{21}^T + M_{22},$$

$$\Xi_{11} = (I_N\otimes S)^T(\Sigma_2\otimes\Omega_2),$$

$$\Xi_{12} = (I_N\otimes S)^T(\Sigma_2\otimes\Omega_2)(I_N\otimes S) - M_{22} - M_{22}^T + N_{22} + N_{22}^T,$$

$$\Xi_{13} = (\Sigma_2\otimes\Omega_2),$$

$$\Xi_{14} = (\Sigma_2\otimes\Omega_2)(I_N\otimes S),$$

$$\Xi_{15} = (\Sigma_2\otimes\Omega_2) - I_{3N}.$$

Proof. Considering the error system (18), we choose the following Lyapunov–Krasovskii functional

$$\begin{aligned}V_m(t) =& e^T(t)P_m e(t) + \int_{t-h}^{t}\Upsilon_m e^T(s)Q_m e(s)ds \\ &+ \int_{-h}^{0}\int_{t+v}^{t}\Upsilon_m\dot{e}^T(s)R_m\dot{e}(s)dsdv\end{aligned}$$

where $m \in \{1,2\}$ is used to represent the sleeping mode ($m = 1$) and the active mode ($m = 2$) of cyber attacks, P_m, Q_m, R_m are positive definite matrices, $\Upsilon_m \triangleq e^{2(-1)^m\alpha_m(t-s)}$, and α_m are positive scalars.

Case 3.1. Suppose that $t \in [kh,(k+1)h) \in \Lambda_n^1$. Taking the time derivative of $V_1(t)$, we have

$$\begin{aligned}\dot{V}_1(t) =& -2\alpha_1 V_1(t) + e^T(t)(2\alpha_1 P_1 + A^T P_1 \\ &+ P_1 A + Q_1)e(t) + 2e(t-\eta(t))^T K_1^T B^T P_1 e(t) \\ &+ 2\Psi(t)^T K_1^T B^T P_1 x(t) \\ &- e^{-2\alpha_1 h}e(t-h)^T Q_1 e(t-h) \\ &+ h\dot{e}^T(t)R_1\dot{e}(t) \\ &+ \Delta^T(t)(I_N\otimes\Omega_1)\Delta(t) - \Delta^T(t)(I_N\otimes\Omega_1)\Delta(t) \\ &- \int_{t-h}^{t-\eta(t)} e^{-2\alpha_1(t-s)}\dot{e}(s)^T R_1\dot{e}(s)ds \\ &- \int_{t-\eta(t)}^{t} e^{-2\alpha_1(t-s)}\dot{e}(s)^T R_1\dot{e}(s)ds \\ &+ 2\xi_1^T(t)M_1(e(t) - e(t-\eta(t)) - \int_{t-\eta(t)}^{t}\dot{e}(s)ds) \\ &+ 2\xi_1^T(t)N_1(e(t-\eta(t)) - e(t-h) - \int_{t-h}^{t-\eta(t)}\dot{e}(s)ds)\end{aligned} \tag{23}$$

where $\xi_1(t) = \left[e^T(t) \quad e^T(t-h) \quad \Psi^T(t) \quad e^T(t-\eta(t))\right]^T$.

According to the SETM (12), we can derive that

$$\begin{aligned}&\Delta^T(t)(I_N\otimes\Omega_1)\Delta(t) \\ &\leq \Psi(t)^T(\Sigma\otimes\Omega_1)\Psi(t) \\ &+ 2\Psi(t)^T(\Sigma\otimes\Omega_1)(I_N\otimes S)e(t-\eta(t)) \\ &+ e(t-\eta(t))^T(I_N\otimes S)^T(\Sigma\otimes\Omega_1)(I_N\otimes S)e(t-\eta(t))\end{aligned} \tag{24}$$

Meanwhile, it can be deduced that

$$-2\xi_1^T(t)M_1\int_{t-\eta(t)}^{t}\dot{e}(s)ds \le h\xi_1^T(t)M_1e^{2\alpha_1 h}R_1^{-1} M_1^T\xi_1(t)+\int_{t-\eta(t)}^{t}e^{-2\alpha_1 h}\dot{e}(s)R_1\dot{e}(s)ds \tag{25}$$

$$-2\xi_1^T(t)N_1\int_{t-h}^{t-\eta(t)}\dot{x}(s)ds \le h\xi_1^T(t)N_1e^{2\alpha_1 h}R_1^{-1} N_1^T\xi_1(t)+\int_{t-h}^{t-\eta(t)}e^{-2\alpha_1 h}\dot{e}(s)R_1\dot{e}(s)ds \tag{26}$$

To simplify the following work, we define $M_1 = \begin{bmatrix}M_{11}^T & 0 & 0 & M_{12}^T\end{bmatrix}^T$, $N_1 = \begin{bmatrix}0 & N_{11}^T & 0 & N_{12}^T\end{bmatrix}^T$, where $M_{11}, M_{12}, N_{11}, N_{12}$ are arbitrary defined matrices. By applying Eqs. (24)–(26) to (23) and using the Schur's complement, it can be inferred that (21) is the sufficient condition to guarantee $\dot{V}_1(t)+2\alpha_1V_1(t)<0$. Integrating both sides of the above inequality yields that

$$V_1(t) < e^{-2\alpha_1(t-kh)}V_1(kh),\ t\in[kh,(k+1)h)\in\Lambda_n^1 \tag{27}$$

Case 3.2. Suppose that $t\in[kh,(k+1)h)\in\Lambda_n^2$. Through a similar analysis procedure as in Case 3.1, it is indicated that (22) is the sufficient condition to guarantee $\dot{V}_2(t)-2\alpha_2V_2(t)<0$. Similarly, we have

$$V_2(t) < e^{2\alpha_2(t-kh)}V_2(kh),\ t\in[kh,(k+1)h)\in\Lambda_n^2 \tag{28}$$

On the basis of Cases 3.1 and 3.2, we are now in a position to investigate the relationship between $V(t)$ and $V(0)$.

Combining the definition of $V_m(t)$ and the sufficient condition (20), we have the following preliminary inference at the time instants when off/on or on/off transitions occur:

$$\begin{cases}V_1(t_{n,0}^{i,1}h)\le\mu_2V_2(t_{n,0}^{i,1^-}h)\\ V_2(t_{n,0}^{i,2}h)\le\alpha_0\mu_1V_1(t_{n,0}^{i,2^-}h)\end{cases} \tag{29}$$

where $\alpha_0=e^{2(\alpha_1+\alpha_2)h}$.

We assume that there are n off/on transitions of cyber attacks over $(0,t)$, which means $t\in[G^n+G_{off}^n,G^{n+1})$ or $t\in[G^{n+1},G^{n+1}+G_{off}^{n+1})$. For $t\in[G^{n+1},G^{n+1}+G_{off}^{n+1})$, according to Eqs. (27)–(29) and Assumption 2.1, one has

$$\begin{aligned}&V(t)\\ &\le e^{-2\alpha_1(t-t_{n+1,0}^{i,1}h)}V_1(t_{n+1,0}^{i,1}h)\\ &\le\mu_2e^{-2\alpha_1(t-t_{n+1,0}^{i,1}h)}V_2(t_{n+1,0}^{i,1^-}h)\\ &\le\mu_2e^{-2\alpha_1(t-t_{n+1,0}^{i,1}h)}e^{2\alpha_2(t_{n+1,0}^{i,1}h-t_{n,0}^{i,2}h)}V_2(t_{n,0}^{i,2}h)\\ &\le\alpha_0\mu_1\mu_2e^{-2\alpha_1(t-t_{n+1,0}^{i,1}h)}e^{2\alpha_2G_{max}}V_1(t_{n,0}^{i,2^-}h)\\ &\vdots\\ &\le e^{-2\alpha_1G_{min}}e^{-\varrho t}V_1(0)\\ &\le e^{-\varrho t}V_1(0)\end{aligned} \tag{30}$$

Remark 3.1. In both the situations, $t\in[G^n+G_{off}^n,G^{n+1})$ and $t\in[G^{n+1},G^{n+1}+G_{off}^{n+1})$, we can deduce the same conclusion as in (30). Here, we omit the similar analysis procedure.

Let $\lambda_1=min\left\{\lambda_{min}(P_m)\right\}$, $\lambda_2=max\left\{\lambda_{max}(P_m)\right\}$, $\lambda_3=max\left\{\lambda_{max}(Q_m)\right\}$, $\lambda_4=max\left\{\lambda_{max}(R_m)\right\}$, $m\in\{1,2\}$, $\zeta=\lambda_2+h\lambda_3+(h^2/2)(\lambda_4+\lambda_5)>0$. From the definition of $V_m(t)$, it is clear that

$$\lambda_1\|e(t)\|^2\le V(t) \tag{31}$$

$$V_1(0)\le\zeta\|\psi_0\|_h^2 \tag{32}$$

Combining Eqs. (30)–(32), we have

$$\|e(t)\|\le\sqrt{\frac{\zeta}{\lambda_1}}e^{-\varrho/2t}\|\psi_0\|_h \tag{33}$$

According to Definition 2.1, it can be concluded that the error system (18) is GES. This completes the proof.

Based on Theorem 3.1, we will give the co-design method of controller gains $\{K_{i,\gamma(t)}\}$ and weighting matrices $\Omega_{\gamma(t)}$ of the SETM (12) in Theorem 3.2.

Theorem 3.2. *For given scalars $\sigma_0\in(0,1)$, $\omega>0$, $\epsilon>0$, $\alpha_1>0$, $\alpha_2>0$, $\mu_1\in(1,\infty)$, $\mu_2\in(1,\infty)$, $G_{min}>0$, $G_{max}>0$, $\tau_a>0$, $h>0$, $\rho_1>0$, $\rho_2>0$, $\rho_3>0$, and prescribed matrices $S=diag\{0,1,1\}$, $\Sigma_1=diag\{\sigma_{11},\sigma_{21},\ldots,\sigma_{N1}\}$, $\Sigma_2=diag\{\sigma_{12},\sigma_{22},\ldots,\sigma_{N2}\}$ with $\sigma_{i1}=\sigma_0$, $\sigma_{i2}=\sigma_0+\omega\epsilon$, $i=1,2,\ldots,N$, satisfying (19). The resultant error system (18) is GES with designed controller gains $K_{im}=Y_{im}X_{im}^{-1}$ $(i\in\{1,2,\ldots,N\})$, if there exist $X_m=diag\{X_{1m},X_{2m},\ldots,X_{Nm}\}>0$, $X_{im}>0$, $\widetilde{Q}_m>0$, $\widetilde{R}_m>0$, $\widetilde{\Omega}_m>0$, and $\widetilde{N}_{ml}$, $\widetilde{M}_{ml}$, $Y_m=diag\{Y_{1m},Y_{2m},\ldots,Y_{Nm}\}$, $m\in\{1,2\}$, $l\in\{1,2\}$, with appropriate dimensions such that*

$$\begin{cases}X_2\le\mu_2X_1, X_1\le\beta_0\mu_1X_2\\ \widetilde{Q}_1\le\mu_2\widetilde{Q}_2, \widetilde{Q}_2\le\mu_1\widetilde{Q}_1\\ \widetilde{R}_1\le\mu_2\widetilde{R}_2, \widetilde{R}_2\le\mu_1\widetilde{R}_1\end{cases} \tag{34}$$

$$\widetilde{\Pi}^1=\begin{bmatrix}\widetilde{\Pi}_{11}^1 & * & *\\ \widetilde{\Pi}_{21}^1 & \widetilde{\Pi}_{22}^1 & *\\ \widetilde{\Pi}_{31}^1 & 0 & \widetilde{\Pi}_{33}^1\end{bmatrix}<0, \tag{35}$$

$$\widetilde{\Pi}^2=\begin{bmatrix}\widetilde{\Pi}_{11}^2 & * & *\\ \widetilde{\Pi}_{21}^2 & \widetilde{\Pi}_{22}^2 & *\\ \widetilde{\Pi}_{31}^2 & 0 & \widetilde{\Pi}_{33}^2\end{bmatrix}<0, \tag{36}$$

$$\widetilde{\Pi}_{11}^1=\begin{bmatrix}\widetilde{\Xi}_1 & * & * & *\\ 0 & \widetilde{\Xi}_2 & * & *\\ Y_1^TB^T & 0 & \widetilde{\Xi}_3 & *\\ \widetilde{\Xi}_4 & \widetilde{N}_{11}^T-\widetilde{N}_{12} & \widetilde{\Xi}_5 & \widetilde{\Xi}_6\end{bmatrix},$$

$$\widetilde{\Pi}_{21}^1=\begin{bmatrix}\sqrt{h}AX_1 & 0 & BY_1 & BY_1\end{bmatrix},$$

$$\widetilde{\Pi}_{22}^1=-2/h\rho_1X_1+1/h\rho_1^2\widetilde{R}_1,$$

$$\widetilde{\Pi}_{31}^1=\begin{bmatrix}\widetilde{M}_{11}^T & 0 & 0 & \widetilde{M}_{12}^T\\ 0 & \widetilde{N}_{11}^T & 0 & \widetilde{N}_{12}^T\end{bmatrix},$$

$$\widetilde{\Pi}_{33}^1=diag\left\{-1/he^{-2\alpha_1h}\widetilde{R}_1,-1/he^{-2\alpha_1h}\widetilde{R}_1\right\},$$

$$\widetilde{\Pi}_{11}^2=\begin{bmatrix}\widetilde{\Xi}_7 & * & * & * & *\\ 0 & \widetilde{\Xi}_8 & * & * & *\\ Y_2^TB^T & 0 & \widetilde{\Xi}_9 & * & *\\ \widetilde{\Xi}_{10} & \widetilde{N}_{11}^T-\widetilde{N}_{12} & \widetilde{\Xi}_{11} & \widetilde{\Xi}_{12} & *\\ Y_2^TB^T & 0 & \widetilde{\Xi}_{13} & \widetilde{\Xi}_{14} & \widetilde{\Xi}_{15}\end{bmatrix},$$

$$\widetilde{\Pi}_{21}^2=\begin{bmatrix}\sqrt{h}AX_2 & 0 & BY_2 & BY_2 & BY_2\end{bmatrix},$$

$$\widetilde{\Pi}_{22}^2=-2/h\rho_2X_2+1/h\rho_2^2\widetilde{R}_2,$$

$$\widetilde{\Pi}_{31}^2=\begin{bmatrix}0 & 0 & \sqrt{\epsilon}X_2 & \sqrt{\epsilon}(I_N\otimes S)X_2 & 0\\ \widetilde{M}_{21}^T & 0 & 0 & \widetilde{M}_{22}^T & 0\\ 0 & \widetilde{N}_{21}^T & 0 & \widetilde{N}_{22}^T & 0\end{bmatrix},$$

$$\widetilde{\Pi}_{33}^2=diag\left\{-2\rho_3X_2+\rho_3^2,-1/h\widetilde{R}_2,-1/h\widetilde{R}_2\right\},$$

$$\widetilde{\Xi}_1=2\alpha_1X_1+X_1A^T+AX_1+\widetilde{Q}_1+\widetilde{M}_{11}+\widetilde{M}_{11}^T,$$

$$\widetilde{\Xi}_2=-e^{-2\alpha_1h}\widetilde{Q}_1-\widetilde{N}_{11}-\widetilde{N}_{11}^T,$$

$$\widetilde{\Xi}_3=(\Sigma_1\otimes\widetilde{\Omega}_1)-((L\otimes I_3)^{-1})^T(I_N\otimes\widetilde{\Omega}_1)((L\otimes I_3)^{-1}),$$

$$\widetilde{\Xi}_4=Y_1^TB^T-\widetilde{M}_{11}^T+\widetilde{M}_{12},$$

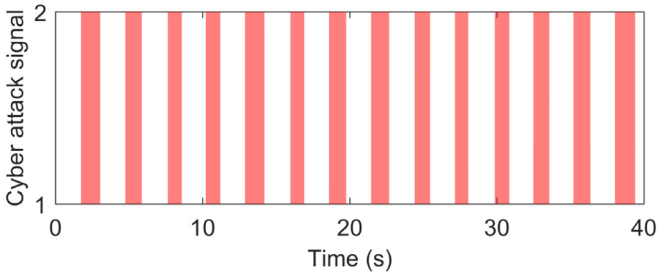

Fig. 3. Cyber attack signal.

$$\widetilde{\Xi}_5 = (I_N \otimes S)^T(\Sigma_1 \otimes \widetilde{\Omega}_1),$$
$$\widetilde{\Xi}_6 = (I_N \otimes S)^T(\Sigma_1 \otimes \widetilde{\Omega}_1)(I_N \otimes S) - \widetilde{M}_{12} - \widetilde{M}_{12}^T + \widetilde{N}_{12} + \widetilde{N}_{12}^T,$$
$$\widetilde{\Xi}_7 = -2\alpha_2 X_2 + X_2 A^T + AP_2 + \widetilde{Q}_2 + \widetilde{M}_{21} + \widetilde{M}_{21}^T,$$
$$\widetilde{\Xi}_8 = -e^{2\alpha_2 h}\widetilde{Q}_2 - \widetilde{N}_{21} - \widetilde{N}_{21}^T,$$
$$\widetilde{\Xi}_9 = (\Sigma_2 \otimes \widetilde{\Omega}_2) - ((L \otimes I_3)^{-1})^T(I_N \otimes \widetilde{\Omega}_2)((L \otimes I_3)^{-1}),$$
$$\widetilde{\Xi}_{10} = Y_2^T B^T - \widetilde{M}_{21}^T + \widetilde{M}_{22},$$
$$\widetilde{\Xi}_{11} = (I_N \otimes S)^T(\Sigma_2 \otimes \widetilde{\Omega}_2),$$
$$\widetilde{\Xi}_{12} = (I_N \otimes S)^T(\Sigma_2 \otimes \widetilde{\Omega}_2)(I_N \otimes S) - \widetilde{M}_{22} - \widetilde{M}_{22}^T + \widetilde{N}_{22} + \widetilde{N}_{22}^T,$$
$$\widetilde{\Xi}_{13} = (\Sigma_2 \otimes \widetilde{\Omega}_2),$$
$$\widetilde{\Xi}_{14} = (\Sigma_2 \otimes \widetilde{\Omega}_2)(I_N \otimes S),$$
$$\widetilde{\Xi}_{15} = (\Sigma_2 \otimes \widetilde{\Omega}_2) - 2\rho_3 X_2 + \rho_3^2.$$

Proof. In Theorem 3.1, let $P_m = diag\ \{P_{1m}, P_{2m}, \cdots, P_{Nm}\} > 0$, $P_{im} > 0$ $(i \in \{1, 2, \ldots, N\})$, and then we assume $X_{im} = P_{im}^{-1} > 0$, $X_m = diag\ \{X_{1m}, X_{2m}, \ldots, X_{Nm}\} > 0$, $K_{im} = Y_{im}X_{im}^{-1}$.

For $P_1 > 0, R_1 > 0$ and $\rho_1 > 0$, it is not difficult to deduce that $(\rho_1 R_1 - P_1)R_1^{-1}(\rho_1 R_1 - P_1) \geq 0$, which can be expressed as

$$-P_1 R_1^{-1} P_1 \leq -2\rho_1 P_1 + \rho_1^2 R_1 \tag{37}$$

Similarly, we have

$$-P_2 R_2^{-1} P_2 \leq -2\rho_2 P_2 + \rho_2^2 R_2 \tag{38}$$

$$-X_2 X_2 \leq -2\rho_3 X_2 + \rho_3^2 \tag{39}$$

According to Eqs. (37)–(39), by pre- and post-multiplying the sufficient condition (21) with $\text{diag}\{I, I, I, I, P_1, I, I\}$, $\text{diag}\{X_1, X_1, X_1, X_1, X_1, X_1, X_1\}$ and their transposes, successively, we can see that (35) is equivalent to (21). In the same way, (36) guarantees the sufficient condition (22). Note that $\widetilde{\Omega}_m = X_{im}\Omega_m X_{im}$, $\widetilde{M}_{11} = X_1 M_{11} X_1$, $\widetilde{M}_{12} = X_1 M_{12} X_1$, $\widetilde{M}_{21} = X_2 M_{21} X_2$, $\widetilde{M}_{22} = X_2 M_{22} X_2$, $\widetilde{N}_{11} = X_1 N_{11} X_1$, $\widetilde{N}_{12} = X_1 N_{12} X_1$, $\widetilde{N}_{21} = X_2 N_{21} X_2$, $\widetilde{N}_{22} = X_2 N_{22} X_2$, $\widetilde{Q}_m = X_m Q_m X_m$, $\widetilde{R}_m = X_m R_m X_m$. It is clear that (34) is the sufficient condition of (20). The proof is completed.

Remark 3.2. In the application of Theorem 3.2, we first gain the matrices X_{im}, Y_{im}, and $\widetilde{\Omega}_m$ by using the LMI Toolbox, then we obtain the controller gains $K_{im} = Y_{im}X_{im}^{-1}$ and the weighting matrices of the SETM $\Omega_m = X_{im}^{-1}\widetilde{\Omega}_m X_{im}^{-1}$.

4. Simulation examples

In this section, a numerical example is used to verify the proposed theorems. The vehicle platoon is composed of five vehicles. Note that all vehicles have the same dynamic characteristics and share the same parameters of the controller gain and the SETM. Suppose that the vehicle length $L = 5$ m, the desired safety distance $r_d = 30$ m and the inertial load $\pi_i = 0.3$.

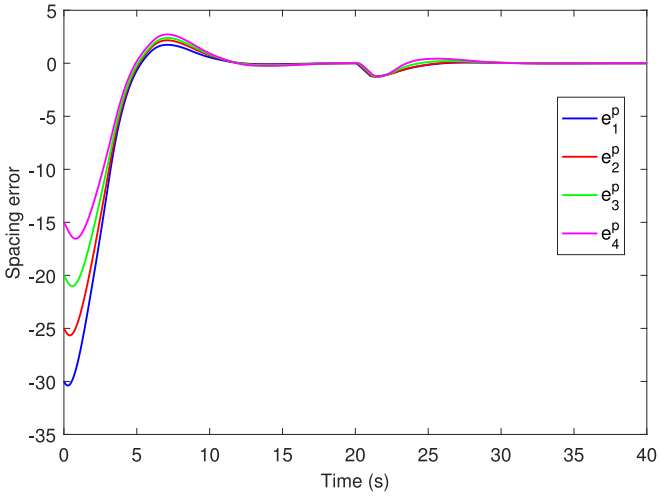

Fig. 4. Response of vehicles' spacing error.

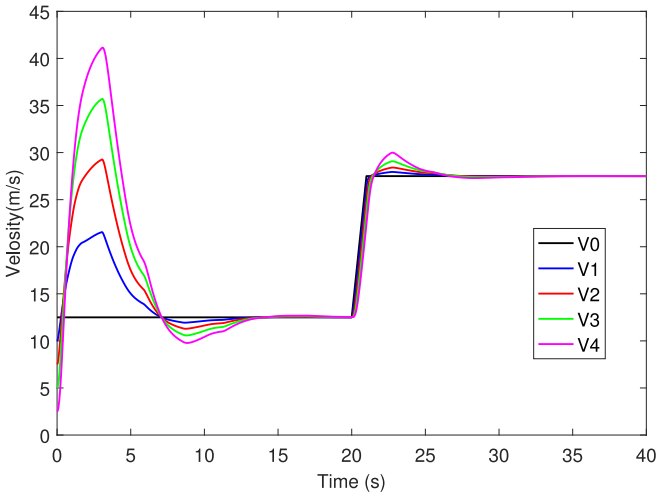

Fig. 5. Response of vehicles' velocity.

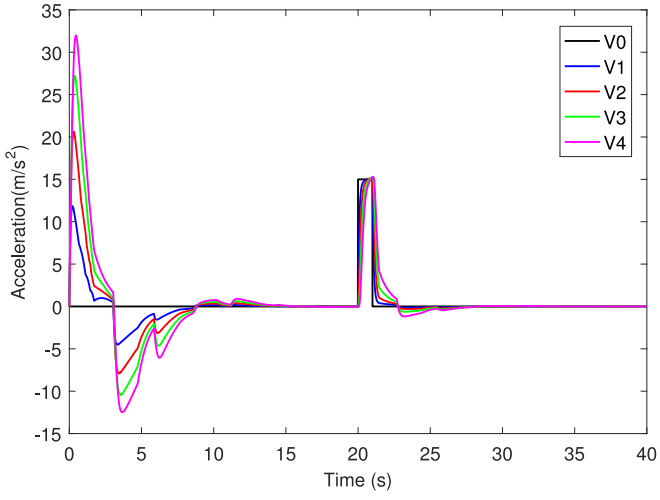

Fig. 6. Response of vehicles' acceleration.

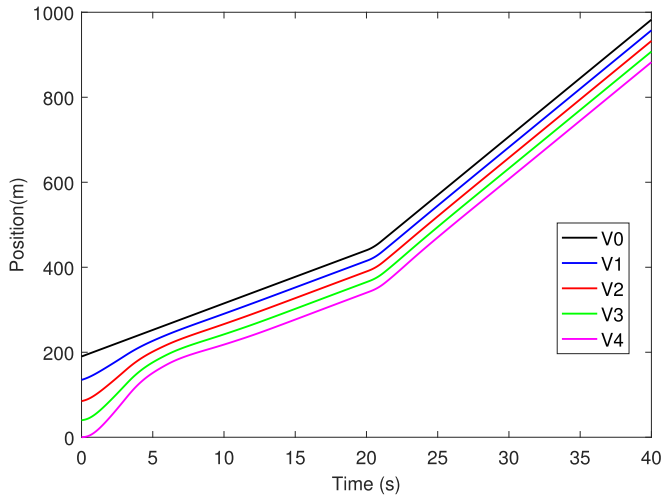

Fig. 7. Response of vehicles' position.

Table 1
Initial status of vehicles.

Vehicle	Position (m)	Velocity (m/s)	Acceleration (m/s^2)
V0	190	12.5	0
V1	135	10	0
V2	85	7.5	0
V3	40	5	0
V4	0	2.5	0

According to (19), the critical parameters involved in Theorem 3.2 are predefined as: $\sigma_0 = 0.2$, $\omega = 0.5$, $\alpha_1 = 0.14$, $\alpha_2 = 0.3$, $\mu_1 = 1.02$, $\mu_2 = 1.02$, $\rho_1 = \rho_2 = \rho_3 = 1.2$, $h = 0.01$ s. Meanwhile, an intermittent cyber attack signal is considered as shown in Fig. 3 with $G_{min} = 2$ s, $G_{max} = 0.8$ s. The injected false data is assumed to be $f_i(t) = \begin{bmatrix} 0 \\ -tanh(0.48(v_i(t) - v_{i-1}(t))) \\ -tanh(0.48(a_i(t) - a_{i-1}(t))) \end{bmatrix}$, which yields $\epsilon = 0.48$.

With the above parameters, feasible solutions of Theorem 3.2 can be found through the LMI toolbox, and we have

$$K_{i1} = \begin{bmatrix} -3.8221 & -9.9405 & -9.5665 \end{bmatrix},$$
$$K_{i2} = \begin{bmatrix} -0.2006 & -0.3793 & -0.2726 \end{bmatrix}. \quad (40)$$

$$\Omega_1 = \begin{bmatrix} 0.0286 & 0.0610 & 0.0482 \\ 0.0610 & 0.1491 & 0.1168 \\ 0.0482 & 0.1168 & 0.1033 \end{bmatrix},$$
$$\Omega_2 = \begin{bmatrix} 0.0056 & 0.0072 & 0.0047 \\ 0.0072 & 0.0108 & 0.0056 \\ 0.0047 & 0.0056 & 0.0068 \end{bmatrix}. \quad (41)$$

Remark 4.1. For the parameters involved in Theorem 3.2, some are selected on experience, for instances, the parameters ρ_1, ρ_2, ρ_3 and ω. In particular, the ones involved in (19) are key parameters, which have a significant effect on system performance. According to the definition of ϱ, the larger the α_1 is, a smaller α_2 will be requested, and we can gain a relatively larger decay rate. Moreover, σ_0 affects the releasing rate, as a rule, a smaller σ_0 is corresponding to a larger triggering tendency.

The initial statuses of five vehicles are shown in Table 1. Figs. 4–7 illustrate the responses of spacing error, velocity, acceleration and position, respectively. It is indicated that the main control objective can be achieved with the proposed control approach in the presence of cyber attacks. Over (0, 20 s), the following vehicles dynamically adjust their velocity and acceleration by using the switched event-triggered feedback controller. The vehicles can maintain the desired safety distance $r_d = 30$ m as shown in Figs. 4 and 7, and each following vehicle traces the same velocity and acceleration as the leading vehicle, accurately and rapidly. During the simulation, the leading vehicle performs a transient process of acceleration as shown in Fig. 6, and good tracing characteristics of following vehicles are demonstrated. Fig. 8 shows the corresponding transmission instant and releasing period of vehicle 2 as a representative. A small amount of sampled data are transmitted during the active time intervals of cyber attacks, which is corresponding to the concept of the SETM. The specific amount of triggers of four vehicles is listed in Table 2. With the proposed SETM, 12.9%, 19.1%, 24.6% and 27.9% of sampled data are transmitted through the network. If a time-triggered communication scheme is adopted, then all the 4000 sampled data will be transmitted. Obviously, the utilization of network resources is significantly improved by the SETM.

Table 2
Initial status of vehicles.

Vehicle	Triggers (SETM)	Triggers (static ETM)
V1	515	1150
V2	764	1435
V3	984	1764
V4	1114	1967

To further verify the effectiveness of the proposed control approach, a comparative simulation analysis is conducted between the proposed SETM and the static ETM. For the simulation of the static ETM, we set $\sigma_i(t) = \sigma_0$ as a constant in both the sleeping intervals and the active intervals. Note that the related parameters are set as the same as that in the SETM. The corresponding releasing period of vehicle 2 is shown in Fig. 9 as a representative. The specific amount of triggers is listed in Table 2, and 28.8%, 35.9%, 44.1%, 49.2% of sampled data are released with the static ETM. Compared with Fig. 8, a larger amount of sampled data are transmitted during the active time intervals. These data have been polluted by malicious attacks, which have a negative impact on system performances. That is the essential reason for the high triggering rate. Figs. 10–13 illustrate the responses of spacing error, velocity, acceleration and position, respectively. From Fig. 10, a slightly shorter settling time can be gained by the static ETM, but greater overshoots of velocity and acceleration are produced as shown in Figs. 11–12. It is indicated there is no significant improvement in the control performance although much more data are triggered. And then we can conclude that the SETM can obtain a better balance between the utilization rate of network resources and the system performance.

5. Conclusion

This work is concerned with the resource-aware control of a vehicle platoon subject to FDI attacks. The cooperative control issue of connected vehicles is considered as a whole, which is interpreted as the stabilization problem of an extended error system. Taking the nature of FDI attacks into account, a switched event-triggered communication scheme is developed, in which the event-triggered mechanism is switched with the variation of attack modes. By such a switching strategy, the utilization rate of network resources can be further improved. From the simulation results, it is indicated that the proposed approaches can guarantee the vehicle system to be stable, that is, each follower vehicle can accurately and rapidly trace the leading one with almost the same velocity and acceleration; meanwhile, a steady safety distance is maintained even during the dynamic adjustment process.

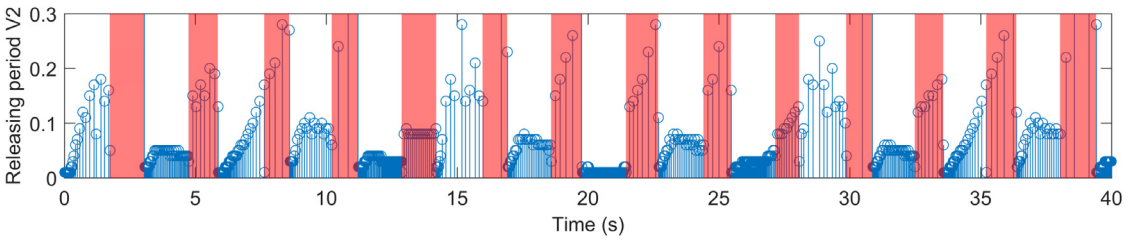

Fig. 8. Releasing period of vehicle 2.

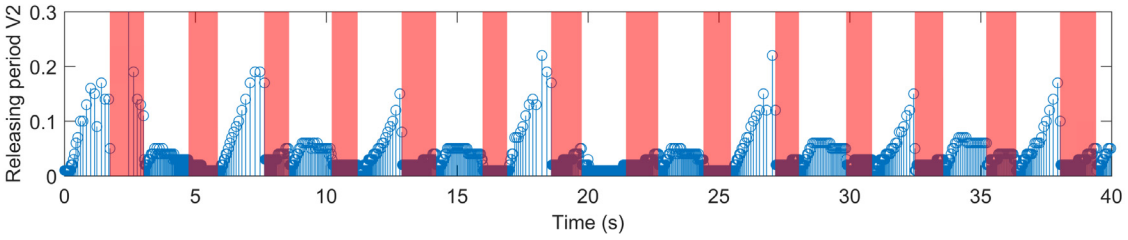

Fig. 9. Releasing period of vehicle 2.

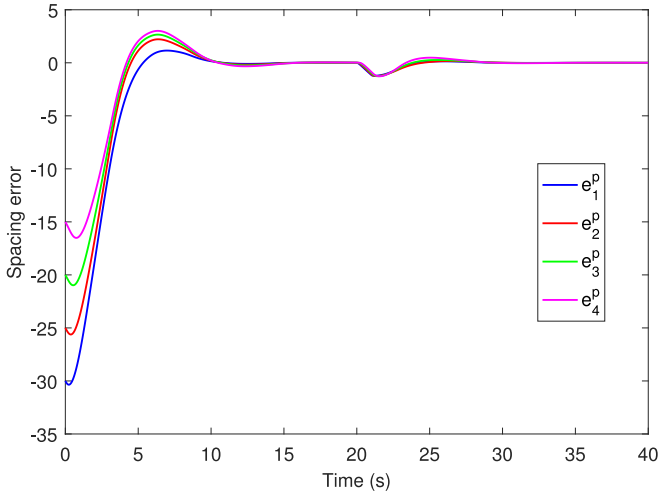

Fig. 10. Response of vehicles' spacing error.

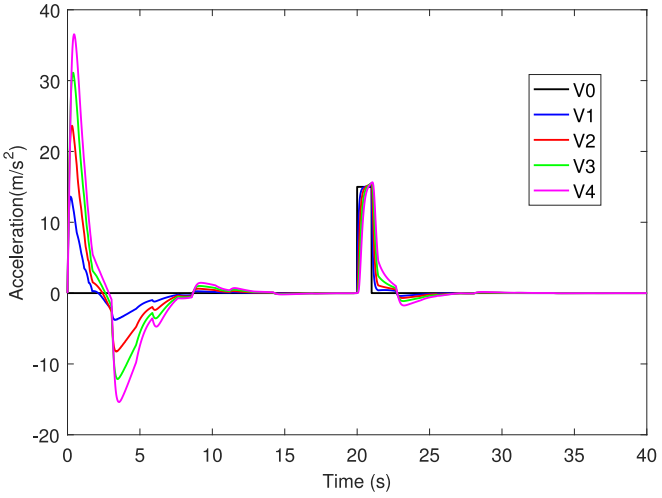

Fig. 12. Response of vehicles' acceleration.

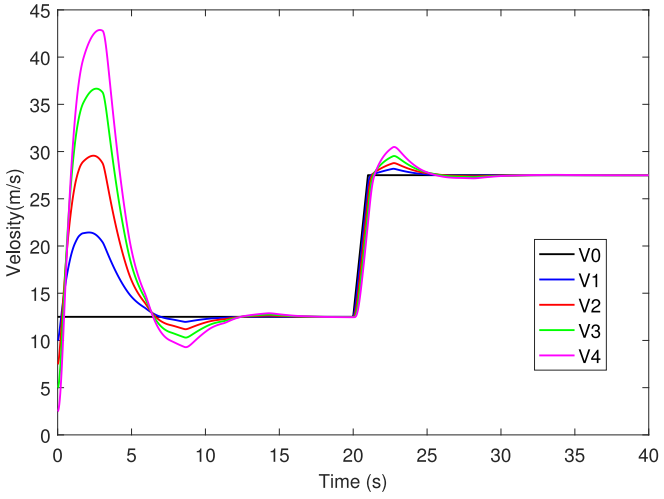

Fig. 11. Response of vehicles' velocity.

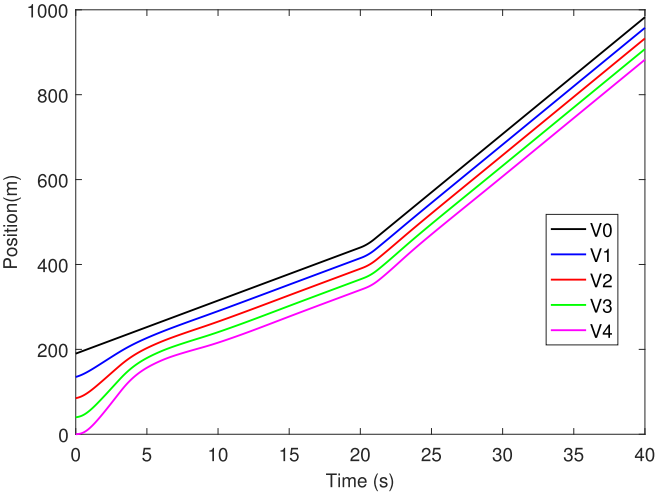

Fig. 13. Response of vehicles' position.

In the future work, we will combine the proposed control scheme with other network-induced imperfections such as transmission delays and packet losses. For potential applications, such a control approach can offer technical supports for automatic drive systems, especially in the aspects of vehicle tracking, vehicular networking safety, and rear-end collision warning.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grant No. 52005266, in part by the Natural Science Foundation of Jiangsu Province of China under Grant BK20200769.

References

[1] Dey KC, Yan L, Wang X, Wang Y, Shen H, Chowdhury M, Yu L, Qiu C, Soundararaj V. A review of communication, driver characteristics, and controls aspects of cooperative adaptive cruise control (CACC). IEEE Trans Intell Transp Syst 2016;17(2):491–509.
[2] Alipour-Fanid A, Dabaghchian M, Zeng K. Impact of jamming attacks on vehicular cooperative adaptive cruise control systems. IEEE Trans Veh Technol 2020;69(11):12679–93.
[3] Liu Y, Pan C, Gao H, Guo G. Cooperative spacing control for interconnected vehicle systems with input delays. IEEE Trans Veh Technol 2017;66(12):10692–704.
[4] Zhang J, Feng T, Yan F, Qiao S, Wang X. Analysis and design on intervehicle distance control of autonomous vehicle platoons. ISA Trans 2020;100:446–53.
[5] Gunter G, Janssen C, Barbour W, Stern RE, Work DB. Model-based string stability of adaptive cruise control systems using field data. IEEE Trans Intell Veh 2020;5(1):90–9.
[6] Merco R, Ferrante F, Pisu P. A hybrid controller for DOS-resilient string-stable vehicle platoons. IEEE Trans Intell Transp Syst 2021;22(3):1697–707.
[7] Wang L, Horn BKP. On the stability analysis of mixed traffic with vehicles under car-following and bilateral control. IEEE Trans Automat Control 2020;65(7):3076–83.
[8] Wen S, Guo G. Cooperative control and communication of connected vehicles considering packet dropping rate. Internat J Systems Sci 2018;49(13):2808–25.
[9] Thunberg J, Lyamin N, Sjoberg K, Vinel A. Vehicle-to-vehicle communications for platooning: Safety analysis. IEEE Netw Lett 2019;1(4):168–72.
[10] Zhao C, Duan X, Cai L, Cheng P. Vehicle platooning with non-ideal communication networks. IEEE Trans Veh Technol 2021;70(1):18–32.
[11] Wang Z, Gao Y, Fang C, Liu L, Zhou H, Zhang H. Optimal control design for connected cruise control with stochastic communication delays. IEEE Trans Veh Technol 2020;69(12):15357–69.
[12] Zhang D, Wang Q-G, Feng G, Shi Y, Vasilakos AV. A survey on attack detection, estimation and control of industrial cyberphysical systems. ISA Trans 2021;116:1–16.
[13] Abdollahi Biron Z, Dey S, Pisu P. Real-time detection and estimation of denial of service attack in connected vehicle systems. IEEE Trans Intell Transp Syst 2018;19(12):3893–902.
[14] Jahanshahi N, Ferrari RM. Attack detection and estimation in cooperative vehicles platoons: A sliding mode observer approach. IFAC-PapersOnLine 2018;51(23):212–7.
[15] Biroon RA, Pisu P, Abdollahi Z. Real-time false data injection attack detection in connected vehicle systems with pde modeling, Vol.2020. Denver, CO, United states; 2020, p. 3267–72, [Online].Available: http://dx.doi.org/10.23919/ACC45564.2020.9147977.
[16] Dutta RG, Hu Y, Yu F, Zhang T, Jin Y. Design and analysis of secure distributed estimator for vehicular platooning in adversarial environment. IEEE Trans Intell Transp Syst 2022;23(4):3418–29.
[17] Li SE, Zheng Y, Li K, Wu Y, Hedrick JK, Gao F, Zhang H. Dynamical modeling and distributed control of connected and automated vehicles: Challenges and opportunities. IEEE Intell Transp Syst Mag 2017;9(3):46–58.
[18] Villarreal-Cervantes MG, Sanchez-Santana JP, Guerrero-Castellanos J. Periodic Event-Triggered Control strategy for a (3,0) mobile robot network. ISA Trans 2020;96:490–500.
[19] Wen S, Guo G, Chen B, Gao X. Event-triggered cooperative control of vehicle platoons in vehicular ad hoc networks. Inform Sci 2018;459:341–53.
[20] Yue D, Tian E, Han Q. A delay system method for designing event-triggered controllers of networked control systems. IEEE Trans Automat Control 2013;58(2):475–81.
[21] Hu S, Yue D, Yin X, Xie X, Ma Y. Adaptive event-triggered control for nonlinear discrete-time systems. Internat J Robust Nonlinear Control 2016;26(18):4104–25.
[22] Li T, Zhao H, Chang Y. A novel event-triggered communication strategy for second-order multiagent systems. ISA Trans 2020;97:93–101.
[23] Gu Z, Yue D, Tian E. On designing of an adaptive event-triggered communication scheme for nonlinear networked interconnected control systems. Inform Sci 2018;422:257–70.
[24] Hu S, Yuan P, Yue D, Dou C, Cheng Z, Zhang Y. Attack-resilient event-triggered controller design of DC microgrids under DoS attacks. IEEE Trans Circuits Syst I Regul Pap 2020;67(2):699–710.
[25] Sun X, Gu Z, Yang F, Yan S. Memory-event-trigger-based secure control of cloud-aided active suspension systems against deception attacks. Inform Sci 2020;543:1–17.
[26] Luo S, Deng F, Chen W-H. Dynamic event-triggered control for linear stochastic systems with sporadic measurements and communication delays. Automatica 2019;107:86–94.
[27] Gu Z, Yan S, Ahn CK, Yue D, Xie X. Event-triggered dissipative tracking control of networked control systems with distributed communication delay. IEEE Syst J 2021. (in press),.
[28] Wei Y, Liyuan W, Ge G. Event-triggered platoon control of vehicles with time-varying delay and probabilistic faults. Mech Syst Signal Process 2017;87:96–117.
[29] Dolk V, Tesi P, De Persis C, Heemels W. Event-triggered control systems under denial-of-service attacks. IEEE Trans Control Netw Syst 2017;4(1):93–105.
[30] Wen S, Guo G, Chen B, Gao X. Cooperative adaptive cruise control of vehicles using a resource-efficient communication mechanism. IEEE Trans Intell Veh 2019;4(1):127–40.
[31] Zhang H, Liu J, Wang Z, Yan H, Zhang C. Distributed adaptive event-triggered control and stability analysis for vehicular platoon. IEEE Trans Intell Transp Syst 2021;22(3):1627–38.
[32] Sun J, Long T. Event-triggered distributed zero-sum differential game for nonlinear multi-agent systems using adaptive dynamic programming. ISA Trans 2021;110:39–52.
[33] Hu S, Yue D, Chen X, Cheng Z, Xie X. Resilient HFiltering for event-triggered networked systems under nonperiodic DoS jamming attacks. IEEE Trans Syst Man Cybern 2021;51(3):1392–403.
[34] Zheng Y, Li SE, Wang J, Cao D, Li K. Stability and scalability of homogeneous vehicular platoon: Study on the influence of information flow topologies. IEEE Trans Intell Transp Syst 2016;17(1):14–26.