Distributed Anti-attack Fault-tolerant Tracking Control for Vehicle Platoon Systems under Cyber-physical Threats

Chun Liu, *Member, IEEE*, Jing Zhao, and Ron J. Patton, *Life Fellow, IEEE*

***Abstract*—Vehicle platoon systems are considered as automatous vehicles in a platoon-based driving pattern in which a following vehicle follows the preceding vehicle and maintains the desired vehicle spacing. This study investigates the leader-following tracking issue of vehicle platoon systems under cyber-physical threats with the distributed anti-attack fault-tolerant tracking control strategy. Vehicle platoon systems, complicated actuator faults in physical layer, and connectivity-mixed attacks in cyber layer are modeled, respectively. Decentralized fault-estimation unknown input observer and distributed anti-attack fault-tolerant tracking control designs are developed in an integrated control framework to guarantee the robust and resilient tracking property of estimation errors and platoon tracking errors as well as the reliable inter-vehicle spacing by virtue of attack activation rate and attack frequency metrics. Simulations validate the proposed distributed anti-attack fault-tolerant tracking control algorithm in pernicious cyber-physical threatened scenarios.**

***Index Terms*—Vehicle platoon systems, cyber-physical threats, distributed control, anti-attack fault-tolerant tracking control, fault-estimation.**

I. Introduction

COMPARED with driving individually, vehicle platoon systems in intelligent transportation fields have received increasing attention in significantly improving road capacity and traffic efficiency from academia, commerce and industry [1]-[3]. A survey including platoon-based cooperative control and vehicular communication is reviewed in [4]. Since actuator faults, such as additive fault [5], potential fault [6], and saturation fault [7] inevitably occur in vehicle platoon systems, and environment disturbances, such as road slope and wind gust inside the network-induced platoon can also influence the velocity-tracking [8] and path-following [9] performance.

Compared with fault diagnosis with reduced excitations for detection, identification, location and isolation of faults [10], to maintain the vehicle platoon stability and to promote the leader-following tracking accuracy in case of failure, reliable fault-tolerant tracking control (FTTC) strategy has attracted significant attention [11]-[13]. An adaptive FTTC protocol is proposed for heterogeneous vehicular platoons involved with input quantization and dead-zone nonlinearity to realize individual vehicle, string and traffic flow stabilities, respectively [14]. The neuroadaptive FTTC scheme with nussbaum function is developed for nonlinear vehicle platoon systems to attenuate the negative effects of unknown direction actuator faults and spacing constraints [15]. Considering that in practice, local vehicles are not able to access internal status signal and global information of vehicle platoon systems, a distributed FTTC framework [16] with local and neighboring output collections needs to be urgently explored. However, plenty of the existing FTTC studies providing different tolerant abilities for vehicle platoon systems mainly deal with the traditional abrupt-type actuator faults [7]-[9], [13] and even require a high-level hardware allocation and reconfiguration [17]. In addition, the large-scale collisions may originate from a single vehicle transmitting early and incipient actuator faults to its neighboring vehicles via vehicle-to-vehicle networks. Thus, the systematized FTTC technologies in a distributed fashion, especially for platoon-based cyber-physical systems despite any vehicle suffering from the complicated abrupt-type and incipient-type actuator faults are essential for cooperative driving of connected vehicles but are rarely studied in detail.

The characteristics of physical constraints and widespread ad hoc network of vehicle platoon systems with computing and digital devices render it fragile and vulnerable not only to physical intrusions [18] but also cyber-attacks (deception attack [19], sensor and actuator attack [20] and denial-of-service attack [21], [22]). Specifically, the active attack detection issues in cooperative vehicle platoon systems under cyber-attacks associated with an adaptive sliding mode observer [23] and information-weighted set-membership filtering estimator [24] are investigated, respectively. The secure tracking control of cooperative driving of autonomous connected vehicles via an adaptive synchronization-based algorithm [25] requires more accurate and reliable vehicle-to-vehicle information, but the essential wireless communication topologies under cyber-attacks are destroyed by various security vulnerabilities, thus leading to dangerous implications for cooperative driving safety. Hence, vehicle platoon systems must be developed to bear such dangers (accidental and deliberate cyber-physical threats) in mind. The defensive and tolerant instincts are equipped for vehicles to operate robustly and healthily under both complicated actuator faults and malicious cyber-attacks with different nodes of action, different timing and different durations. Indeed, there are limited FTTC studies with resilient

This work was supported by National Natural Science Foundation of China (62103250); Shanghai Sailing Program (21YF1414000). *(Corresponding author: Chun Liu.)*

C. Liu is with the School of Mechatronic Engineering and Automation, and also with the School of Artificial Intelligence, Shanghai University, Shanghai 200444, China (e-mail: Chun_Liu@shu.edu.cn).

J. Zhao is with the Shanghai Microsate Engineering Center, Shanghai, 200120, China (e-mail: zhaojingashley@163.com).

R. J. Patton is with the School of Engineering and Computer Science, University of Hull, Hull HU6 7RX, U.K. (e-mail: r.j.patton@hull.ac.uk).

secure management on integrating both fault compensation and attack defense in the networked vehicle platoon systems [26], [27]. To tackle the dilemma, the development of an improved distributed anti-attack FTTC protocol for vehicle platoon systems under cyber-physical threats is necessary but challenging, as the synchronization tracking target with an anti-attack performance of vehicles cannot be straightforward addressed by existing FTTC techniques based on balanced graph theory [13], [17] or switching topology policies [12].

The major innovations are summarized as follows. (i) Compared with cooperative FTTC issues of vehicle platoon systems under individual adversarial cyber-attacks [19], [20], [25] or traditional abrupt-type faults [7], [13], this study contributes greatly in providing both strong resilience to preserving/broken connectivities caused by connectivity-mixed attacks in cyber layer and robust offset to complicated constraints from abrupt-/incipient-type actuator faults in physical layer comprehensively. (ii) Unlike the separated observer-based fault-estimation [5], [9], [11] or attack detection-based FTTC schemes [23], [24], an integrated control framework is developed with the advantageous combination of the decentralized fault-estimation unknown input observer (UIO) design and distributed anti-attack FTTC design for the safe and reliable maneuvering in all possible cyber-physical threat conditions. (iii) The common average dwelling time indicator between stable and unstable sub-topologies [12] is circumvented by attack activation rate and attack frequency metrics for connectivity-mixed attacks to overcome the limitation of not being able to distinguish between the real-time impact of attacks and faults. The matched network with one-dimensional information flow between platoon vehicles is replaced and generalized to unmatched and switching topologies with multi-dimensional information interactions, eventually achieving an exponential platoon tracking performance and maintaining inter-vehicle spacing with the distributed anti-attack FTTC algorithm.

The remainder is formulated as follows. The vehicle platoon systems and cyber-physical threat are modeled in Section II. Sections III proposes the decentralized fault-estimation UIO and distributed anti-attack FTTC designs. Simulation in Section IV validates the efficiency of the distributed anti-attack FTTC algorithm. Conclusions are provided in Section V.

II. Model description and system formulation

A. Vehicle platoon system modeling

Consider that the vehicle platoon systems consist of $N+1$ vehicles. The ith following vehicle ($i = 1, \cdots, N$) with the homogeneous dynamics in physical layer is described as

$$\begin{cases} \dot{p}_i(t) = v_i(t) \\ \dot{v}_i(t) = a_i(t) + d_i^v(t) \\ \dot{a}_i(t) = -\frac{1}{\tau}a_i(t) + \frac{1}{\tau}u_i(t) + d_i^a(t), i = 1, \cdots, N \end{cases} \tag{1}$$

where $p_i(t), v_i(t)$ and $a_i(t)$ denote the position, velocity and acceleration of the ith following vehicle, respectively, $u_i(t)$ represents the actual control input, $d_i^v(t)$ and $d_i^a(t)$ denote the airflow or road surface-induced disturbance in the velocity channel and the modeling uncertainty-induced disturbance in the acceleration channel, respectively, and τ is the time constant denoted as the engine dynamics.

The spacing $l_i(t)$ between the (i-1)th following vehicle and the ith following one is denoted as $l_i(t) = p_{i-1}(t) - p_i(t) - L, i = 1, \cdots, N$ with L denoted as the length of each vehicle. It follows from [3] that the desired spacing $l_i^r(t)$ between two neighboring vehicles is defined as $l_i^r(t) = r_i + hv_i(t)$, where r_i is the desired static spacing and h is the time headway.

Define the internal state, the available output by position and velocity sensors, and the external disturbance as $x_i(t) = [p_i(t)\ v_i(t)\ a_i(t)\ e_i^r(t)]^T, y_i = [p_i(t)\ v_i(t)]^T$ and $\omega_i(t) = [0\ d_i^v(t)\ d_i^a(t)\ hd_i^v(t) - v_{i-1}(t)]^T$, respectively. The dynamics of the ith following vehicle can be rewritten as

$$\dot{x}_i(t) = Ax_i(t) + Bu_i(t) + \omega_i(t), y_i(t) = Cx_i(t) \tag{2}$$

with

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -\frac{1}{\tau} \\ 0 & 1 & h & 0 \end{bmatrix}, B = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\tau} \\ 0 \end{bmatrix}, C = \begin{bmatrix} I & \mathbf{0} \end{bmatrix} \tag{3}$$

where the spacing error is denoted as $e_i^r(t) = l_i^r(t) - l_i(t)$, system matrices A, C are modeled with an observable condition, and C^T is given to be full column rank.

The leading vehicle (indexed as 0) only requires to send messages (position and velocity) to the cyber layer. Then, the dynamics of the ideal leading vehicle without external disturbance modeling can be rewritten as

$$\dot{x}_0(t) = Ax_0(t) + Bu_0(t), y_0(t) = Cx_0(t) \tag{4}$$

where $x_0(t) = [p_0(t)\ v_0(t)\ a_0(t)\ e_0^r(t)]^T, y_0 = [p_0(t)\ v_0(t)]^T$. The actual input of the leading vehicle is designed as $u_0(t) = -K_x x_0(t)$ with the designed state-feedback gain K_x in [12].

Assumption 2.1: The influence of the airflow, road surface, or vehicle uncertainty in the respective velocity and acceleration channels, namely, the external disturbance, is satisfied with an upper bound, i.e., $|d_i^v(t)| \le \bar{d}^v$ and $|d_i^a(t)| \le \bar{d}^a$.

B. Cyber-physical threat modeling

1) Complicated actuator fault modeling in physical layer: consider that the complicated actuator fault inevitably occurs with additive functions in the control input channels. Subsequently, the actual control input $u_i(t)$ contains two items, namely, the designed control input $u_i^d(t)$ and the complicated actuator fault modeling with fault parameters $\epsilon_i^f, \bar{f}_i$ and T_i^f,

$$u_i(t) = \begin{cases} u_i^d(t), t < T_i^f \\ u_i^d(t) + \left(1 - e^{-\epsilon_i^f(t - T_i^f)}\right)\bar{f}_i, t \ge T_i^f \end{cases} \tag{5}$$

where ϵ_i^f and $\bar{f}_i$ represent the fault decay rate and constant fault upper bound with intrinsic characteristics of system faults, and T_i^f denotes the fault occurring time instant of each vehicle. Notably, it indicates that the complicated actuator fault in the control input channel is denoted as the abrupt-type actuator fault (*quick decay rate with* $\epsilon_i^f \ge \bar{\epsilon}$) and incipient-type actuator fault (*slow decay rate with* $\underline{\epsilon} \le \epsilon_i^f < \bar{\epsilon}$), respectively.

Assumption 2.2: The distinguishing boundary values of the abrupt-type and incipient-type actuator faults and the healthy and faulty actuators in each input are ascertained manually in advance with the explicit positive scalars $\bar{\epsilon}$ and $\underline{\epsilon}$.

2) Connectivity-mixed attack modeling in cyber layer: connectivity-mixed attacks on the networked topology have two consequences by adding and removing communication links, forming a connectivity-preserving topology and a connectivity-broken topology respectively.

Connectivity-preserving topology (cyber-attacks *slightly* remove or increase the links between vehicles) still maintains connectivity, and contains a directed spanning tree rooted in the leader. The connectivity-broken topology (cyber-attacks *significantly* remove or increase the links between vehicles) becomes paralyzed and disconnected, but the broken connectivity can be restored through a repair mechanism. Under different connectivity-mixed attacks, a switching signal $s(t) : [0, \infty) \to \mathcal{S} = \{1, \cdots, h\}$ is created to connect each topology. The switching time series $t_k, k \in \mathbb{N}$ is defined over $[t_0, t)$. Suppose the non-overlapping and uniformly bounded intervals $[t_k, t_{k+1})$ of infinite sequences, where each switching topology is time-invariant with specific cyber-attacks.

A switching topology $\mathcal{G}_{s(t)}$ is a pair $(\nu, \varepsilon_{s(t)}, \mathcal{A}_{s(t)})$, where $\nu = \{\nu_1, \cdots, \nu_N\}$ is a nonempty finite set of nodes, $\varepsilon_{s(t)} \subseteq \nu \times \nu$ is a set of switching edges, and (ν_i, ν_j) is an edge that represents an ordered pair of nodes $\nu_i, \nu_j, i, j = 1, \cdots, N$. Adjacency matrix is denoted by $\mathcal{A}_{s(t)} = [a_{ij}^{s(t)}] \in \mathbb{R}^{N\times N}$, where $a_{ij}^{s(t)}$ is the weight coefficient of edge (ν_i, ν_j) and $a_{ii}^{s(t)} = 0, a_{ij}^{s(t)} > 0$ if $(\nu_i, \nu_j) \in \varepsilon_{s(t)}$; otherwise, $a_{ij}^{s(t)} = 0$. Laplacian matrix is denoted by $\mathcal{L}_{s(t)} = \mathcal{D}_{s(t)} - \mathcal{A}_{s(t)} = [l_{ij}^{s(t)}] \in \mathbb{R}^{N\times N}$, where $\mathcal{D}_{s(t)} = [d_{ii}^{s(t)}] \in \mathbb{R}^{N\times N}$ is a diagonal matrix with $d_{ii}^{s(t)} = \sum_{j=1}^{N} a_{ij}^{s(t)}$. The diagonal matrix of straight-through leader is denoted by $\mathcal{B}_{s(t)} = \mathrm{diag}\{b_1^{s(t)}, \cdots, b_N^{s(t)}\}$, where $b_i^{s(t)}$ is the information interaction between the leader and node ν_i. If $b_i^{s(t)} = 1$, node ν_i can access the leader via a directed path; otherwise, $b_i^{s(t)} = 0$. An information-exchange matrix is denoted by $\mathcal{H}_{s(t)} = \mathcal{L}_{s(t)} + \mathcal{B}_{s(t)}$. The set $\{\mathcal{G}_1, \cdots, \mathcal{G}_h\}$ denotes the switching topology $\mathcal{G}_{s(t)}$ and $\{\mathcal{H}_1, \cdots, \mathcal{H}_h\}$ denotes the information-exchange matrix $\mathcal{H}_{s(t)}$ for $s(t) \in \mathcal{S}$.

For the switching topologies $\{\mathcal{G}_1, \cdots, \mathcal{G}_q\}, \{\mathcal{G}_{q+1}, \cdots, \mathcal{G}_h\}$ under connectivity-mixed attacks, the switching signal $s(t)$ is modeled as $s(t) \in \mathcal{S} = \mathcal{S}_p \cup \mathcal{S}_b = \{1, \cdots, q, q+1, \cdots, h\}, h \geq 2$, where $\mathcal{S}_p$ and $\mathcal{S}_b$ are the set of q connectivity-preserving and (h-q) connectivity-broken topologies, respectively. Denote $N_{\mathcal{S}}(t_0, t) = N_{\mathcal{S}_p}(t_0, t) + N_{\mathcal{S}_b}(t_0, t), \forall t > t_0 \geq 0$ as the activation number of connectivity-mixed attacks for the switching signal $s(t) \in \mathcal{S}$ over $[t_0, t)$, where $N_{\mathcal{S}_p}(t_0, t)$ and $N_{\mathcal{S}_b}(t_0, t)$ denote the activation numbers of the connectivity-preserving and connectivity-broken topologies, respectively. Then, the total activation durations of topologies that maintain connectivities and break connectivities over $[t_0, t)$ are denoted as $T_p(t_0, t)$ and $T_b(t_0, t)$ as follows,

$$T_{p(b)}(t_0, t) = \textstyle\sum_{k\in\mathbb{N}, s(t_k)\in\mathcal{S}_{p(b)}} (t_{k+1} - t_k) \tag{6}$$

Here, two metrics of connectivity-mixed attacks, i.e., attack activation rate and attack frequency are defined as follows.

Definition 2.1 (attack activation rate): Denote $\mathcal{R}_{\mathcal{S}_p}(t_0, t)$ for $s(t) \in \mathcal{S}_p$ and $\mathcal{R}_{\mathcal{S}_b}(t_0, t)$ for $s(t) \in \mathcal{S}_b$ as the connectivity-preserving and connectivity-broken activation rates over $[t_0, t)$,

$$\mathcal{R}_{\mathcal{S}_{p(b)}}(t_0, t) = \frac{T_{p(b)}(t_0,t)}{t-t_0} \tag{7}$$

Definition 2.2 (attack frequency): Let $\mathcal{F}_{\mathcal{S}}(t_0, t)$ for $s(t) \in \mathcal{S}$ be the connectivity-mixed attack frequency over $[t_0, t)$,

$$\mathcal{F}_{\mathcal{S}}(t_0, t) = \frac{N_{\mathcal{S}_p}(t_0,t)+N_{\mathcal{S}_b}(t_0,t)}{t-t_0} \tag{8}$$

C. Problem formulation

The main objectives of this study can be listed as follows. i) To ensure the reliable communication and safe travelling of vehicle platoon systems under cyber-physical threats, the proposed control framework should maintain the desired spacing gap $l_i(t)$ between two neighboring vehicles to avoid vehicle collisions. ii) The exponential leader-following tracking control issue of the modeled vehicle platoon systems (2) and (4) is addressed via a distributed anti-attack FTTC strategy if for $\forall t \geq t_0$, there exist positive scalars, i.e., the amplitude $\mu > 0$ and decay rate $\rho > 0$ such that

$$\|x_i(t) - x_0(t)\|^2 \leq \mu e^{-\rho(t-t_0)} \|x_i(t_0) - x_0(t_0)\|^2 \tag{9}$$

Lemma 2.1 [12]: The symmetric positive definite matrix is denoted by $\Upsilon_{s(t)}\mathcal{H}_{s(t)} + \mathcal{H}_{s(t)}^T\Upsilon_{s(t)}, s(t) \in \mathcal{S}$, where $\Upsilon_{s(t)} = \mathrm{diag}\{\varphi_{s(t),1}^{-1}, \cdots, \varphi_{s(t),N}^{-1}\}$ is diagonal positive definite with each element $\varphi_{s(t),i}, i = 1, \cdots, N$ of matrix $\varphi_{s(t)} = \mathcal{H}_{s(t)}^{-T} 1_N$, where the vector is denoted by $1_N = [1 \cdots 1]^T$.

Remark 2.1: (i) In open and dynamic vehicle driving environments and under weakly connected network conditions, the connected topology of vehicle platoon systems is vulnerable to connectivity-mixed attacks (link-break failures). Malicious attackers attempt to block efficient information transmission between vehicles, ultimately leading to broken communication connections and poor spacing tracking performance of vehicle platoon systems. Distinguishing from deception attacks [19], actuator/sensor attacks [20] and DoS attacks [22], this study addresses cyber security vulnerabilities, and identifies and classifies cyber-physical threats in vehicle platoon systems, in particular by modeling connectivity-preserving attacks with a directed spanning tree and connectivity-broken attacks without a spanning tree. (ii) It is also assumed that topologies under connectivity-mixed attacks are resilient and recoverable, and that topology switching can be detected by some intelligent anti-attack devices. Meanwhile, the unified bounds on attack frequency $\mathcal{F}_{\mathcal{S}}(t_0, t)$ and attack activation rates $\mathcal{R}_{\mathcal{S}_{p(b)}}(t_0, t)$ are preset to achieve an exponential leader-following tracking control performance of vehicle platoon systems.

III. Main results

In this section, Fig. 1 consists mainly of the vehicle platoon systems suffered from complicated actuator faults in physical layer and the switching topologies affected by connectivity-mixed attacks in cyber layer. Furthermore, the control framework containing the decentralized fault-estimation UIO design and the distributed anti-attack FTTC design is proposed for the modeled vehicle platoon systems under cyber-physical threats.

A. Decentralized fault-estimation UIO design under complicated actuator faulty scenario

Notably, the complicated abrupt- and incipient-type actuator faults are smooth and differentiable after the fault occurring instant $t \geq T_i^f$. Then, it is feasible to denote the augmented state

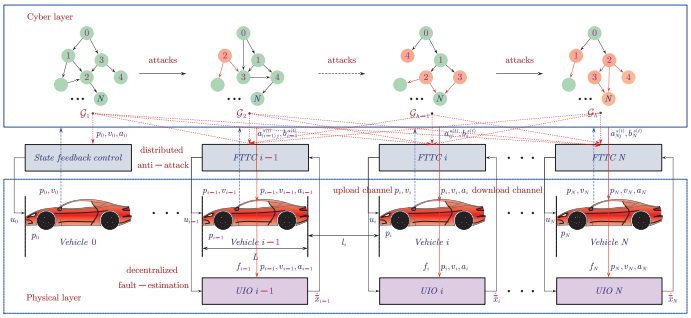

Fig. 1. Decentralized fault-estimation UIO and distributed anti-attack FTTC of vehicle platoon systems under cyber-physical threats.

as $\bar{x}_i(t) = [x_i^T(t)\ (1 - e^{-\epsilon_i^f (t-T_i^f)})\bar{f}_i]^T$ with an internal fault description $f_i(t) = (1 - e^{-\epsilon_i^f (t-T_i^f)})\bar{f}_i$ and further denote the augmented uncertainty as $\bar{\omega}_{fi}(t) = [\omega_i^T(t)\ \epsilon_i^f e^{-\epsilon_i^f (t-T_i^f)}\bar{f}_i]^T$.

Subsequently, the augmented dynamics of the ith following vehicle with the differentiable fault $f_i(t)$ are established as

$$\begin{cases} \dot{\bar{x}}_i(t) = \bar{A}\bar{x}_i(t) + \bar{B}u_i^d(t) + \bar{\omega}_{fi}(t) \\ y_i(t) = \bar{C}\bar{x}_i(t) \end{cases} \tag{10}$$

with the following augmented system matrices,

$$\bar{A} = \begin{bmatrix} A & B \\ \mathbf{0}_{1\times 4} & 0 \end{bmatrix}, \bar{B} = \begin{bmatrix} B \\ 0 \end{bmatrix}, \bar{C} = \begin{bmatrix} C & \mathbf{0}_{2\times 1} \end{bmatrix} \tag{11}$$

In order to estimate the unavailable state and fault information of vehicle platoon systems under complicated actuator faulty scenario, the UIO of the decentralized fault-estimation scheme is developed considering the dispersed structure and single-flow feature. The characteristic of a decentralized single stream is that the UIO design only requires the signal available for each vehicle and simultaneously blocks information from other observers within physical distances. Then, the decentralized fault-estimation UIO expression for the augmented dynamics (10) is designed as follows

$$\begin{cases} \dot{z}_i(t) = Mz_i(t) + J\bar{C}\bar{x}_i(t) + Gu_i^d(t) \\ \hat{\bar{x}}_i(t) = z_i(t) + H\bar{C}\bar{x}_i(t) \end{cases} \tag{12}$$

where $z_i(t)$ represents the state of the decentralized UIO, and $\hat{\bar{x}}_i(t) = [\hat{x}_i^T(t)\ \hat{f}_i^T(t)]^T$ represents the estimation of $\bar{x}_i(t) = [x_i^T(t)\ (1-e^{-\epsilon_i^f (t-T_i^f)})\bar{f}_i]^T$, where $\hat{x}_i(t)$ is the state estimation of $x_i(t)$ and $\hat{f}_i(t)$ is the fault estimation of $f_i(t)$ instead of hyper-parameters in fault description. Matrices M, G, J and H are devised with proper dimensions.

Denote the estimation error as $\tilde{e}_i(t) = \bar{x}_i(t) - \hat{\bar{x}}_i(t) = [e_{xi}^T(t)\ e_{f_i}^T(t)]^T$ with the state estimation error $e_{xi}(t) = x_i(t) - \hat{x}_i(t)$ and the fault estimation error $e_{f_i}(t) = f_i(t) - \hat{f}_i(t)$. Hence, the ith estimation error dynamics are formulated as

$$\begin{aligned} \dot{\tilde{e}}_i(t) = &\left(\Theta\bar{A} - J_1\bar{C}\right)\tilde{e}_i(t) + \left(\Theta\bar{B} - G\right)u_i^d(t) \\ &+ \left(\left(\Theta\bar{A} - J_1\bar{C}\right)H - J_2\right)\bar{C}\bar{x}_i(t) + \Theta\bar{\omega}_{fi}(t) \\ &+ \left(\Theta\bar{A} - J_1\bar{C} - M\right)\left(\hat{\bar{x}}_i(t) - H\bar{C}\bar{x}_i(t)\right) \end{aligned} \tag{13}$$

where $\Theta = I - H\bar{C}$ and $J = J_1 + J_2$.

In order to decouple the introduced items $u_i^d(t), \bar{x}_i(t)$ and $\hat{\bar{x}}_i(t)$ from the estimation error dynamics (13), the equality condition of Hurwitz matrix M and matrices G, J_1, J_2, Θ and H are formed as follows

$$\begin{cases} \Theta\bar{A} - J_1\bar{C} = M \\ \left(\Theta\bar{A} - J_1\bar{C}\right)H = J_2 \\ \Theta\bar{B} = G \end{cases} \tag{14}$$

Subsequently, the estimation error systems are rewritten as

$$\dot{\tilde{e}}_i(t) = \left(\Theta\bar{A} - J_1\bar{C}\right)\tilde{e}_i(t) + \Theta\bar{\omega}_{fi}(t) \tag{15}$$

and the global estimation error systems are given as

$$\dot{\tilde{e}}(t) = (I_N \otimes (\Theta\bar{A} - J_1\bar{C}))\tilde{e}(t) + (I_N \otimes \Theta)\bar{\omega}_f(t) \tag{16}$$

where global vectors $\tilde{e}(t) = [\tilde{e}_1^T(t), \cdots, \tilde{e}_N^T(t)]^T$ and $\bar{\omega}_f(t) = [\bar{\omega}_{f1}^T(t), \cdots, \bar{\omega}_{fN}^T(t)]^T$, and $\otimes$ is the Kronecker product.

Remark 3.1: (i) The Hurwitz characteristic of the M-matrix allows the robustness and asymptotic stability of the estimation error systems (15) and (16). The presence of two solvable matrices H and J_1 makes the solution of the corresponding UIO gains M, G and J in the decentralized fault-estimation design (12) under the equation constraints (14) more intuitive and efficient, i.e., $M = (I_5 - H\bar{C})\bar{A} - J_1\bar{C}, G = (I_5 - H\bar{C})\bar{B}$ and $J = J_1 + ((I_5 - H\bar{C})\bar{A} - J_1\bar{C})H$. (ii) Non-differential dilemmas resulting from intermittent points in the timing instants of complicated abrupt time-varying actuator faults can be fitted with differentiable approximation functions, including but not limited to the hyperbolic tangent function.

B. Distributed anti-attack FTTC design under cyber-physical threatened scenario

The ith distributed anti-attack FTTC design of the vehicle platoon systems under cyber-physical threatened scenario, i.e., the complicated actuator fault $f_i(t) = (1 - e^{-\epsilon_i^f (t-T_i^f)})\bar{f}_i$ in physical layer and connectivity-mixed attacks ($s(t) \in \mathcal{S} = \mathcal{S}_p \cup \mathcal{S}_b$) is devised with an intensive combination of physical fault tolerance items and anti-attack consensus tracking items,

$$\begin{aligned} u_i^d(t) = &\overbrace{-K_x\hat{x}_i(t) - \hat{f}_i(t)}^{\text{physical fault tolerance}} \\ &\underbrace{+\gamma K\left(\sum_{j=1}^{N} a_{ij}^{s(t)}\left(y_j(t) - y_i(t)\right) + b_i^{s(t)}\left(y_0(t) - y_i(t)\right)\right)}_{\text{anti-attack consensus tracking}} \end{aligned} \tag{17}$$

where γ is a positive scalar and K represents an anti-attack consensus tracking gain matrix.

Denote a state platoon tracking error as $e_i(t) = x_i(t) - x_0(t)$. Then, with the help of the distributed anti-attack FTTC scheme (17), the corresponding state platoon tracking error dynamics are derived as follows

$$\begin{aligned} \dot{e}_i(t) = &\left(A - BK_x\right)e_i(t) + B\left[K_x\ I\right]\tilde{e}_i(t) + \omega_i(t) \\ &+\gamma BK\left(\textstyle\sum_{j=1}^{N} a_{ij}^{s(t)}\left(y_j(t) - y_i(t)\right)\right) \\ &+\gamma BK\left(b_i^{s(t)}\left(y_0(t) - y_i(t)\right)\right) \end{aligned} \tag{18}$$

and the global state platoon tracking error systems are

$$\begin{aligned} \dot{e}(t) = &\left(I_N \otimes (A - BK_x) - \gamma(\mathcal{H}_{s(t)} \otimes BKC)\right)e(t) \\ &+ (I_N \otimes B\left[K_x\ I\right])\tilde{e}(t) + \omega(t) \end{aligned} \tag{19}$$

where $e(t) = [e_1^T(t), \cdots, e_N^T(t)]^T, \omega(t) = [\omega_1^T(t), \cdots, \omega_N^T(t)]$, and $\mathcal{H}_{s(t)} = \mathcal{L}_{s(t)} + \mathcal{B}_{s(t)}$ is the information-exchange matrix.

This study aims to devise the decentralized fault-estimation UIO and distributed anti-attack FTTC co-design such that the exponential leader-following tracking control problem with the desired spacing of the vehicle platoon systems can be addressed. The following sufficient condition is given for vehicle platoon systems under cyber-physical threatened scenario, i.e., the complicated abrupt-type and incipient-type actuator faults in physical layer and connectivity-mixed attacks in cyber layer.

Theorem 3.1: Consider the leader-following vehicle platoon systems (2) and (4) under cyber-physical threats. Given positive scalars $\chi_1, \chi_2, \chi_3, \chi_4, \bar{\gamma}$ and $\sigma_{\mathcal{S}}$, a distributed anti-attack FTTC strategy (17) with the consensus tracking gain $K = B^T P^{-1}(C^T C)^{-1} C^T$ can achieve the exponential leader-following tracking control performance and the desired inter-vehicle spacing to avoid collision phenomena, if there exists a symmetric positive-definite matrix P, matrices K_x, H, J_1 and positive scalars ϱ_1, ϱ_2 such that

$$(A - BK_x)P + P(A - BK_x)^T + \lambda_{\max}(\Upsilon_{s(t)}^2)\bar{\varphi} I < -\chi_1 P \tag{20}$$

$$(A - BK_x)P + P(A - BK_x)^T + I + (1 - \bar{\gamma})BB^T < \chi_2 P \tag{21}$$

$$\begin{bmatrix} \frac{1}{\varrho_1}\Omega_{11} + K_x^T K_x + \chi_3 I & \frac{1}{\varrho_1}\Omega_{12} + K_x^T \\ \star & \frac{1}{\varrho_1}\Omega_{22} + \frac{1+\varrho_1+\varrho_1\chi_3}{\varrho_1} I \end{bmatrix} \tag{22}$$

$$\varrho_2 \leq \varrho_1 \left(2\underline{\varphi} - \chi_3 \varrho_1\right) \tag{23}$$

where $\bar{\varphi} = \max_{i=1,\cdots,N} \varphi_{s(t),i}$ for $s(t) \in \mathcal{S}_p$, $\Omega_{11} = (A - H_1 CA - J_{11}C) + (A - H_1 CA - J_{11}C)^T + (I - H_1 C)(I - H_1 C)^T, \Omega_{12} = B - H_1 CB - A^T C^T H_2^T - C^T J_{12}^T - (I - H_1 C)C^T H_2^T$, and $\Omega_{22} = -H_2 CB - B^T C^T H_2^T + H_2 C(H_2 C)^T$ with $H = [H_1^T \ H_2^T]^T$ and $J_1 = [J_{11}^T \ J_{12}^T]^T$.

Furthermore, the positive scalar γ in the distributed anti-attack FTTC scheme (17) for $s(t) \in \mathcal{S}$ is constrained within the upper and lower bounds as follows

$$\frac{\lambda_{\max}(\Upsilon_{s(t)}^2)}{\lambda_{\min}(\Upsilon_{s(t)}\mathcal{H}_{s(t)} + \mathcal{H}_{s(t)}^T \Upsilon_{s(t)})} \leq \gamma \leq \frac{\bar{\gamma}}{\lambda_{\min}(\mathcal{H}_{s(t)} + \mathcal{H}_{s(t)}^T)} \tag{24}$$

For a positive decay rate $\rho_{\mathcal{S}} \in (0, \rho^\star)$ with the chosen constant $\rho^\star \in (0, \eta_p)$ and $\eta_p > 0$, the connectivity-mixed attack frequency $\mathcal{F}_{\mathcal{S}}(t_0, t)$ satisfies with the following form

$$\mathcal{F}_{\mathcal{S}}(t_0, t) \leq \frac{\rho^\star - \rho_{\mathcal{S}}}{\ln \bar{\xi} + \ln\left(\frac{\bar{\varphi}}{\underline{\varphi}}\right)} \tag{25}$$

and each connectivity-preserving and connectivity-broken activation rates $\mathcal{R}_{\mathcal{S}_p}(t_0, t)$ and $\mathcal{R}_{\mathcal{S}_b}(t_0, t)$ over $[t_0, t)$ yield to

$$\mathcal{R}_{\mathcal{S}_p}(t_0, t) \geq \frac{\eta_b + \rho^\star}{\eta_p + \eta_b}, \mathcal{R}_{\Gamma_b}(t_0, t) \leq \frac{\eta_p - \rho^\star}{\eta_p + \eta_b} \tag{26}$$

where $\eta_p = \min(\chi_1, \chi_3 \varrho_1), \eta_b = \max(\chi_2, \chi_4 \varrho_1), \bar{\xi} = (1 + h^2)\bar{d}_i^{v^2} + \bar{d}_i^{a^2} + \bar{d}$ with the chosen scalar $\bar{d} > 0$, and $\underline{\varphi} = \min_{i=1,\cdots,N} \varphi_{s(t),i}$ for $s(t) \in \mathcal{S}_p$.

Hence, the exponential leader-following tracking problem of the vehicle platoon systems under cyber-physical threats is solved with the derived state platoon tracking error,

$$\|e_i(t)\|^2 \leq \mu_{\mathcal{S}} e^{-\rho_{\mathcal{S}}(t - t_0)} \|e_i(t_0)\|^2 \tag{27}$$

with the following amplitude $\mu_{\mathcal{S}}$ expressed as

$$\mu_{\mathcal{S}} = \frac{\left(\max\{\lambda_{\max}(\varphi_{s(t),i}^{-1} P^{-1}), \lambda_{\max}(P^{-1})\} + \sigma_{\mathcal{S}}\right)\bar{\xi}}{\min\left\{\lambda_{\min}(\varphi_{s(t),i}^{-1} P^{-1}), \lambda_{\min}(P^{-1})\right\}} \tag{28}$$

Proof. Consider a piece-wise Lyapunov function candidate $V_1(t)$ containing $V_1^p(t)$ for $s(t) \in \mathcal{S}_p$ and $V_1^b(t)$ for $s(t) \in \mathcal{S}_b$,

$$V_1(t) = \begin{cases} V_1^p(t) = \sum_{i=1}^N e_i^T(t) \varphi_{s(t),i}^{-1} P^{-1} e_i(t), s(t) \in \mathcal{S}_p \\ V_1^b(t) = \sum_{i=1}^N e_i^T(t) P^{-1} e_i(t), s(t) \in \mathcal{S}_b \end{cases} \tag{29}$$

where matrix P is symmetric and positive definite, and $\varphi_{s(t),i}^{-1}$ is the ith component of the diagonal positive definite matrix $\Upsilon_{s(t)}$ for $i = 1, \cdots, N$ and $s(t) \in \mathcal{S}_p$ in Lemma 2.1.

Denote the anti-attack consensus tracking gain matrix as $K = B^T P^{-1}(C^T C)^{-1} C^T$, and the derivative of the Lyapunov candidate $V_1^p(t)$ for $s(t) \in \mathcal{S}_p$ under connectivity-preserving topologies is obtained as

$$\begin{aligned} \dot{V}_1^p(t) &= \sum_{i=1}^N \mathcal{E}_i^T \varphi_{s(t),i}^{-1} \left((A - BK_x)P + P(A - BK_x)^T\right) \mathcal{E}_i \\ &\quad + 2\sum_{i=1}^N \mathcal{E}_i^T \varphi_{s(t),i}^{-1} B[K_x \ I]\tilde{e}_i + 2\sum_{i=1}^N \mathcal{E}_i^T \varphi_{s(t),i}^{-1} \omega_i \\ &\quad + 2\gamma \sum_{i=1}^N \mathcal{E}_i^T \varphi_{s(t),i}^{-1} BB^T (\sum_{j=1}^N a_{ij}^{s(t)} (\mathcal{E}_j - \mathcal{E}_i) - b_i^{s(t)} \mathcal{E}_i) \\ &= \mathcal{E}^T \left(\Upsilon_{s(t)} \otimes \left((A - BK_x)P + P(A - BK_x)^T\right)\right) \mathcal{E} \\ &\quad - \gamma \mathcal{E}^T \left((\Upsilon_{s(t)} \mathcal{H}_{s(t)} + \mathcal{H}_{s(t)}^T \Upsilon_{s(t)}) \otimes BB^T\right) \mathcal{E} \\ &\quad + 2\sum_{i=1}^N \mathcal{E}_i^T \varphi_{s(t),i}^{-1} B[K_x \ I]\tilde{e}_i + 2\sum_{i=1}^N \mathcal{E}_i^T \varphi_{s(t),i}^{-1} \omega_i \\ &\leq \mathcal{E}^T (\Upsilon_{s(t)} \otimes ((A - BK_x)P + P(A - BK_x)^T \\ &\quad + \lambda_{\max}(\Upsilon_{s(t)}^2) \bar{\varphi} I)) \mathcal{E} + \tilde{e}^T (I_N \otimes \mathcal{K}) \tilde{e} + \omega^T \omega \end{aligned} \tag{30}$$

where $\mathcal{E}_i = P^{-1} e_i$ is each element of $\mathcal{E} = [\mathcal{E}_1^T, \cdots, \mathcal{E}_N^T]^T$ for convenience, $\mathcal{K} = [K_x^T K_x \quad K_x^T; K_x \quad I]$, $\bar{\varphi} = \max \varphi_{s(t),i}, i = 1. \cdots, N$, and the positive scalar in the distributed anti-attack FTTC design is constrained within $\gamma \geq \frac{\lambda_{\max}(\Upsilon_{s(t)}^2)}{\lambda_{\min}(\Upsilon_{s(t)}\mathcal{H}_{s(t)} + \mathcal{H}_{s(t)}^T \Upsilon_{s(t)})}$ for $s(t) \in \mathcal{S}_p$ from (24).

Then, the first-order derivative of the Lyapunov candidate $V_1^b(t)$ for $s(t) \in \mathcal{S}_b$ is obtained as

$$\begin{aligned} \dot{V}_1^b(t) &\leq \mathcal{E}^T \left(I_N \otimes \left((A - BK_x)P + P(A - BK_x)^T + I\right)\right) \mathcal{E} \\ &\quad - \gamma \mathcal{E}^T \left((\mathcal{H}_{s(t)} + \mathcal{H}_{s(t)}^T) \otimes BB^T\right) \mathcal{E} \\ &\quad + 2\mathcal{E}^T \left(I_N \otimes B[K_x \ I]\right) \tilde{e} + \omega^T \omega \\ &\leq \mathcal{E}^T (I_N \otimes ((A - BK_x)P + P(A - BK_x)^T + I \\ &\quad + (1 - \bar{\gamma})BB^T)) \mathcal{E} + \tilde{e}^T (I_N \otimes \mathcal{K}) \tilde{e} + \omega^T \omega \end{aligned} \tag{31}$$

where $\bar{\gamma} \geq \gamma \lambda_{\min}(\mathcal{H}_{s(t)} + \mathcal{H}_{s(t)}^T)$ for $s(t) \in \mathcal{S}_b$ from (24).

Consider the Lyapunov candidate $V_2(t)$ containing the estimation error and the derivative of complicated actuator fault,

$$V_2(t) = \frac{1}{\varrho_1} \sum_{i=1}^N \tilde{e}_i^T(t) \tilde{e}_i(t) + \frac{1}{\varrho_2} \sum_{i=1}^N [e_i^f e^{-\epsilon_i^f (t - T_i^f)} \bar{f}_i]^2 \tag{32}$$

where ϱ_1 and ϱ_2 are positive constants.

The complicated abrupt-type and incipient-type actuator faults in input channel of vehicle platoon systems in physical

layer are modelled with exponential changing features. Then, the derivative of the Lyapunov candidate $V_2(t)$ is obtained as

$$\begin{aligned}\dot{V}_2(t) &= \tfrac{2}{\varrho_1}\textstyle\sum_{i=1}^{N}\tilde{e}_i^T(t)\left((\Theta\bar{A}-J_1\bar{C})\tilde{e}_i(t)+\Theta\bar{\omega}_i(t)\right)\\ &\quad+\tfrac{2}{\varrho_2}\textstyle\sum_{i=1}^{N}(\epsilon_i^f e^{-\epsilon_i^f(t-T_i^f)}\bar{f}_i)(-(\epsilon_i^f)^2e^{-\epsilon_i^f(t-T_i^f)}\bar{f}_i)\\ &\le \tfrac{1}{\varrho_1}\textstyle\sum_{i=1}^{N}\tilde{e}_i^T(t)((\Theta\bar{A}-J_1\bar{C})+(\Theta\bar{A}-J_1\bar{C})^T\\ &\quad+\Theta\Theta^T)\tilde{e}_i(t)+\tfrac{1}{\varrho_1}\omega^T(t)\omega(t)\\ &\quad+\textstyle\sum_{i=1}^{N}\left(\tfrac{1}{\varrho_1}-\tfrac{2\epsilon_{\min}}{\varrho_2}\right)[\epsilon_i^f e^{-\epsilon_i^f(t-T_i^f)}\bar{f}_i]^2\end{aligned} \tag{33}$$

where $\epsilon_{\min}=\min\epsilon_i^f, i=1,\cdots,N$.

Denote the new Lyapunov candidate as $V(t,s(t))=V_1(t)+V_2(t)$. According to the inequality constraints (20) and (21), $(A-BK_x)^TP+P(A-BK_x)^T+\lambda_{\max}(\Upsilon_{s(t)}^2)\bar{\varphi}I+\chi_1P<0$ and $(A-BK_x)P+P(A-BK_x)^T+I+(1-\bar{\gamma})BB^T-\chi_2P<0$ are derived with the chosen scalars $\chi_1>0$ and $\chi_2>0$. Then, the derivative of the considered new Lyapunov candidate is derived via $\frac{1}{\varrho_1}((\Theta\bar{A}-J_1\bar{C})+(\Theta\bar{A}-J_1\bar{C})^T+\Theta\Theta^T)+\mathcal{K}+\chi_3I<0$ from (22) as follows

$$\begin{aligned}&\dot{V}(t,s(t))\mid s(t)\in\mathcal{S}_p=\dot{V}_1^p(t)+\dot{V}_2(t)\\ &<-\chi_1\mathcal{E}^T(t)\left(\Upsilon_{\gamma(t)}\otimes P\right)\mathcal{E}(t)-\chi_3\tilde{e}^T(t)\tilde{e}(t)\\ &\quad+\tfrac{1+\varrho_1}{\varrho_1}\omega^T(t)\omega(t)+\textstyle\sum_{i=1}^{N}\left(\tfrac{1}{\varrho_1}-\tfrac{2\epsilon_{\min}}{\varrho_2}\right)[\epsilon_i^f e^{-\epsilon_i^f(t-T_i^f)}\bar{f}_i]^2\\ &=-\chi_1V_1^p(t)-\chi_3\varrho_1V_2(t)+\tfrac{1+\varrho_1}{\varrho_1}\omega^T(t)\omega(t)\\ &\quad+\textstyle\sum_{i=1}^{N}\left(\tfrac{\chi_3\varrho_1}{\varrho_2}+\tfrac{1}{\varrho_1}-\tfrac{2\epsilon_{\min}}{\varrho_2}\right)[\epsilon_i^f e^{-\epsilon_i^f(t-T_i^f)}\bar{f}_i]^2\\ &<-\min\left(\chi_1,\chi_3\varrho_1\right)V(t,s(t))+\tfrac{1+\varrho_1}{\varrho_1}\omega^T(t)\omega(t)\end{aligned} \tag{34}$$

$$\begin{aligned}&\dot{V}(t,s(t))\mid s(t)\in\mathcal{S}_b=\dot{V}_1^b(t)+\dot{V}_2(t)\\ &<\chi_2\mathcal{E}^T(t)\left(I_N\otimes P\right)\mathcal{E}(t)+\chi_4\tilde{e}^T(t)\tilde{e}(t)\\ &\quad+\tfrac{1+\varrho_1}{\varrho_1}\omega^T(t)\omega(t)+\textstyle\sum_{i=1}^{N}\left(\tfrac{1}{\varrho_1}-\tfrac{2\epsilon_{\min}}{\varrho_2}\right)[\epsilon_i^f e^{-\epsilon_i^f(t-T_i^f)}\bar{f}_i]^2\\ &<\max\left(\chi_2,\chi_4\varrho_1\right)V(t,s(t))+\tfrac{1+\varrho_1}{\varrho_1}\omega^T(t)\omega(t)\end{aligned} \tag{35}$$

where $\frac{\chi_3\varrho_1}{\varrho_2}+\frac{1}{\varrho_1}-\frac{2\epsilon_{\min}}{\varrho_2}\le 0$ and $-\frac{\chi_4\varrho_1}{\varrho_2}+\frac{1}{\varrho_1}-\frac{2\epsilon_{\min}}{\varrho_2}\le 0$ are satisfied under the scalar inequality constraint $\varrho_2\le\varrho_1(2\underline{\epsilon}-\chi_3\varrho_1)$ with the positive scalars $\underline{\epsilon}>0$ and $\chi_2>0$ from (23). Furthermore, $\chi_4>0$ is selected under the derived matrix condition $\frac{1}{\varrho_1}((\Theta\bar{A}-J_1\bar{C})+(\Theta\bar{A}-J_1\bar{C})^T+\Theta\Theta^T)+\mathcal{K}-\chi_4I<0$.

Integrating both left and right items of $\dot{V}(t,s(t))$ in (34) and (35) over $t\in[t_k,t_{k+1})$, and it follows that

$$V(t,s(t))<\begin{cases}\xi e^{-\eta_p(t-t_k)}V(t_k,s(t_k))+\frac{\xi}{\eta_p}, s(t)\in\mathcal{S}_p\\ \xi e^{\eta_b(t-t_k)}V(t_k,s(t_k))-\frac{\xi}{\eta_b}, s(t)\in\mathcal{S}_b\end{cases} \tag{36}$$

where $\eta_p=\min(\chi_1,\chi_3\varrho_1),\eta_b=\max(\chi_2,\chi_4\varrho_1)$ and $\xi=\frac{1+\varrho_1}{\varrho_1}\omega^T(t)\omega(t)$.

Therefore, it follows from $s(t)\in\mathcal{S}=\mathcal{S}_p\cup\mathcal{S}_b$ that

$$V(t,s(t))<\bar{\xi}e^{\eta_bT_b(t_k,t)-\eta_pT_p(t_k,t)}V(t_k,s(t_k)) \tag{37}$$

where $T_p(t_k,t)$ and $T_b(t_k,t)$ denote the total activation durations of topologies that preserve and break connectivities over $[t_k,t)$, respectively, and $\bar{\xi}=(1+h^2)\bar{d}_i^{v^2}+\bar{d}_i^{a^2}+\bar{d}$ with the selected positive scalar $\bar{d}$.

Since $\underline{\varphi}V_1^p(t)\le V_1^b(t)\le\overline{\varphi}V_1^p(t)$ is satisfied, where $\underline{\varphi}=\min\varphi_{s(t),i}$ and $\overline{\varphi}=\max\varphi_{s(t),i}, s(t)\in\mathcal{S}_p, i=1,\cdots,N$. Subsequently, $V(t_k,s(t_k))\le\frac{\overline{\varphi}}{\underline{\varphi}}V(t_k^-,s(t_k^-))$ is obtained at each switching instant t_k. Thus, the new Lyapunov function $V(t,s(t))$ is derived as follows

$$\begin{aligned}&V(t,s(t))<\bar{\xi}e^{\eta_bT_b(t_k,t)-\eta_pT_p(t_k,t)}\tfrac{\overline{\varphi}}{\underline{\varphi}}V(t_k^-,s(t_k^-))\\ &<\cdots<\bar{\xi}^{k+1}e^{\eta_bT_b(t_0,t)-\eta_pT_p(t_0,t)}\left(\tfrac{\overline{\varphi}}{\underline{\varphi}}\right)^kV(t_0,s(t_0))\\ &\le\bar{\xi}e^{N_{\mathcal{S}}(t_0,t)(\ln\bar{\xi}+\ln(\frac{\overline{\varphi}}{\underline{\varphi}}))+\eta_bT_b(t_0,t)-\eta_pT_p(t_0,t)}V(t_0)\end{aligned} \tag{38}$$

where $k=N_{\mathcal{S}}(t_0,t)$ denotes the activation number of the connectivity-mixed attacks and $V(t_0)$ denotes the initial Lyapunov candidate for the switching signal $s(t_0)$.

According to the two metrics of connectivity-mixed attacks, i.e., the activation rates $\mathcal{R}_{\mathcal{S}_p}(t_0,t),\mathcal{R}_{\mathcal{S}_b}(t_0,t)$ and the attack frequency $\mathcal{F}_{\mathcal{S}}(t_0,t)$ are constrained within (25) and (26), $N_{\mathcal{S}}(t_0,t)(\ln\bar{\xi}+\ln(\frac{\overline{\varphi}}{\underline{\varphi}}))+\eta_bT_b(t_0,t)-\eta_pT_p(t_0,t)\le-\rho_{\mathcal{S}}(t-t_0)$ is finally achieved with help of $N_{\mathcal{S}}(t_0,t)(\ln\bar{\xi}+\ln(\frac{\overline{\varphi}}{\underline{\varphi}}))\le(\rho^\star-\rho_{\mathcal{S}})(t-t_0)$ and $\eta_bT_b(t_0,t)-\eta_pT_p(t_0,t)\le-\rho^\star(t-t_0)$, where the decay rate $\rho_{\mathcal{S}}\in(0,\rho^\star),\rho^\star\in(0,\eta_p)$ and $\eta_p>0$. Subsequently, it follows that $V(t,s(t))<\bar{\xi}e^{-\rho_{\mathcal{S}}(t-t_0)}V(t_0)$.

With the definition of the new Lyapunov function $V(t,s(t))$, the initial Lyapunov candidate $V(t_0)$ is also constrained within

$$\begin{aligned}&V(t_0)\le\max\left\{\lambda_{\max}(\varphi_{s(t),i}^{-1}P^{-1}),\lambda_{\max}(P^{-1})\right\}\\ &\times\textstyle\sum_{i=1}^{N}\|e_i(t_0)\|^2+\frac{\max\limits_{i=1,\cdots,N}\left(\frac{1}{\varrho_1}\|\tilde{e}_i(t_0)\|^2\right)}{\min\limits_{i=1,\cdots,N}\|e_i(t_0)\|^2}\textstyle\sum_{i=1}^{N}\|e_i(t_0)\|^2\end{aligned} \tag{39}$$

Define $\Gamma_{\mathcal{S}}=\max\{\lambda_{\max}(\varphi_{s(t),i}^{-1}P^{-1}),\lambda_{\max}(P^{-1})\}+\sigma_{\mathcal{S}}$,

$$\begin{aligned}&\min\left\{\lambda_{\min}(\varphi_{s(t),i}^{-1}P^{-1}),\lambda_{\min}(P^{-1})\right\}\textstyle\sum_{i=1}^{N}\|e_i(t)\|^2\\ &\le V(t,s(t))\le\bar{\xi}\Gamma_{\mathcal{S}}e^{-\rho_{\mathcal{S}}(t-t_0)}\textstyle\sum_{i=1}^{N}\|e_i(t_0)\|^2\end{aligned} \tag{40}$$

This indicates that with a positive decay rate $\rho_{\mathcal{S}}$ and an appropriate scalar $\sigma_{\mathcal{S}}$, the exponential leader-following state platoon tracking error yields

$$\begin{aligned}\|e_i(t)\|^2&\le\frac{\Gamma_{\mathcal{S}}\bar{\xi}e^{-\rho_{\mathcal{S}}(t-t_0)}\|e_i(t_0)\|^2}{\min\left\{\lambda_{\min}(\varphi_{s(t),i}^{-1}P^{-1}),\lambda_{\min}(P^{-1})\right\}}\\ &\le\mu_{\mathcal{S}}e^{-\rho_{\mathcal{S}}(t-t_0)}\|e_i(t_0)\|^2\end{aligned} \tag{41}$$

where $\mu_{\mathcal{S}}$ is the positive amplitude from (28).

Remark 3.2: This proofs that each state platoon tracking error $e_i(t)\to0$ with the leader-following tracking and spacing maintaining objectives, i.e., $x_i(t)\to x_0(t),e_i^r(t)\to0$ and $l_i^r(t)\to l_i(t)$. Meanwhile, the exponential type of the new Lyapunov function $V(t,s(t))$ finally indicates that $\tilde{e}_i(t)\to0$ with the state and fault estimation goals, i.e., $\hat{x}_i(t)\to x_i(t)$ and $\hat{f}_i(t)\to f_i(t)$ for $t\to\infty$. Furthermore, the proposed anti-attack FTTC protocol (17) guarantees the convergence of the spacing errors of the neighboring vehicles and the exponential leader-following tracking control performance of the vehicle platoon systems (2) and (4) under the complicated actuator faults as well as the connectivity-mixed attacks ($s(t)\in\mathcal{S}$).

Remark 3.3: (i) Compared to current conventional actuator fault modelling results, i.e., the stuck-at-fixed-level, loss-of-effectiveness fault and total failure of steering systems [6], actuator saturation [9] and sensor-induced faults of vehicles [10], a low-complexity prescribed actuator fault is presented with an exponential function, without the aid of an auxiliary division mechanism, thus enabling a unified bridge between

abrupt-type and incipient-type forms. (ii) The main prerequisite or limitation for the solution of the nonlinear matrix inequalities (20) and (21) is the partial priori knowledge of the switching topologies (parameters $\Upsilon_{s(t)}$ and $\bar{\varphi}$) under connectivity-mixed attacks and the designed parameter γ in the distributed anti-attack FTTC strategy. Furthermore, the repair mechanism implies the fact that the topologies influenced by connectivity-mixed attacks are resilient and recoverable, and that topology switching phenomenon can be identified by certain intelligent anti-attack detections.

IV. Simulation Results

In this section, a vehicle platoon system-based network of one healthy leading vehicle and three faulty following vehicles is illustrated under cyber-physical threats, i.e., the simultaneous actuator faults in physical layer and connectivity-mixed attacks in cyber layer. Comparative simulations of vehicle platoon systems are illustrated to validate the effectiveness of the developed distributed anti-attack FTTC algorithm.

As for the parameter values of one healthy leading vehicle and three homogeneous following vehicles in [3], the engine index $\tau = 0.1$ is set and the length of each vehicle L is selected as 2m. The airflow, road surface or vehicle uncertainty-induced external disturbances are listed as $d_1^v(t) = 0.03\sin 0.07\pi t\text{m.s}^{-2}, d_1^a(t) = 0.05\cos 0.05\pi t\text{m.s}^{-2}, d_2^v(t) = 0.02\sin 0.1\pi t\text{m.s}^{-2}, d_2^a(t) = 0.03\sin 0.7\pi t\text{m.s}^{-2}, d_3^v(t) = 0.01\cos 0.02\pi t\text{m.s}^{-2}$ and $d_3^a(t) = 0.04\sin 0.03\pi t\text{m.s}^{-2}$.

The distinguishing boundary values of the abrupt-type and incipient-type actuator faults and the healthy and faulty vehicles are given as $\bar{\epsilon} = 0.2$ and $\underline{\epsilon} = 0.002$, respectively. The internal fault description $f_i(t)$ with the complicated abrupt-/incipient-type forms in control input channel of the first and second following vehicles is preset as

$$f_1(t) = 0.05(1-e^{-0.08t})\text{m.s}^{-2}, 20 \le t \le 50$$
$$f_2(t) = \begin{cases} 0.1(1-e^{-0.05t})\text{m.s}^{-2}, 20 \le t < 40 \\ 2(1-e^{-0.8t})\text{m.s}^{-2}, 40 \le t \le 50 \end{cases} \quad (42)$$

The derived gain matrices in the decentralized fault estimation UIO expression (12) are computed as follows

$$M = \begin{bmatrix} -0.4999 & 0.0001 & 0 & 0.001 & 0 \\ 0.0001 & -0.4999 & 0 & 0.001 & 0 \\ 0 & 0 & -0.5 & 0.0001 & 0 \\ 0.001 & 0.001 & 0.0001 & -0.4902 & 0 \\ -0.1451 & -0.1451 & -0.0161 & -1.4505 & -47.8793 \end{bmatrix}$$
$$J = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ -229.2429 & 47.8793 \end{bmatrix}, H = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 4.7879 & 0 \end{bmatrix} \quad (43)$$

and $G = [\mathbf{0}_{1\times 4} \ -47.8793]^T$.

The multiple switching topologies $\mathcal{G}_{s(t)}$ of vehicle platoon systems (i.e., the initial topology $\mathcal{G}_1$, preserving topology $\mathcal{G}_2$ and broken topology $\mathcal{G}_3$) under connectivity-mixed attacks are depicted in Fig. 2, in which the green(red) nodes represent healthy(faulty) vehicles, the black(red) arrows represent healthy(faulty) information flows, connectivity-preserving topology activates at 10s, and connectivity-broken topology plays a role at 30s and recoveries to connections between the second and third following vehicles under a repair mechanism.

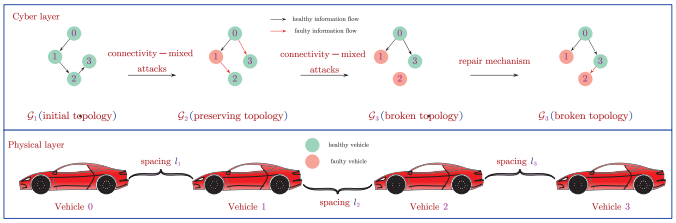

Fig. 2. The switching topologies $\mathcal{G}_{s(t)}$ under connectivity-mixed attacks.

In the presence of complicated abrupt-type and incipient-type actuator faults in the first and second following vehicles, simulation studies of vehicle platoon systems under connectivity-mixed attacks in Figs. 3-6 are provided to substantiate the effectiveness and merits of the distributed anti-attack FTTC algorithm on maintaining the desired platooning performance and fault/attack tolerance. Fig. 3 illustrates the position leader-following tracking performance of vehicle platoon systems under the switching conditions caused by cyber-attacks ($\mathcal{G}_1$: healthy topology $\rightarrow$ $\mathcal{G}_2$: connectivity-preserving topology $\rightarrow$ $\mathcal{G}_3$: connectivity-broken topology). Meanwhile, the velocity tracking and acceleration tracking details are depicted in Fig. 4 and Fig. 5 under the same switching time periods, i.e., $\mathcal{G}_1 \rightarrow \mathcal{G}_2 \rightarrow \mathcal{G}_3$, thus guaranteeing the safe platooing performance. The spacing errors $e_i^r(t), i = 0, 1, 2, 3$ are shown in Fig. 6 to maintain the desired spacing gap and to prevent vehicle collision phenomenon. Note that the first vehicle has an incipient-type actuator fault at 20s, and the second one processes a complicated abrupt-/incipient-type actuator fault at each fault occurring time instants $20\text{s}, 40\text{s}$, resulting in attenuated oscillations in position, velocity, acceleration, and spacing error time response tracking channels. Moreover, severe peak oscillations with different amplitudes are illustrated due to the connectivity-mixed attacks when multiple switchings occur at 10s and 30s. Moreover, the designed control input of the three following vehicles under cyber-physical threats is described in Fig. 7 with the explicit moments of failure and attacks. Finally, the tracking control issue of the considered vehicle platoon systems under cyber-physical threats is addressed with the proposed distributed anti-attack FTTC strategy.

Furthermore, comparative results shed light on the benefits of our decentralized fault-estimation UIO design in Fig. 8 and Fig. 9 while providing guidelines for designing the distributed anti-attack FTTC design. Specifically, Fig. 8 shows the rated and estimated values of the incipient-type actuator fault of the first following vehicle at 20s. Fig. 9 depicts the rated and estimated values of the complicated abrupt-/incipient-type actuator faults of the second following vehicle at the respective fault occurring time $20\text{s}, 40\text{s}$. Under the same fault type, occurrence time, and fault/attack tolerance effect, the estimation tracking errors show similar convergence characteristics and only produce tracking oscillation delays under connectivity-mixed attacks at the switching occurrence time instants, i.e., 10s and 30s. In contrast to the accurate estimation

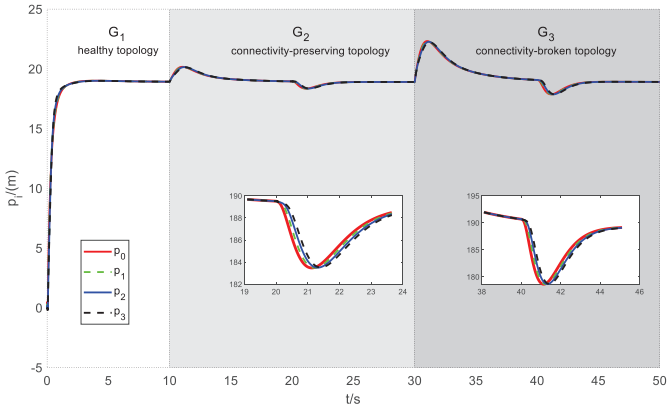

Fig. 3. Position tracking under cyber-physical threats.

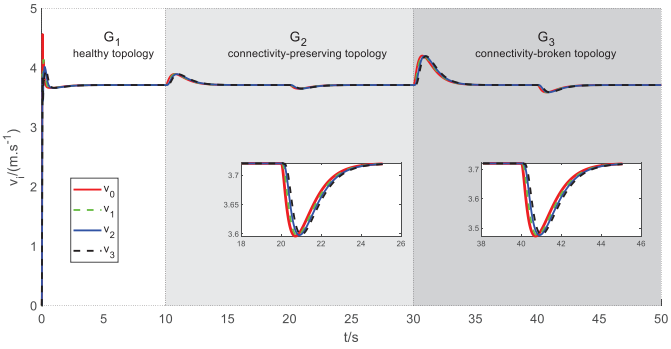

Fig. 4. Velocity tracking under cyber-physical threats.

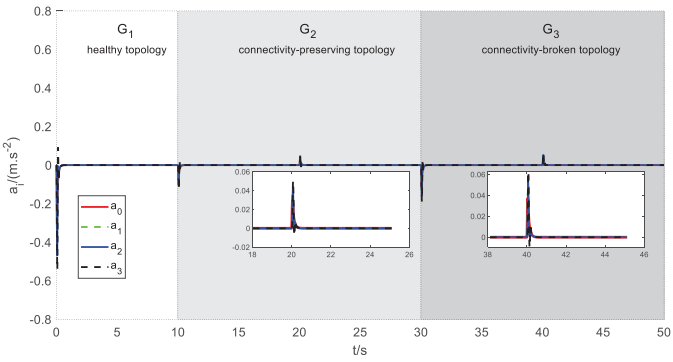

Fig. 5. Acceleration tracking under cyber-physical threats.

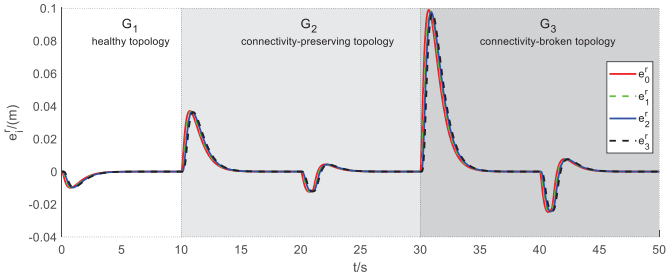

Fig. 6. Spacing error tracking under cyber-physical threats.

of actuator faults using the average dwelling time technique in [12], the irregular oscillation fluctuations in Fig. 8 and Fig.

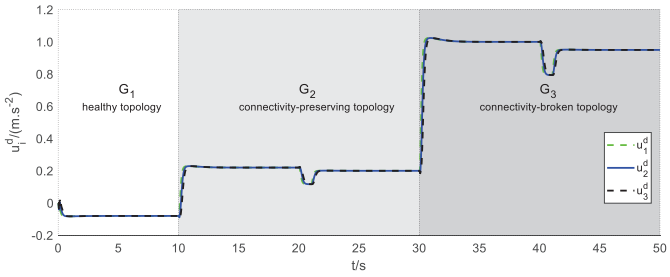

Fig. 7. Control input of the following vehicles under cyber-physical threats.

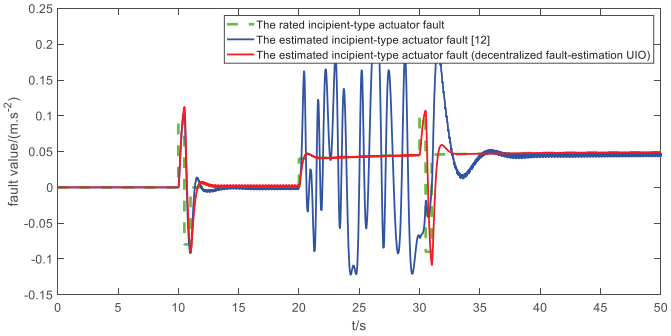

Fig. 8. Rated and estimated values of incipient-type actuator fault $f_1(t)$.

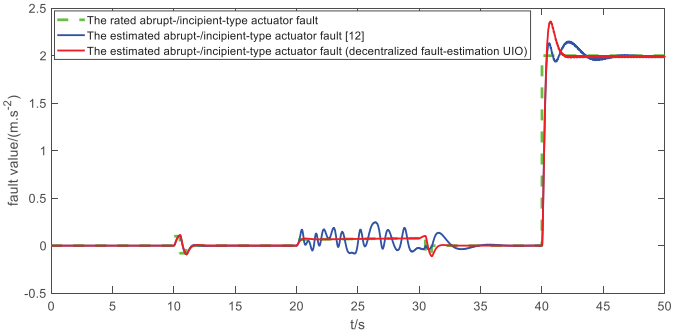

Fig. 9. Rated and estimated values of the complicated abrupt-/incipient-type actuator fault $f_2(t)$.

9 under the action of the incipient-type actuator fault cannot effectively achieve a valid and effective estimation of the rated value due to the inability to distinguish between the effects of attacks and faults in real-time simulation period. Meanwhile, in the case of the complicated abrupt-/incipient-type actuator faults, fluctuations cannot be eliminated due to the presence of abrupt-type faults, even if the fault estimation effectiveness is mitigated during the fault occurring time instants. In this case, our decentralized fault-estimation UIO design in the distributed anti-attack FTTC scheme can achieve an excellent estimation effect in vehicle platoon systems despite the persistent deviation or continuous non-dissipation oscillation under the considered connectivity-mixed attacks.

V. Conclusion

An integrated framework of decentralized fault-estimation UIO and distributed anti-attack FTTC designs is proposed in this study to comprehensively solve the cyber-physical threats

of vehicle platoon systems, including connectivity-preserving/-broken constraints (switching topologies under connectivity-mixed attacks in cyber layer) and complicated limits (exponential deflections caused by abrupt-/incipient-type actuator faults in physical layer). Simulation are provided to substantiate the effectiveness and merits of the distributed anti-attack FTTC algorithm on improving the desired platooning performance and fault/attack tolerance. Future studies should focus on the improved integration of cooperative fault-estimation and FTTC strategies of vehicle platoon systems in spite of simultaneous actuator/sensor faults and denial-of-service attacks with an event-triggered mechanism and dynamical task planning of platoon formation with a substantial reduction in networked resources when message transmission fails intermittently.

REFERENCES

[1] F. Michaud, P. Lepage, P. Frenette and et al., "Coordinated maneuvering of automated vehicles in platoons," *IEEE Trans. Intell. Transp. Syst.*, vol. 7, no. 4, pp. 437-447, 2006.

[2] T. Zeng, O. Semiari, W. Saad and M. Bennis, "Joint communication and control for wireless autonomous vehicular platoon systems," *IEEE Trans. Commun.*, vol. 67, no. 11, pp. 7907-7922, 2019.

[3] D. D. Li and G. Guo, "Prescribed performance concurrent control of connected vehicles with nonlinear third-order dynamics," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 14793-14802, 2020.

[4] D. Jia, K. Lu, J. Wang et al., "A survey on platoon-based vehicular cyber-physical systems," *IEEE Commun. Surv. Tutor.*, vol. 18, no. 1, pp. 263-284, 2016.

[5] M. R. Boukhari, A. Chaibet, M. Boukhnifer, and S. Glaser, "Two longitudinal fault tolerant control architectures for an autonomous vehicle," *Math. Comput. Simul.*, vol. 156, pp. 236-253, 2019.

[6] Y. L. Wang, C. F. Zong, K. Li, and H. Chen, "Fault-tolerant control for in-wheel-motor-driven electric ground vehicles in discrete time," *Mech. Syst. Signal Proc.*, vol. 121, pp. 441-454, 2019.

[7] C. Pan, Y. Chen, Y. Liu and I. Ali, "Adaptive resilient control for interconnected vehicular platoon with fault and saturation," *IEEE Trans. Intell. Transp. Syst.*, 2021. DOI: 10.1109/TITS.2021.3087940.

[8] W. F. Li, Z. C. Xie, J. Zhao, and P. K. Wong, "Velocity-based robust fault tolerant automatic steering control of autonomous ground vehicles via adaptive event triggered network communication," *Mech. Syst. Signal Proc.*, vol. 143, 106798, 2020.

[9] T. Chen, L. Chen, X. Xu and et al., "Passive actuator-fault-tolerant path following control of autonomous ground electric vehicle with in-wheel motors, Advances in Engineering Software," *Adv. Eng. Softw.*, vol. 134, pp. 22-30, 2019.

[10] A. Lopes and R. E. Araujo, "Active fault diagnosis method for vehicles in platoon formation," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 3590-3603, 2020.

[11] E. Hashemi, M. Pirani, A. Khajepour and et al., "Fault tolerant consensus for vehicle state estimation: a cyber-physical Approach," *IEEE Trans. Ind. Inform.*, vol. 15, no. 9, pp. 5129-5138, 2019.

[12] C. Liu, B. Jiang, K. Zhang, and R. J. Patton, "Distributed fault-tolerant consensus tracking control of multi-agent systems under fixed and switching topologies," *IEEE Trans. Circuits Syst. I-Regul. Pap.*, vol. 68, no. 4, pp. 1646-1658, 2021.

[13] J. H. Han, J. Z. Zhang, C. K. He and et al., "Adaptive distributed finite-time fault-tolerant controller for cooperative braking of the vehicle platoon," *IET Intell. Transp. Syst.*, vol. 15, no. 12, pp. 1562-1581, 2021.

[14] G. Guo, P. Li and L. Hao, "Adaptive fault-tolerant control of platoons with guaranteed traffic flow stability," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 6916-6927, 2020.

[15] X. G. Guo, W. D. Xu, J. L. Wang, and J. H. Park, "Distributed neuroadaptive fault-tolerant sliding-mode control for 2-D plane vehicular platoon systems with spacing constraints and unknown direction faults," *Automatica*, vol. 129, 109675, 2021.

[16] T. Chen, L. Chen, X. Xu and et al., "Passive fault-tolerant path following control of autonomous distributed drive electric vehicle considering steering system fault," *Mech. Syst. Signal Proc.*, vol. 123, pp. 298-315, 2019.

[17] Y. Feng, B. Hu, H. Hao and et al., "Design of distributed cyber-physical systems for connected and automated vehicles with implementing methodologies," *IEEE Trans. Ind. Inform.*, vol. 14, no. 9, pp. 4200-4211, 2018.

[18] H. Guo, J. Liu, Q. Dai and et al., "A distributed adaptive triple-step nonlinear control for a connected automated vehicle platoon with dynamic uncertainty," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3861-3871, 2020.

[19] Z. Ju, H. Zhang and Y. Tan, "Distributed deception attack detection in platoon-based connected vehicle systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 4609-4620, 2020.

[20] X. Jin, W. M. Haddad, Z. P. Jiang and et al., "An adaptive learning and control architecture for mitigating sensor and actuator attacks in connected autonomous vehicle platoons," *Int. J. Adapt. Control Signal Process.*, vol. 33, no. 12, pp. 1788-1802, 2019.

[21] 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.*, 2021. DOI: 10.1109/TCYB.2021.3074318.

[22] D. Zhang, Y. P. Shen, S. Q. Zhou and et al., "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, 2021.

[23] N. Jahanshahi and R. M. G. Ferrari, "Attack detection and estimation in cooperative vehicles platoons: a sliding mode observer approach," *IFAC-PapersOnLine*, vol. 51, no. 23, pp. 212-217, 2018.

[24] M. Zhou, L. S. Han, H. W. Lu, et al., "Attack detection based on invariant state set for SDN-enabled vehicle platoon control system," *Veh. Commun.*, vol. 34, 100417, 2022.

[25] A. Petrillo, A. Pescapé and S. Santini, "A secure adaptive control for cooperative driving of autonomous connected vehicles in the presence of heterogeneous communication delays and cyberattacks," *IEEE Trans. Cybern.*, vol. 51, no. 3, pp. 1134-1149, 2021.

[26] Z. P. Zhou, F. L. Zhu, D. Z. Xu and et al., "Attack resilient control for vehicle platoon system with full states constraint under actuator faulty scenario, Applied Mathematics and Computation," *Appl. Math. Comput.*, vol. 419, 126874, 2022.

[27] B. Wang, B. Zhang and R. Su, "Optimal tracking cooperative control for cyber-physical systems: dynamic fault-tolerant control and resilient management," *IEEE Trans. Ind. Inform.*, vol. 17, no. 1, pp. 158-167, 2021.