This article has been accepted for publication in IEEE Transactions on Vehicular Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TVT.2024.3406608

Distributed Fault-tolerant Consensus Control of Vehicle Platoon Systems with DoS Attacks

Chun Liu, *Member, IEEE*, Zhiwei Xia, and Ron J. Patton, *Life Fellow, IEEE*

***Abstract*—Vehicle platoon systems are regarded as autonomous vehicles in the platooning pattern, in which vehicles drive in sequence and maintain the desired inter-vehicle spacing. This paper investigates the platoon control problem of vehicle platoon dynamics under cyber-physical threats through the distributed fault-tolerant consensus control protocol. Complicated sensor and actuator faults in the physical layer and aperiodic denial-of-service (DoS) attacks in the cyber layer are modeled, respectively. Decentralized fault-estimation unknown input observers and event-triggered distributed anti-DoS-attack fault-tolerant consensus controllers are devised in a co-designed framework, thus maintaining not only the tolerance and resilience of platoon consensus errors and estimation errors but also the secure vehicle avoidance spacing by virtue of attack frequency and average dwelling time indicators. Simulations and experiments validate the distributed control algorithm in the pernicious short-cycle and long-cycle DoS attack scenarios.**

***Index Terms*—Distributed fault-tolerant consensus control, decentralized fault-estimation, vehicle platoon systems, aperiodic DoS attacks, actuator and sensor faults.**

I. Introduction

With increasing scientific and commercial interest in intelligent transportation fields worldwide, a strong demand arises for the development of intelligent vehicle platoon systems with reliability and autonomy to improve traffic efficiency and road capacity compared to driving alone [1]. The robust consensus control for connected homogeneous vehicular platooning with speed limitations is proposed in [2] and further extended to heterogeneous platoon systems with quantized and switching topologies [3]. Conventional consensus platoon control schemes are also developed to investigate the energy-efficient coordination of automated and connected vehicles with the co-optimization objective of vehicle velocity and gear selection [4]. A comprehensive review of the essential aspects of cyber-physical platoon-based vehicle systems (vehicle clustering/platooning, adaptive cooperative cruise, and vehicle communications) is reviewed in [5], including vehicle networking architecture, standards, traffic dynamics, etc. As typical cyber-physical multi-vehicle intelligent systems, vehicle platoon systems are susceptible to physical constraints including saturation limit [6], time-varying fault direction [7], actuator bias [8], sensor deviation [9] and even noisy measurement [10] like road gradients and wind gusts. Other networked constraints such as limited information delay [11], switching topologies [12], varied communication range [13], and vehicular ad-hoc networks and DoS attacks [14], [15] can also affect velocity-tracking [16] and path-following performance [17].

Due to structural damages or hardware defects, the actuating components or sensing devices of intelligent vehicles become more vulnerable to tiny faults and fatal failures in real-world driving. Compared with the fault diagnosis [18] based on detection, identification, localization, and isolation, reliable fault-tolerant consensus control (FTCC) strategy that maintains the stability of vehicle scheduling and promotes the accuracy of multi-vehicle coordination under physical fault scenarios has attracted significant attention [19], [20]. An adaptive FTCC mechanism is developed in [21] to ensure the string and flow stabilities of vehicular platoons subject to system heterogeneity, dead-zone nonlinearity, and input quantization. The Nussbaum function-based neuroadaptive FTTC strategy is proposed for nonlinear platoon dynamics with spacing constraints to compensate for unknown directional actuator faults [22]. Considering that the full internal state information and global signals of platoon driving systems are not available to local vehicles in practice, there is an urgent need to explore a distributed FTCC framework with a collection of local outputs and neighboring interactions. However, most existing FTCC strategies focus on traditional additive and multiplicative actuator faults or specific abrupt failures [8], [17], even requiring high levels of tolerant resource allocation and reconfiguration [23]. In the studies mentioned, the complicated sensor and actuator faults are initially overlooked. It is important to highlight that vehicle collisions can occur due to the accumulation of malicious fault messages transmitted through vehicle-to-vehicle networks, conveying minor and initial sensor and actuator faults to neighboring vehicles. Hence, enhancing the novel distributed FTCC framework, incorporating the direct adaptation of observable information from estimation to tolerance systems, is crucial yet challenging for cooperative driving in the presence of composite incipient/abrupt-type faults.

The physical limitations and the extensive networks of platoon vehicles with digital and computing facilities contribute to the vulnerability to both the physical damages [24] and malicious attacks [25]. Unlike various cyber attacks (deception attacks [26], false data injection attacks [27], actuator and sensor attacks [28]) that tamper with the accuracy and integrity of interactive data, DoS attacks in platoon systems cause

This work was supported by National Natural Science Foundation of China (62103250, 62333011, 62273223, and 62336005); Shanghai Sailing Program (21YF1414000); Project of Science and Technology Commission of Shanghai Municipality, China (22JC1401401). *(Corresponding author: Chun Liu.)*

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

Z. W. Xia is with the School of Mechatronic Engineering and Automation, Shanghai University, Shanghai 200444, China (e-mail: xzw_shu@shu.edu.cn)

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

© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Vehicular Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TVT.2024.3406608

disruptions in the information transmission in the cyber layer [14], [29]. The safety and security aspects of the different attacked locations (in-vehicle communication, sensing devices, and vehicle-to-vehicle networks) for automated and connected vehicles are outlined in [30], including the attack resilience and anomaly detection strategies. Specifically, the distributed secure platoon control algorithm is developed for vehicle platoon dynamics subjected to DoS attacks using time-delay switched models to eventually achieve an exponential tracking performance [31]. The resilient anti-DoS-attack platoon control mechanism is developed to attain internal stability of vehicular cyber-physical systems with the propagation of disturbances [32]. However, there has been relatively limited research conducted on FTCC schemes that address hostile aperiodic DoS attacks and unpredictable faults, which may vary in terms of action points, moments, durations, and levels of damage [33]. The difficulty of its distributed FTCC is that existing strategies under switching topologies or balanced graph mechanism [12], [23], [31] do not directly address the simultaneous consensus tracking and anti-attack performance of the damaged vehicles. The algebraic Riccati equations (ARE)-based fault-tolerant distributed tracking protocol with resilient defense management is developed for vehicle platoon dynamics to defend the connectivity-mixed attacks [34]. In addition, given the dominant advantage of reducing the communication burden, the inter-vehicle platoon dynamics by security breaches should take into account such dangers (intentional and accidental cyber-physical threats) by applying event-triggered FTCC protocols [35], [36]. To tackle the dilemma of simultaneous abrupt and incipient sensor and actuator faults in the physical hierarchy and aperiodic DoS attacks in the cyber hierarchy, it is significant but challenging to develop an advanced distributed FTCC protocol for vehicle platoon systems to equip them with tolerance and resilience capabilities for vehicle avoidance and safe driving.

The major contributions are illustrated as follows.

(i) The cyber-physical safety and security issue in vehicle platoon dynamics contributes to furnishing both strong tolerances to composite constraints by abrupt-/incipient-type sensor and actuator faults in the physical hierarchy and robust resilience to paralyzed connectivities from aperiodic DoS attacks in the cyber hierarchy. By extending from our previous study [34] on consensus characterization of connectivity-mixed attacks to segmental modeling of DoS attacks, an actionable implementation in both simulations and experiments is further substantiated through an integrated framework, i.e., unknown input observer (UIO) in decentralized fault-estimation fashion and FTCC in distributed anti-DoS-attack form.

(ii) The balance between the exponential mean-square consensus and vehicle avoidance-driven inter-vehicle spacing is guaranteed even under cyber-physical threats. A low-complexity event-triggered distributed FTCC mechanism is devised to reduce the occupation in vehicle platoon networks by virtue of multi-dimensional sensor fault estimation and output interaction error-based triggering threshold, especially in pernicious long-cycle and short-cycle DoS attack scenarios. Furthermore, the switching indicator [31] or attack activation rate [34] is circumvented by dual-constraint metrics, i.e., attack frequency and average dwelling time (ADT), to enable more accurate and reliable tracking of faults without an auxiliary approximation of unknown disturbance bounds and an elimination of Zeno behavior in accumulation of triggering instants.

The remaining parts are expressed as follows. Vehicle platoon dynamics including complicated faults and aperiodic DoS attacks in Section II are established. Section III develops the decentralized fault-estimation UIO and distributed anti-DoS-attack FTCC co-design in DoS attack dormancy and activation cases. Simulations and experiments illustrate the practicality and advantage of the event-triggered FTCC algorithm in Section IV. Conclusions are ultimately outlined in Section V.

Notations: $\otimes$ denotes the Kronecker product, $\mathrm{He}(\star) = \star + \star^T$, $\mathbf{1}_N = [1, \cdots, 1]^T \in \mathbb{R}^N$, and $x = \mathrm{col}(x_i) = [x_1^T, \cdots, x_N^T]^T \in \mathbb{R}^N$.

II. Model description and system formulation

A. Graph theory

The graph $\mathcal{G}$ is defined as a pair $(\nu, \vartheta, \mathcal{A})$, where $\nu = \{\nu_1, \cdots, \nu_N\}$ represents a nonempty finite node set, $\vartheta \subseteq \nu \times \nu$ denotes the edge set, and $\mathcal{A} = [a_{ij}] \in \mathbb{R}^{N\times N}$ is the adjacency matrix. In the adjacency matrix, a_{ij} is the weight coefficient of the edge (ν_i, ν_j), and $a_{ii} = 0$ while $a_{ij} > 0$ if $(\nu_i, \nu_j) \in \vartheta$; otherwise, $a_{ij} = 0$. A node ν_j is considered as a neighbor of node ν_i if $(\nu_i, \nu_j) \in \vartheta$. The set of neighbors of node ν_i is denoted as $\mathcal{N}_i = \{\nu_j \in \nu \mid (\nu_i, \nu_j) \in \vartheta\}$. The Laplacian matrix is represented as $\mathcal{L} = \mathcal{D} - \mathcal{A} = [l_{ij}] \in \mathbb{R}^{N\times N}$, where $\mathcal{D} = [d_{ii}] \in \mathbb{R}^{N\times N}$ is a diagonal matrix with $d_{ii} = \sum_{j=1}^{N} a_{ij}$. Assuming that the eigenvalues of $\mathcal{L}$ are denoted as $\lambda_1(\mathcal{L}), \cdots, \lambda_N(\mathcal{L})$, it follows that $0 = \lambda_1(\mathcal{L}) \leq \lambda_2(\mathcal{L}) \leq \cdots \leq \lambda_N(\mathcal{L})$ with the semi-positive definite Laplacian matrix.

B. Platoon vehicle modeling

Consider a system of $N+1$ vehicles operating as a vehicle platoon. The ith homogeneous platoon dynamics $(i = 1, \cdots, N+1)$ are modeled as

$$\begin{cases} \dot{p}_i(t) = v_i(t) \\ \dot{v}_i(t) = a_i(t) + d_i^v(t) \\ \dot{a}_i(t) = -\frac{1}{\tau} a_i(t) + \frac{1}{\tau}\left(u_i(t) + f_{ai}(t)\right) + d_i^a(t) \end{cases} \tag{1}$$

where $p_i(t) \in \mathbb{R}, v_i(t) \in \mathbb{R}$ and $a_i(t) \in \mathbb{R}$ represent the position, velocity and acceleration, $u_i(t) \in \mathbb{R}$ represents the control input, $f_{ai}(t) \in \mathbb{R}$ represents the actuator fault occurring in the input layer, $d_i^a(t) \in \mathbb{R}$ and $d_i^v(t) \in \mathbb{R}$ represent the uncertainty-induced disturbance in the acceleration layer and the airflow or road surface-induced disturbance in the velocity layer, and τ denotes the engine-induced time scalar.

The ith spacing $l_i(t), i = 1, \cdots, N$ between the neighboring vehicles is modeled as $l_i(t) = p_{i+1}(t) - p_i(t) - L$ with L represented as the vehicle length. Furthermore, denote the vehicle state vector, the sensor fault-induced output vector, and the introduced disturbance as $x_i(t) = [l_i(t)\ v_i(t)\ a_i(t)]^T, y_i = [l_i(t)\ v_i(t)]^T$ and $\omega_i(t) = [v_{i+1}(t)\ d_i^v(t)\ d_i^a(t)]^T$.

The model of the ith vehicle $(i = 1, \cdots, N)$ with the complicated sensor and actuator faults is established as

$$\begin{cases} \dot{x}_i(t) = Ax_i(t) + B\left(u_i(t) + f_{ai}(t)\right) + \omega_i(t) \\ y_i(t) = Cx_i(t) + Ff_{si}(t) \end{cases} \tag{2}$$

© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Vehicular Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TVT.2024.3406608

with

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

where $f_{si}(t)=[f_{si}^{1}(t)\ f_{si}^{2}(t)]$ is the sensor fault occurring in the output channel and F is the known fault-induced matrix.

1) Complicated actuator and sensor fault modeling in the physical input and output layers: the complicated forms $f_{ai}(t)$ and $f_{si}(t)$ are modeled as the abrupt and incipient faults (*distinguishable exponential type*) with the following elements

$$\left\{\begin{array}{l} f_{ai}\left(t\right)=\left(1-e^{-\epsilon_a(t-T_a)}\right)\bar{f}_{ai}\\ f_{si}^{\varrho}\left(t\right)=\left(1-e^{-\epsilon_s^{\varrho}(t-T_s^{\varrho})}\right)\bar{f}_{si}^{\varrho},\varrho=1,2\end{array}\right. \tag{4}$$

where $\bar{f}_{ai}(\bar{f}_{si}^{\varrho}),T_a(T_s^{\varrho})$ and $\epsilon_a(\epsilon_s^{\varrho})$ denote the bias actuator or sensor fault bounds, fault occurring instants, and decay rates of each vehicle, respectively. Specifically, the complicated sensor and actuator faults in the physical output and input layers are denoted as the incipient type (*slow-varying decay rate*) when $\underline{\epsilon}_a\leq\epsilon_a<\bar{\epsilon}_a,\underline{\epsilon}_s^{\varrho}\leq\epsilon_s^{\varrho}<\bar{\epsilon}_s^{\varrho}$ and the abrupt type (*quick-varying decay rate*) when $\epsilon_a\geq\bar{\epsilon}_a,\epsilon_s^{\varrho}\geq\bar{\epsilon}_s^{\varrho}$.

Assumption 2.1: The unknown exponential decay rates of the incipient-/abrupt-type faults ϵ_a and ϵ_s^{ϱ} exist while the distinguishable boundary values of the faulty and healthy actuators/sensors in the output and input channels are determined artificially with the positive scalars $\underline{\epsilon}_a$ and $\underline{\epsilon}_s^{\varrho}$.

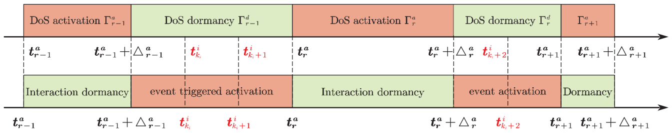
DoS activation Γ_{r-1}^a
DoS dormancy Γ_{r-1}^d
DoS activation Γ_r^a
DoS dormancy Γ_r^d
Γ_{r+1}^a
t_{r-1}^a
$t_{r-1}^a+\triangle_{r-1}^a$
$t_{k_i}^i$
$t_{k_i+1}^i$
t_r^a
$t_r^a+\triangle_r^a$
$t_{k_i+2}^i$
t_{r+1}^a
$t_{r+1}^a+\triangle_{r+1}^a$
Interaction dormancy
event triggered activation
Interaction dormancy
event activation
Dormancy
t_{r-1}^a
$t_{r-1}^a+\triangle_{r-1}^a$
$t_{k_i}^i$
$t_{k_i+1}^i$
t_r^a
$t_r^a+\triangle_r^a$
$t_{k_i+2}^i$
t_{r+1}^a
$t_{r+1}^a+\triangle_{r+1}^a$

Fig. 1. Aperiodic DoS activation and dormancy intervals.

2) Aperiodic DoS attack modeling in the cyber layer: resource-limited adversary attackers typically launch intermittent DoS attacks in the cyber layer that cause irregular interruption of multi-vehicle interactive networks during the attack activation period. The aperiodic DoS attacks can terminate the malicious attack pattern at intervals and remain dormant, thus accumulating energy for the next DoS attack. For $t\geq t_0\in\mathbb{R}$, given $r\in\mathbb{N}$, aperiodic DoS attack sequence is denoted as $\{t_r^a\}_{r\in\mathbb{N}}$ over $[t_0,t)$, where t_r^a and $t_{r+1}^a=t_r^a+\Delta_r$ are the consecutive activation instants with the time-varying aperiodic sampling interval Δ_r. Denote $\Gamma_r^a=[t_r^a,t_r^a+\Delta_r^a)$ as the rth DoS activation interval with $t_{r+1}^a>t_r^a+\Delta_r^a$ with each rth interval $\Delta_r^a>0$.

Definition 2.1: Define the total activation interval of DoS attacks as $\Gamma^a(t_0,t)=\cup\Gamma_r^a\cap[t_0,t]$ over $[t_0,t)$, where information interaction is prohibited in networked vehicle platoon systems (interaction dormancy). Define $\Gamma^d(t_0,t)=[t_0,t]\setminus\Gamma^a(t_0,t)$ as the total dormancy interval of DoS attacks over $[t_0,t)$, where the interaction is allowed, the networked topology holds connected and unchanged, and the updated control signal is activated at $\{\cdots,t_{k_i}^i,t_{k_i+1}^i\cdots\}$ during the proposed event-triggered activation (DoS dormancy) in Fig. 1.

Definition 2.2 (DoS attack number): Define $N_{\Gamma}(t_0,t)=N_{\Gamma^a}(t_0,t)+N_{\Gamma^d}(t_0,t),\forall t>t_0\geq 0$, where $N_{\Gamma^a}(t_0,t)$ and $N_{\Gamma^d}(t_0,t)$ represent the numbers of aperiodic DoS activation and dormancy attacks, respectively.

Definition 2.3 (DoS attack frequency): Define $\mathcal{F}_{\Gamma^a}(t_0,t)=\frac{N_{\Gamma^a}(t_0,t)}{t-t_0}$ as the DoS attack frequency over $[t_0,t)$.

Definition 2.4 (ADT indicator): For $\Gamma^a(t_0,t)$, there exists a chattering bound $\Gamma_0\geq 0$ and ADT indicator $\tau_a>0$ such that $\Gamma^a(t_0,t)=\sum_{r\in\mathbb{N}}\Delta_r^a\leq\Gamma_0+\frac{t-t_0}{\tau_a}$ for $t\geq t_0$.

Lemma 2.1: Given connected graph $\mathcal{G}$ with Laplacian matrix $\mathcal{L}$, there exists an orthogonal matrix $\Psi=[\frac{1}{\sqrt{N}}\mathbf{1}_N\ \ \psi_2\ \ \psi_3\cdots\psi_N]\in\mathbb{R}^{N\times N}$ such that $\Psi\Psi^T=I_N$ and $\mathcal{L}\mathcal{M}=\mathcal{M}\mathcal{L}=\mathcal{L}$, where $\mathcal{M}=I_N-\frac{1}{N}\mathbf{1}_N\mathbf{1}_N^T$ and $\psi_i\in\mathbb{R}^N,i=2,\cdots,N$ is an orthogonal eigenvector of $\mathcal{L}$ with an eigenvalue $\lambda_i(\mathcal{L})$, i.e., $\mathcal{L}\psi_i=\lambda_i(\mathcal{L})\psi_i$. Then, denote $\psi=[\psi_2\ \psi_3\cdots\psi_N]$, and it is derived as $\psi\psi^T=\mathcal{M}$.

Proof. Under the orthogonal matrix definition Ψ, $\Psi\Psi^T=[\frac{1_N}{\sqrt{N}}\ \psi][\frac{1_N}{\sqrt{N}}\ \psi]^T=\frac{1}{N}1_N1_N^T+\psi\psi^T=I_N-\mathcal{M}+\psi\psi^T=I_N$ with $\psi=[\psi_2\ \psi_3\cdots\psi_N]$ and $\mathcal{M}=I_N-\frac{1}{N}1_N1_N^T$. Hence, $\mathcal{M}=\psi\psi^T$ is derived. Furthermore, $\mathcal{L}\mathcal{M}=\mathcal{L}-\frac{1}{N}\mathcal{L}1_N1_N^T=\mathcal{M}\mathcal{L}=\mathcal{L}$ is obtained under the Laplacian matrix property.

C. Problem formulation

The main objectives are scheduled as follows. i) To guarantee the credible inter-vehicle network and reliable cruises of platoon vehicles under the cyber-physical threats (complicated sensor and actuator faults and aperiodic DoS attacks), the proposed control mechanism balances the target spacing $l_i(t)$ between two successive vehicles with vehicle crash avoidance. ii) The mean-square exponential consensus control problem of the platoon vehicles (2) with complicated faults (4) is solved through the distributed FTCC strategy if there exists a positive amplitude μ and a positive decay rate λ such that

$$\begin{array}{l}\left\|x_i(t)-\frac{1}{N}\sum_{i=1}^{N}x_i(t)\right\|^2\\ \leq\mu e^{-\lambda(t-t_0)}\left\|x_i(t_0)-\frac{1}{N}\sum_{i=1}^{N}x_i(t_0)\right\|^2,\forall t\geq t_0\end{array} \tag{5}$$

Remark 2.1: (i) In contrast to the traditional single classification modeling of vehicle faults [6], [8] that consider specific partial loss, bias or saturation faults, a low-complexity general fault model with an exponential decay rate in both actuation and sensing channels is proposed without a subsidiary multi-classification mechanism, thus building a unified architecture for both incipient and abrupt-type forms of actuator and sensor deflects. (ii) Compared with a priori knowledge of road surface, airflow, and system uncertainty-induced perturbation bounds [32], the assumption of the known upper bounds of the external disturbances $d_i^a(t)$ and $d_i^v(t)$ in the acceleration and velocity layers is successfully relaxed without an auxiliary approximation to the unknown boundaries.

Remark 2.2: In complex and open vehicle cruise environments, the topological connectivity of platoon vehicles is susceptible to intermittent DoS attacks (link-break malfunctions). Hostile aggressors attempt to prevent coherent signal transmission among the accessible vehicles, aborting data interactions and ultimately resulting in poor spacing tracking performance. However, the defense system of the smart vehicle can continuously initiate relink requests until network connectivity is restored during the DoS attack dormancy interval. Intelligent

© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Vehicular Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TVT.2024.3406608

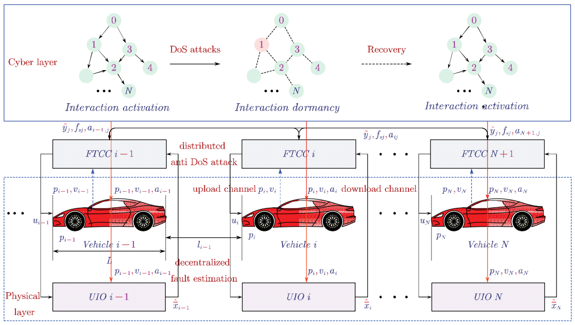

Fig. 2. Decentralized fault-estimation UIO and distributed anti-DoS-attack FTCC co-design.

defender further redefines the scheduling of controller update events even under different action nodes, moments, duration, and damage levels of faults and attacks. Compared with the easily or partially detectable determinism of periodic DoS attacks and known attack strategies [14], [31], [32], the DoS attacks executed by the adversary in this study are modeled as occurring non-periodically and typically disrupting networked interactions while assuming that the topology is resilient and recoverable and that certain bounds of DoS attack frequency and ADT are accessible by smart counter-attack devices.

III. Fault-Estimation UIO and Anti-DoS-Attack FTCC Designs

The control framework incorporates the UIO protocol in the decentralized fault-estimation and FTCC scheme in the distributed DoS-resistance for platoon vehicles under cyber-physical threats in Fig. 2. It primarily consists of platoon vehicles experiencing complicated incipient-/abrupt-type actuator and sensor faults in the physical output and input layers, as well as intermittent interaction interruptions subject to aperiodic DoS attacks in the cyber layer.

A. Decentralized fault-estimation UIO design

The involved incipient and abrupt-type actuator and sensor faults are differentiable and smooth after the fault occurrences $t \geq T_a$ and $t \geq T_s^\varrho$. Notably, it is attainable to define the augmented state as $\bar{x}_i(t) = [x_i^T(t)\ f_{ai}\ f_{si}^T]^T$ and the augmented uncertainty as $\bar{\omega}_i(t) = [\omega_i^T(t)\ \dot{f}_{ai}\ \dot{f}_{si}^T]^T$.

Then, the augmented system of vehicle i with the differentiable faults $\dot{f}_{ai}(t)$ and $\dot{f}_{si}(t)$ is established as

$$\begin{cases} \dot{\bar{x}}_i(t) = \bar{A}\bar{x}_i(t) + \bar{B}u_i(t) + \bar{\omega}_i(t) \\ y_i(t) = \bar{C}\bar{x}_i(t) \end{cases} \tag{6}$$

with the following system matrices as $\bar{C} = [C\ \mathbf{0}_{2\times 1}\ F]$,

$$\bar{A} = \begin{bmatrix} A & B & \mathbf{0}_{3\times 2} \\ \mathbf{0}_{1\times 3} & 0 & \mathbf{0}_{1\times 2} \\ \mathbf{0}_{2\times 3} & \mathbf{0}_{2\times 1} & \mathbf{0}_{2\times 2} \end{bmatrix}, \bar{B} = \begin{bmatrix} B \\ 0 \\ \mathbf{0}_{2\times 1} \end{bmatrix} \tag{7}$$

To simultaneously evaluate the non-measured states and hidden faults of platoon vehicles under complicated actuator and sensor faults modeled by distinguishability, especially in the case of restricted communication interactions under DoS attacks, the UIO scheme requires only the available information while shielding signals from other observers within physically limited distances for each vehicle. This is the feature of a single-stream, decentralized structure that can overcome the difficulty of obtaining information from distributed interactions. Then, the UIO design is expressed as

$$\begin{cases} \dot{z}_i(t) = \left(\Theta\bar{A} - J\bar{C}\right) z_i(t) + \Theta\bar{B}u_i(t) \\ \qquad + \left(J + \left(\Theta\bar{A} - J\bar{C}\right)H\right) y_i(t) \\ \hat{\bar{x}}_i(t) = z_i(t) + Hy_i(t) \end{cases} \tag{8}$$

where $z_i(t)$ represents the UIO state, and $\hat{\bar{x}}_i(t) = [\hat{x}_i^T(t)\ \hat{f}_{ai}(t)\ \hat{f}_{si}^T(t)]^T$ represents the estimation of the augmented state $\bar{x}_i(t)$, where $\hat{x}_i(t), \hat{f}_{ai}(t)$ and $\hat{f}_{si}(t)$ represent the state, actuator and sensor fault estimations of $x_i(t), f_{ai}(t)$ and $f_{si}(t)$, respectively. The UIO gains Θ, H and J in (8) are designed with appropriate dimensions without hyperparameters in fault-estimation description.

Denote the estimation error as $e_{i1}(t) = \bar{x}_i(t) - \hat{\bar{x}}_i(t) = [e_{xi}^T(t)\ e_{ai}(t)\ e_{si}^T(t)]^T$ with $e_{xi}(t) = x_i(t) - \hat{x}_i(t)$, $e_{ai}(t) = f_{ai}(t) - \hat{f}_{ai}(t)$, and $e_{si}(t) = f_{si}(t) - \hat{f}_{si}(t)$, respectively. Furthermore, define $\Theta = I_6 - H\bar{C}$ and $W = \Theta\bar{A} - J\bar{C}$, and the estimation error systems can be derived as

$$\dot{e}_{i1}(t) = We_{i1}(t) + \Theta\bar{\omega}_i(t) \tag{9}$$

and the global estimation error expression is derived as

$$\dot{e}_1(t) = (I_N \otimes W)e_1(t) + (I_N \otimes \Theta)\bar{\omega}(t) \tag{10}$$

where $e_1(t) = \mathrm{col}(e_{i1}(t))$ and $\bar{\omega}(t) = \mathrm{col}(\bar{\omega}_i(t))$.

Remark 3.1: The Hurwitz estimation gain $\Theta\bar{A} - J\bar{C}$ guarantees the asymptotic stability and robustness of the estimation errors (9) and (10). The existence solution of gains J and H allows the decoupling calculation of the UIO matrices in the decentralized fault-estimation framework to be more intuitive. In addition, non-differentiable dilemmas caused by transient intermittent points of time-varying abrupt sensor and actuator faults in the physical layer can be fitted with fine-tunable approximations.

B. Distributed anti-DoS-attack FTCC design

The distributed FTCC strategy of the platoon vehicles is designed with a powerful combination of fault-estimation-based tolerance and anti-DoS-attack resilience. Meanwhile, to address the dilemma of redundancy or blockage of networked resources, an event-based control mechanism is added into the FTCC scheme in updating the triggering signal at the event-based time sequence $\{t_0^i, t_1^i, \cdots, t_{k_i}^i, \cdots\}$, i.e., the ith vehicle can successfully update during the dormancy interval $\Gamma^d(t_0, t)$ of DoS attacks. During each $t \in [t_{k_i}^i, t_{k_i+1}^i)$, the event-triggered distributed FTCC controller is designed based on the estimation and interaction information as follows

$$\begin{aligned} u_i(t) = & \overbrace{-K_1\hat{\bar{x}}_i(t) - K_2F\sum_{j\in\mathcal{N}_i} a_{ij}\left(\hat{f}_{sj}(t) - \hat{f}_{si}(t)\right)}^{\text{fault tolerance (estimation)}} \\ & \underbrace{+K_2\sum_{j\in\mathcal{N}_i} a_{ij}\left(\tilde{y}_j(t) - \tilde{y}_i(t)\right)}_{\text{DoS}-\text{attack resilience (interaction)}} \end{aligned} \tag{11}$$

© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Vehicular Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TVT.2024.3406608

where $K_1 = [K_x \;\; 1 \;\; \mathbf{0}_{1\times 2}]$ represents the compensation-based gain with the state-estimation matrix K_x, K_2 represents the interaction-based matrix, and $\tilde{y}_i(t) = y_i(t^i_{k_i(t)})$ denotes the latest successfully triggered output interaction with $k_i(t)$ denoted as the last triggering instant as follows

$$k_i(t) = \left\{ \begin{array}{ll} -1, & \text{when } \Gamma^d(t_0,t) = \emptyset \\ \sup\{k_i \in \mathbb{N} \mid t^i_{k_i} \in \Gamma^d(t_0,t)\}, & \text{otherwise} \end{array} \right. \tag{12}$$

Denote the output interaction error as $\delta_i(t) = \tilde{y}_i(t) - y_i(t)$, and it follows that

$$\begin{aligned} &\dot{x}_i(t) = (A - BK_x)\, x_i(t) + BK_1 e_{i1}(t) + \omega_i(t) \\ &+BK_2 \textstyle\sum_{j\in\mathcal{N}_i} a_{ij} \left(C\left(x_j(t) - x_i(t)\right) + \delta_j(t) - \delta_i(t)\right) \\ &+BK_2 F \textstyle\sum_{j\in\mathcal{N}_i} a_{ij} \left(e_{sj}(t) - e_{si}(t)\right) \end{aligned} \tag{13}$$

and the global state dynamics of vehicle i are described as

$$\begin{aligned} \dot{x}(t) = &\left(I_N \otimes (A - BK_x) - \mathcal{L} \otimes BK_2 C\right) x(t) \\ &+ \left(I_N \otimes BK_1 - \mathcal{L} \otimes BK_2 F E_s\right) e_1(t) \\ &- \left(\mathcal{L} \otimes BK_2\right) \delta(t) + \omega\left(t\right) \end{aligned} \tag{14}$$

where $x(t) = \mathrm{col}(x_i(t)), \delta(t) = \mathrm{col}(\delta_i(t)), \omega(t) = \mathrm{col}(\omega_i(t))$, and $E_s = [\mathbf{0}_{2\times 3} \;\; \mathbf{0}_{2\times 1} \;\; I_2]$.

To solve the problem of wasted or unnecessary utilization of communication resources, the event-triggered protocol for the updated sequence $\{t^i_{k_i}\}_{k_i\in\mathbb{N}}$ is devised by using the static threshold strategy with the estimated sensor fault $\hat{f}_{si}(t)$ and the output interaction $\tilde{y}_i(t)$ in a distributed fashion,

$$\begin{aligned} \|\delta_i(t)\| \le \theta_i &\left\| \textstyle\sum_{j\in\mathcal{N}_i} a_{ij} \left(\tilde{y}_j(t) - \tilde{y}_i(t)\right) \right\| \\ -\theta_i &\left\| F \textstyle\sum_{j\in\mathcal{N}_i} a_{ij} \left(\hat{f}_{sj}(t) - \hat{f}_{si}(t)\right) \right\| \end{aligned} \tag{15}$$

where $\theta_i > 0$ is the static event-triggered threshold. Specifically, it indicates that the distributed FTCC controller (11) can be successfully triggered and updated during the hibernation of aperiodic DoS attacks when and only when the output interaction error $\delta_i(t)$ is below the predefined threshold function of the adjacency messages (15).

Denote the mean-square platoon consensus error as $e_{i2}(t) = x_i(t) - \frac{1}{N}\sum_{i=1}^{N} x_i(t)$. With the application of the distributed FTCC strategy (11) combined with fault tolerance and DoS-attack resilience capabilities, the corresponding global platoon consensus error systems are obtained as

$$\begin{aligned} \dot{e}_2(t) = &(I_N \otimes (A - BK_x) - \mathcal{L} \otimes BK_2 C) e_2(t) \\ &+(\mathcal{M} \otimes BK_1 - \mathcal{L} \otimes BK_2 F E_s) e_1(t) \\ &-(\mathcal{L} \otimes BK_2)\delta(t) + (\mathcal{M} \otimes I_4)\omega(t) \end{aligned} \tag{16}$$

where $e_2(t) = \mathrm{col}(e_{i2}(t))$ and $\mathcal{M}$ is defined in Lemma 2.1.

Theorem 3.1: Each vehicle with the event-triggered distributed FTCC strategy (11), (15) can achieve the exponential mean-square consensus property of the vehicle platoon dynamics (2) in the presence of the complicated actuator/sensor faults in the input/output channels and aperiodic DoS attacks in the interaction channel when the following conditions hold:

(1) Given the positive scalars $\varepsilon_1, \varepsilon_2, \varepsilon_3, \rho_1, \mu_1, \mu_2, \mu_4, \eta_\Gamma$ and the chattering bound Γ_0, there exists a symmetric positive-definite matrix P, positive-definite matrices R, Q_1, Q_2, and matrices K_x, H, J such that

$$-Q_1 - \mathrm{He}(PBK_x) + \tfrac{1}{2}\rho_1 k_1^2 I_3 + Q_2 < 0 \tag{17}$$

$$\mathrm{He}(W) + \Theta\Theta^T - \xi I_6 < 0 \tag{18}$$

$$\max\{\tfrac{\varepsilon_2}{\varepsilon_1}, \tfrac{\varepsilon_3}{\varepsilon_1}\} \le \min\{2\underline{\epsilon}_{a(s)} - \alpha_1, 2\underline{\epsilon}_{a(s)} + \alpha_2\} \tag{19}$$

where an ARE is denoted as $\mathrm{He}(PA) - PBR^{-1}B^TP + Q_1 = 0$, $\xi = \min\{-\frac{\varepsilon_1\mu_1 k_1^2 k_2^2 + 4\varepsilon_1\mu_2 k_4^2 \lambda^2_{\max}(\mathcal{M})}{4\lambda_{\min}(Q_2)} - \frac{2\varepsilon_1 k_2^2 \bar{\theta}^2 \lambda_N^2(\mathcal{L})}{2\rho_1(1-2\bar{\theta}^2\lambda_N^2(\mathcal{L}))} - \alpha_1, \alpha_2 - \frac{\varepsilon_1\mu_4 k_4^2 \lambda^2_{\max}(\mathcal{M})}{\lambda_{\min}(\bar{Q}_2)}\}$ with $k_1 = \|PBR^{-1}B^TP\|, k_2 = \|C^\dagger F E_s\|, k_4 = \|PBK_1\|$, $\bar{\theta} = \max\theta_i \in (0, \frac{\sqrt{2}}{2}\lambda_N^{-1}(\mathcal{L}))$, $\bar{Q}_2 = Q_2 - PBR^{-1}B^TP + \frac{1}{2}\rho_1 k_1^2 I_3$, and $\underline{\epsilon}_s = \min\limits_{\varrho=1,2} \epsilon_s^\varrho$. The positive decay rate-based scalars are constrained within $\alpha_1 \le \frac{\bar{\mu}_1\lambda_{\min}(Q_2)}{\lambda_{\max}(P)} - \frac{2\bar{\theta}^2\lambda_N^2(\mathcal{L})}{2\rho_1(1-2\bar{\theta}^2\lambda_N^2(\mathcal{L}))\lambda_{\max}(P)}, \alpha_2 \ge -\frac{\bar{\mu}_2\lambda_{\min}(\bar{Q}_2)}{\lambda_{\min}(P)}$ with $\bar{\mu}_1 = 1 - \frac{1}{\mu_1} - \frac{1}{\mu_2} - \frac{1}{\mu_3}, \bar{\mu}_2 = 1 - \frac{1}{\mu_4} - \frac{1}{\mu_5}$, where $\mu_3 \le -\frac{\lambda_{\min}(Q_2)}{\varepsilon_1 k_5^2 \lambda^2_{\max}(\mathcal{M})}, \mu_5 \le -\frac{\lambda_{\min}(\bar{Q}_2)}{\varepsilon_1 k_5^2 \lambda^2_{\max}(\mathcal{M})}$ with $k_5 = \|P\|$.

(2) The interaction-based gain in the event-triggered distributed FTCC scheme (11) is designed as $K_2 = \tilde{\tau}R^{-1}B^TPC^\dagger$ with $\tilde{\tau} \ge \lambda_2^{-1}(\mathrm{He}(\mathcal{L}))$. For a positive scalar $\sigma^* \in (0, \alpha_1)$, the DoS attack frequency and ADT indicator are satisfied with

$$\left\{ \begin{array}{l} \mathcal{F}_{\Gamma^a}(t_0,t) \le \sigma^* \ln^{-1}(\varpi_1^{-1}\varpi_2) \\ \tau_a > (\alpha_1 - \sigma^*)^{-1}(\alpha_1 + \alpha_2) \end{array} \right. \tag{20}$$

where $\varpi_1 = \lambda_{\min}(P)$ and $\varpi_2 = \lambda_{\max}(P)$.

Proof. The aperiodic DoS attacks can switch intermittently between attack dormancy and activation and can be divided into Case I with the interval $\Gamma^d(t_0,t)$ and Case II with the interval $\Gamma^a(t_0,t)$ in Definition 2.1. In Case I, aperiodic DoS attacks remain dormancy, and the event-triggered distributed FTCC mechanism is activated, allowing the propagation of the output interaction information $\sum_{j\in\mathcal{N}_i} a_{ij}(\tilde{y}_j(t) - \tilde{y}_i(t))$ (DoS-attack resilience) and the adjacency estimation information $\sum_{j\in\mathcal{N}_i} a_{ij}(\hat{f}_{sj}(t) - \hat{f}_{si}(t))$ (fault-tolerance). In Case II, when DoS attacks are activated and the event-triggered mechanism is not established, i.e., the threshold function (15) is violated, the distributed interaction is then not permitted and the proposed FTCC strategy can only make full use of the scattered estimation information $\hat{\bar{x}}_i(t)$ to remain valuable information.

Case I: DoS attack dormancy with event triggering

Consider the first Lyapunov function $V_1(t) = e_2^T(t)(I_N \otimes P)e_2(t)$ with the symmetric positive-definite matrix P, and the first-order derivative of $V_1(t)$ is derived as

$$\begin{aligned} &\dot{V}_1 = e_2^T(I_N \otimes \mathrm{He}(P(A - BK_x)))e_2 + e_2^T(\mathrm{He}(\mathcal{M}) \otimes P)\omega \\ &-e_2^T(\mathrm{He}(\mathcal{L}) \otimes PBK_2C)e_2 + e_2^T(\mathrm{He}(\mathcal{M}) \otimes PBK_1)e_1 \\ &-e_2^T(\mathrm{He}(\mathcal{L}) \otimes PBK_2FE_s)e_1 - e_2^T(\mathrm{He}(\mathcal{L}) \otimes PBK_2)\delta \\ &\le e_2^T(I_N \otimes \mathrm{He}(P(A - BK_x)))e_2 + k_5\rho_4^{-1}\omega^T\omega \\ &-e_2^T(I_N \otimes PBR^{-1}B^TP)e_2 \\ &+\tfrac{1}{2}\rho_1 k_1^2 e_2^T e_2 + \tfrac{1}{2}\rho_1^{-1}k_3^2\delta^T\delta + \tfrac{1}{2}\rho_2 k_1^2 e_2^T e_2 + \tfrac{1}{2}\rho_2^{-1}k_2^2 e_1^T e_1 \\ &+k_4\rho_3\lambda^2_{\max}(\mathcal{M})e_2^T e_2 + k_4\rho_3^{-1}e_1^T e_1 + k_5\rho_4\lambda^2_{\max}(\mathcal{M})e_2^T e_2 \\ &\le -\lambda_{\min}(Q_2)e_2^T e_2 + \tfrac{1}{2}\rho_1^{-1}k_3^2\delta^T\delta \\ &+(\tfrac{1}{2}\rho_2 k_1^2 + k_4\rho_3\lambda^2_{\max}(\mathcal{M}) + k_5\rho_4\lambda^2_{\max}(\mathcal{M}))e_2^T e_2 \\ &+(\tfrac{1}{2}\rho_2^{-1}k_2^2 + k_4\rho_3^{-1})e_1^T e_1 + k_5\rho_4^{-1}\omega^T\omega \end{aligned} \tag{21}$$

where $K_2 = \tilde{\tau}R^{-1}B^TPC^\dagger$ with the fine-tuning scalar $\tilde{\tau} \ge \lambda_2^{-1}(\mathrm{He}(\mathcal{L}))$, $k_1 = \|PBR^{-1}B^TP\|, k_2 = \|C^\dagger FE_s\|, k_3 = \|C^\dagger\|, k_4 = \|PBK_1\|, k_5 = \|P\|$, and $\rho_i > 0, i = 1, \cdots, 4$.

© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Vehicular Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TVT.2024.3406608

Furthermore, $\mathrm{He}(P(A-K_x)) - PBR^{-1}B^TP + \frac{1}{2}\rho_1 k_1^2 I_3 < -Q_2$ is derived according to the matrix inequality (17) and ARE constraint $\mathrm{He}(PA) - PBR^{-1}B^TP + Q_1 = 0$.

According to the proposed distributed interaction information and sensor fault estimation, it follows that

$$\begin{aligned}&\|\textstyle\sum_{i=1}^N \sum_{j\in\mathcal{N}_i} a_{ij}(\tilde{y}_j(t) - \tilde{y}_i(t))\| - \|(\mathcal{L}\otimes F)\hat{f}_s(t)\| \\ &\le \lambda_N(\mathcal{L})(\|\delta(t)\| + k_3^{-1}\|e_2(t)\| + k_2k_3^{-1}\|e_1(t)\|)\end{aligned} \tag{22}$$

where $\hat{f}_s(t) = \mathrm{col}(\hat{f}_{si}(t))$.

Since the output interaction error $\delta_i(t)$ and event-triggered mechanism $\|\delta_i(t)\| \le \theta_i(\|\sum_{j\in\mathcal{N}_i} a_{ij}(\tilde{y}_j(t) - \tilde{y}_i(t))\| - \|F\sum_{j\in\mathcal{N}_i} a_{ij}(\hat{f}_{sj}(t) - \hat{f}_{si}(t))\|)$ holds in (15) during the dormancy interval $\Gamma^d(t_0,t)$ of hostile DoS attacks, the quadratic output interaction error norm is given as

$$\delta^T(t)\delta(t) \le \frac{2\bar{\theta}^2\lambda_N^2(\mathcal{L})(k_3^{-2}e_2^T(t)e_2(t) + k_2^2k_3^{-2}e_1^T(t)e_1(t))}{1-2\bar{\theta}^2\lambda_N^2(\mathcal{L})} \tag{23}$$

where the upper bound $\bar{\theta} = \max_{i=1,\cdots,N} \theta_i \in (0, \frac{\sqrt{2}}{2}\lambda_N^{-1}(\mathcal{L}))$.

Then, an ingenious combination is equivalent to

$$\begin{aligned}&\dot{V}_1 \le -\lambda_{\min}(Q_2)e_2^Te_2 + \tfrac{1}{2}\rho_1^{-1}k_3^2\delta^T\delta \\ &+(\tfrac{1}{\mu_1} + \tfrac{1}{\mu_2} + \tfrac{1}{\mu_3})\lambda_{\min}(Q_2)e_2^Te_2 \\ &+(\tfrac{\mu_1k_1^2k_2^2}{4\lambda_{\min}(Q_2)} + \tfrac{\mu_2k_4^2\lambda_{\max}^2(\mathcal{M})}{\lambda_{\min}(Q_2)})e_1^Te_1 + \tfrac{\mu_3k_5^2\lambda_{\max}(\mathcal{M})}{\lambda_{\min}(Q_2)}\omega^T\omega \\ &\le (-\bar{\mu}_1\lambda_{\min}(Q_2) + \tfrac{2\bar{\theta}^2\lambda_N^2(\mathcal{L})}{2\rho_1(1-2\bar{\theta}^2\lambda_N^2(\mathcal{L}))})e_2^Te_2 + \tfrac{\mu_3k_5^2\lambda_{\max}(\mathcal{M})\omega^T\omega}{\lambda_{\min}(Q_2)} \\ &+(\tfrac{\mu_1k_1^2k_2^2}{4\lambda_{\min}(Q_2)} + \tfrac{\mu_2k_4^2\lambda_{\max}^2(\mathcal{M})}{\lambda_{\min}(Q_2)} + \tfrac{2\bar{\theta}^2k_2^2\lambda_N^2(\mathcal{L})}{2\rho_1(1-2\bar{\theta}^2\lambda_N^2(\mathcal{L}))})e_1^Te_1 \\ &\le -\alpha_1\lambda_{\max}(P)e_2^Te_2 + \tfrac{\mu_3k_5^2\lambda_{\max}^2(\mathcal{M})}{\lambda_{\min}(Q_2)}\omega^T\omega \\ &+(\tfrac{\mu_1k_1^2k_2^2}{4\lambda_{\min}(Q_2)} + \tfrac{\mu_2k_4^2\lambda_{\max}^2(\mathcal{M})}{\lambda_{\min}(Q_2)} + \tfrac{2\bar{\theta}^2k_2^2\lambda_N^2(\mathcal{L})}{2\rho_1(1-2\bar{\theta}^2\lambda_N^2(\mathcal{L}))})e_1^Te_1\end{aligned} \tag{24}$$

where each scalar $\rho_2 = \frac{2\lambda_{\min}(Q_2)}{\mu_1k_1^2}, \rho_3 = \frac{\lambda_{\min}(Q_2)}{\mu_2k_4\lambda_{\max}^2(\mathcal{M})}, \rho_4 = \frac{\lambda_{\min}(Q_2)}{\mu_3k_5\lambda_{\max}^2(\mathcal{M})}$ with $\mu_i > 0, i = 1,2,3$, $\bar{\mu}_1 = 1 - \frac{1}{\mu_1} - \frac{1}{\mu_2} - \frac{1}{\mu_3}$ and $\alpha_1 \le \frac{\bar{\mu}_1\lambda_{\min}(Q_2)}{\lambda_{\max}(P)} - \frac{2\bar{\theta}^2\lambda_N^2(\mathcal{L})}{2\rho_1(1-2\bar{\theta}^2\lambda_N^2(\mathcal{L}))\lambda_{\max}(P)}$.

Subsequently, consider a second Lyapunov function $V_2(t)$,

$$V_2(t) = \frac{e_1^T(t)e_1(t)}{\varepsilon_1} + \frac{\dot{f}_a^T(t)\dot{f}_a(t)}{\varepsilon_2} + \frac{\dot{f}_s^T(t)\dot{f}_s(t)}{\varepsilon_3} \tag{25}$$

where $\varepsilon_i > 0, i = 1,2,3$ and $f_a(t) = \mathrm{col}(f_{ai}(t))$.

With the definition of the exponential faults of the sensors and actuators (4) in the output and input channels, the correlation between the first- and second-order derivatives of the fault elements $f_{ai}(t)$ and $f_{si}^{\varrho}(t)$ is expressed as

$$\ddot{f}_{ai}(t) = -\epsilon_a\dot{f}_{ai}(t), \ddot{f}_{si}^{\varrho}(t) = -\epsilon_s^{\varrho}\dot{f}_{si}^{\varrho}(t), \varrho = 1,2 \tag{26}$$

Then, it follows that

$$\begin{aligned}&\dot{V}_2 \le \tfrac{1}{\varepsilon_1}e_1^T(I_N\otimes(\mathrm{He}(W) + \Theta\Theta^T))e_1 \\ &\quad+\tfrac{1}{\varepsilon_1}\bar{\omega}^T\bar{\omega} + \tfrac{2}{\varepsilon_2}\dot{f}_a^T\ddot{f}_a + \tfrac{2}{\varepsilon_3}\dot{f}_s^T\ddot{f}_s \\ &\le \tfrac{1}{\varepsilon_1}e_1^T(I_N\otimes(\mathrm{He}(W) + \Theta\Theta^T))e_1 \\ &\quad+(\tfrac{1}{\varepsilon_1} - \tfrac{2\epsilon_a}{\varepsilon_2})\dot{f}_a^T\dot{f}_a + (\tfrac{1}{\varepsilon_1} - \tfrac{2\underline{\epsilon}_s}{\varepsilon_3})\dot{f}_s^T\dot{f}_s + \tfrac{1}{\varepsilon_1}\bar{\omega}^T\bar{\omega}\end{aligned} \tag{27}$$

where $\underline{\epsilon}_s = \min_{\varrho=1,2} \epsilon_s^{\varrho}$.

Finally, $\alpha_1\lambda_{\max}(P) \le \bar{\mu}_1\lambda_{\min}(Q_2) - \frac{2\bar{\theta}^2\lambda_N^2(\mathcal{L})}{2\rho_1(1-2\bar{\theta}^2\lambda_N^2(\mathcal{L}))}$ and $(\frac{\mu_1k_1^2k_2^2+4\mu_2k_4^2\lambda_{\max}^2(\mathcal{M})}{4\lambda_{\min}(Q_2)} + \frac{2k_2^2\bar{\theta}^2\lambda_N^2(\mathcal{L})}{2\rho_1(1-2\bar{\theta}^2\lambda_N^2(\mathcal{L}))})I_6 + \frac{1}{\varepsilon_1}(\mathrm{He}(W) + \Theta\Theta^T) + \frac{\alpha_1}{\varepsilon_1}I_6 < 0$ are intuitively obtained from (18) and the upper bound constraint of α_1. Then, under the derived inequalities $\frac{\alpha_1}{\varepsilon_2} + \frac{1}{\varepsilon_1} - \frac{2\epsilon_a}{\varepsilon_2} \le 0$ and $\frac{\alpha_1}{\varepsilon_3} + \frac{1}{\varepsilon_1} - \frac{2\underline{\epsilon}_s}{\varepsilon_3} \le 0$ from (19), it is derived that

$$\begin{aligned}&\dot{V}_1 + \dot{V}_2 \le -\alpha_1\lambda_{\max}(P)e_2^Te_2 - \alpha_1V_2 \\ &+(\tfrac{\alpha_1}{\varepsilon_2} + \tfrac{1}{\varepsilon_1} - \tfrac{2\epsilon_a}{\varepsilon_2})\dot{f}_a^T\dot{f}_a + (\tfrac{\alpha_1}{\varepsilon_3} + \tfrac{1}{\varepsilon_1} - \tfrac{2\underline{\epsilon}_s}{\varepsilon_3})\dot{f}_s^T\dot{f}_s \\ &+(\tfrac{1}{\varepsilon_1} + \tfrac{\mu_3k_5^2\lambda_{\max}^2(\mathcal{M})}{\lambda_{\min}(Q_2)})\omega^T\omega \le -\alpha_1(V_1 + V_2)\end{aligned} \tag{28}$$

where $\mu_3 \le -\frac{\lambda_{\min}(Q_2)}{\varepsilon_1k_5^2\lambda_{\max}^2(\mathcal{M})}$ is set manually.

Case II: DoS attack activation without event triggering

Given that the adjacency interaction or sensor fault estimation cannot be efficiently transmitted during the activation interval $\Gamma^a(t_0,t)$ of aperiodic DoS attacks, its original design of interaction error-based event-triggered threshold function (15) does not necessarily hold. The corresponding FTCC scheme based on locally estimated information compensation for a non-event-triggered policy is modified as $u_i(t) = -K_1\hat{\hat{x}}_i(t)$ in a decentralized fashion, and the mean-square platoon consensus error systems are rewritten as $\dot{e}_2(t) = (I_N\otimes(A - BK_x))e_2(t) + (\mathcal{M}\otimes BK_1)e_1(t) + (\mathcal{M}\otimes I_4)\omega(t)$.

Consider the same Lyapunov functions $V_1(t)$ and $V_2(t)$ followed in Case I, and it is obtained that

$$\begin{aligned}&\dot{V}_1 \le e_2^T(I_N\otimes\mathrm{He}(P(A - BK_x)))e_2 + k_4\rho_3\lambda_{\max}^2(\mathcal{M})e_2^Te_2 \\ &\quad+k_4\rho_3^{-1}e_1^Te_1 + k_5(\rho_4\lambda_{\max}^2(\mathcal{M})e_2^Te_2 + \rho_4^{-1}\omega^T\omega) \\ &\le -\bar{\mu}_2\lambda_{\min}(Q_2 - PBR^{-1}B^TP + \tfrac{1}{2}\rho_1k_1^2I_3)e_2^Te_2 \\ &\quad+\tfrac{\mu_4k_4^2\lambda_{\max}^2(\mathcal{M})}{\lambda_{\min}(\bar{Q}_2)}e_1^Te_1 + \tfrac{\mu_5k_5^2\lambda_{\max}^2(\mathcal{M})}{\lambda_{\min}(\bar{Q}_2)}\omega^T\omega \\ &\le \alpha_2\lambda_{\min}(P)e_2^Te_2 + \tfrac{\mu_4k_4^2\lambda_{\max}^2(\mathcal{M})}{\lambda_{\min}(\bar{Q}_2)}e_1^Te_1 + \tfrac{\mu_5k_5^2\lambda_{\max}^2(\mathcal{M})}{\lambda_{\min}(\bar{Q}_2)}\omega^T\omega\end{aligned} \tag{29}$$

where $\alpha_2\lambda_{\min}(P) \ge -\bar{\mu}_2\lambda_{\min}(\bar{Q}_2)$ is obtained with the lower bound constraint of scalar α_2 and $\bar{Q}_2 = Q_2 - PBR^{-1}B^TP + \frac{1}{2}\rho_1k_1^2I_3, \rho_3 = \frac{\lambda_{\min}(\bar{Q}_2)}{\mu_4k_4^2\lambda_{\max}^2(\mathcal{M})}, \rho_4 = \frac{\lambda_{\min}(\bar{Q}_2)}{\mu_5k_5^2\lambda_{\max}^2(\mathcal{M})}$ with $\mu_4 > 0, \mu_5 > 0$, and $\bar{\mu}_2 = 1 - \frac{1}{\mu_4} - \frac{1}{\mu_5}$.

Then, $\frac{\mu_4k_4^2\lambda_{\max}^2(\mathcal{M})}{\lambda_{\min}(\bar{Q}_2)}I_6 + \frac{1}{\varepsilon_1}(\mathrm{He}(W) + \Theta\Theta^T) - \frac{\alpha_2}{\varepsilon_1}I_6 < 0$ is also derived from (18). Under another inequalities $-\frac{\alpha_2}{\varepsilon_2} + \frac{1}{\varepsilon_1} - \frac{2\epsilon_a}{\varepsilon_2} \le 0, -\frac{\alpha_2}{\varepsilon_3} + \frac{1}{\varepsilon_1} - \frac{2\underline{\epsilon}_s}{\varepsilon_3} \le 0$ (19), it also follows that

$$\begin{aligned}&\dot{V}_1 + \dot{V}_2 \le \alpha_2\lambda_{\min}(P)e_2^Te_2 + \alpha_2V_2 \\ &+(\tfrac{1}{\varepsilon_1} - \tfrac{\alpha_2}{\varepsilon_2} - \tfrac{2\epsilon_a}{\varepsilon_2})\dot{f}_a^T\dot{f}_a + (\tfrac{1}{\varepsilon_1} - \tfrac{\alpha_2}{\varepsilon_3} - \tfrac{2\underline{\epsilon}_s}{\varepsilon_3})\dot{f}_s^T\dot{f}_s \\ &+(\tfrac{1}{\varepsilon_1} + \tfrac{\mu_5k_5^2\lambda_{\max}^2(\mathcal{M})}{\lambda_{\min}(\bar{Q}_2)})\omega^T\omega \le \alpha_2(V_1 + V_2)\end{aligned} \tag{30}$$

where $\mu_5 \le -\frac{\lambda_{\min}(Q_2 - PBR^{-1}B^TP + \frac{1}{2}\rho_1k_1^2I_3)}{\varepsilon_1k_5^2\lambda_{\max}^2(\mathcal{M})}$ is set in advance.

Finally, denote the piecewise Lyapunov function $V(t) = V_d(t)$ for $t \in [t_{r-1}^a + \Delta_{r-1}^a, t_r^a)$, and denote $V(t) = V_a(t)$ for $[t_r^a, t_r^a + \Delta_r^a)$ in Fig. 1. Integrate both sides of $\dot{V}_d \le -\alpha_1V_d$ and $\dot{V}_a \le \alpha_2V_a$ during $t \in [t_{r-1}^a + \Delta_{r-1}^a, t_r^a + \Delta_r^a)$,

$$V(t) \le \left\{\begin{array}{l} e^{-\alpha_1(t-t_{r-1}^a-\Delta_{r-1}^a)}V_d(t_{r-1}^a + \Delta_{r-1}^a) \\ e^{\alpha_2(t-t_r^a)}V_a(t_r^a)\end{array}\right. \tag{31}$$

Notable, $V_d(t_{k_i}^i) \le \frac{\varpi_2}{\varpi_1}V_d(t_{k_i}^{i-})$ and $V_a(t_{k_i}^i) \le \frac{\varpi_2}{\varpi_1}V_a(t_{k_i}^{i-})$ are obtained at each event-triggered instant $t_{k_i}^i$ with $\varpi_1 = \lambda_{\min}(P)$ and $\varpi_2 = \lambda_{\max}(P)$.

© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Vehicular Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TVT.2024.3406608

Subsequently, $V_d(t)$ for $t \in [t^a_{r-1} + \Delta^a_{r-1}, t^a_r)$ and $V_a(t)$ for $t \in [t^a_r, t^a_r + \Delta^a_r)$ are rewritten as

$$\begin{aligned} V_d(t) &\leq \tfrac{\varpi_2}{\varpi_1} e^{-\alpha_1(t-t^a_{r-1}-\Delta^a_{r-1})} V_d(t^{a-}_{r-1} + \Delta^{a-}_{r-1}) \\ &\leq \tfrac{\varpi_2}{\varpi_1} e^{-\alpha_1(t-t^a_{r-1}-\Delta^a_{r-1})} [e^{\alpha_2(t-t^a_{r-1})} V_a(t^a_{r-1})] \\ &\leq (\tfrac{\varpi_2}{\varpi_1})^2 e^{-\alpha_1(t-t^a_{r-1}-\Delta^a_{r-1})} e^{\alpha_2(t-t^a_{r-1})} V_d(t^{a-}_{r-1}) \leq \\ &\cdots \leq e^{\ln(\frac{\varpi_2}{\varpi_1}) N_{\Gamma^a}(t_0,t)} e^{-\alpha_1|\Gamma^d(t_0,t)|+\alpha_2|\Gamma^a(t_0,t)|} V_d(t_0) \end{aligned} \tag{32}$$

$$V_a(t) \leq e^{\ln(\frac{\varpi_2}{\varpi_1}) N_{\Gamma^a}(t_0,t) - \alpha_1|\Gamma^d(t_0,t)| + \alpha_2|\Gamma^a(t_0,t)|} V_a(t_0) \tag{33}$$

It then follows from Definitions 2.1-2.4 that $|\Gamma^d(t_0,t)| = t - t_0 - |\Gamma^a(t_0,t)|$ with $\Gamma^a(t_0,t) \leq \Gamma_0 + \frac{t-t_0}{\tau_a}$, where τ_a and Γ_0 are denoted as the ADT indicator and chattering bound, respectively. Based on the constraint condition of DoS attack frequency $\mathcal{F}_{\Gamma^a}(t_0,t) = \frac{N_{\Gamma^a}(t_0,t)}{t-t_0} \leq \frac{\sigma^*}{\ln(\frac{\varpi_2}{\varpi_1})}$ and ADT indicator $\tau_a > \frac{\alpha_1+\alpha_2}{\alpha_1-\sigma^*}$ in (20), for $\forall t \geq t_0$, it follows that

$$\begin{aligned} &V(t) \\ &\leq e^{(\alpha_1+\alpha_2)\Gamma_0 + \ln(\frac{\varpi_2}{\varpi_1}) N_{\Gamma^a}(t_0,t) + (\frac{\alpha_1+\alpha_2}{\tau_a} - \alpha_1)(t-t_0)} V(t_0) \\ &\leq e^{(\alpha_1+\alpha_2)\Gamma_0 - \alpha_1(t-t_0) + \frac{\alpha_1+\alpha_2}{\tau_a}(t-t_0) + \sigma^*(t-t_0)} V(t_0) \\ &= e^{(\alpha_1+\alpha_2)\Gamma_0} e^{-\lambda_\Gamma(t-t_0)} V(t_0) \end{aligned} \tag{34}$$

where the decay rate is denoted as $\lambda_\Gamma = \alpha_1 - \frac{\alpha_1+\alpha_2}{\tau_a} - \sigma^* > 0$ with $\sigma^* \in (0, \alpha_1)$.

Obviously, $V(t) \geq \varpi_1 \|e_{i2}(t)\|^2$ is derived, and the initial Lyapunov expression with t_0 is also derived as

$$V(t_0) \leq (\varpi_2 + \varpi_3) N \|e_{i2}(t_0)\|^2 \tag{35}$$

where $\varpi_3 = \frac{\max\limits_{i=1,\cdots,N} \left\{ \frac{1}{\varepsilon_1}\|e_{i1}(t_0)\|^2 + \frac{1}{\varepsilon_2}\|\dot{f}_{ai}(t_0)\|^2 + \frac{1}{\varepsilon_3}\|\dot{f}_{si}(t_0)\|^2 \right\}}{\min\limits_{i=1,\cdots,N} \|e_{i2}(t_0)\|^2}$.

Finally, introduce an appropriate scalar $\eta_\Gamma > 0$. Hence, the mean-square consensus control property of the platoon vehicles is exponentially achieved with the platoon consensus error,

$$\begin{aligned} &\|e_{i2}(t)\|^2 \\ &\leq \varpi_1^{-1} e^{(\alpha_1+\alpha_2)\Gamma_0} (\varpi_2 + \eta_\Gamma) N e^{-\lambda_\Gamma(t-t_0)} \|e_{i2}(t_0)\|^2 \\ &= \mu_\Gamma e^{-\lambda_\Gamma(t-t_0)} \|e_{i2}(t_0)\|^2 \end{aligned} \tag{36}$$

with the amplitude $\mu_\Gamma = \varpi_1^{-1} e^{(\alpha_1+\alpha_2)\Gamma_0} (\varpi_2 + \eta_\Gamma) N$ and the decay rate $\lambda_\Gamma = \alpha_1 - \tau_a^{-1}(\alpha_1 + \alpha_2) - \sigma^*$.

Hence, all approximations $\|e_{i2}(t)\| \to \|e_{i2}(t_0)\|$, $x_i \to \hat{x}_i, f_{ai}(t) \to \hat{f}_{ai}, f_{si}(t) \to \hat{f}_{si}$ and $x_i \to \frac{1}{N}\sum_{i=1}^N x_i$ are eventually obtained as $t \to +\infty$ with the derived amplitude $\mu_\Gamma > 0$ and decay rate $\lambda_\Gamma > 0$ in (36). This indicates that the mean-square consensus control objective of the platoon vehicles is exponentially achieved with safe collision avoidance through the event-triggered distributed FTCC strategy. The proof is ultimately finalized.

Remark 3.2: The detailed calculation of the event-triggered distributed FTCC strategy of vehicle platoon systems is briefly illuminated in Algorithm 1.

Remark 3.3: At the triggering events $\{t^i_{k_i}\}_{k_i \in \mathbb{N}}$, a Zeno behavior is effectively excluded by determining the following updated control time sequence,

$$t^i_{k_i+1} = \begin{cases} t^i_{k_i} + \chi_i, \text{ if } k_i \in \{(i,k_i) \in \nu \times \mathbb{N} \mid t^i_{k_i} \in \cup_{r\in\mathbb{N}} \Gamma^a_r\} \\ t^i_{k_i} + \Delta^z_{k_i}, \text{ otherwise} \end{cases} \tag{38}$$

where interexecution $\Delta^z_{k_i} = \max\{\inf_{t > t^i_{k_i}} \{t - t^i_{k_i} \mid \|\delta_i(t)\| = \theta_i\|\sum_{j\in\mathcal{N}_i} a_{ij}(\tilde{y}_j(t) - \tilde{y}_i(t))\| - \theta_i\|F\sum_{j\in\mathcal{N}_i} a_{ij}(\hat{f}_{sj}(t) - \hat{f}_{si}(t))\|\}, \upsilon_i\}$ is enforced with $\chi_i > 0$ and $\upsilon_i > 0$.

Algorithm 1 Event-triggered distributed FTCC.

```
1: Solving an ARE: $\mathrm{He}(PA) - PBR^{-1}B^TP + Q_1 = 0$ to get the symmetric positive-definite matrix $P$ and positive-definite matrices $Q_1, R$.
2: Solving the linear matrix inequality: $-Q_1 - \mathrm{He}(PBK_x) + \frac{1}{2}\rho_1 k_1^2 I_3 + Q_2 < 0$ (17) to get the positive-definite matrix $Q_2$ and matrix $K_x$.
3: Solving the following linear matrix inequality:
   $\begin{bmatrix} \Omega_{11} & \Omega_{12} & \Omega_{13} & \Omega_{14} & \mathbf{0}_{3\times1} & -H_1F \\ \star & \Omega_{22} & \Omega_{23} & -H_2C & 1 & -H_2F \\ \star & \star & \Omega_{33} & -H_3C & \mathbf{0}_{2\times1} & \Omega_{36} \\ \star & \star & \star & -I_4 & \mathbf{0}_{4\times1} & \mathbf{0}_{4\times2} \\ \star & \star & \star & \star & -1 & \mathbf{0}_{1\times2} \\ \star & \star & \star & \star & \star & -I_2 \end{bmatrix} < 0 \quad (37)$
   to obtain the estimation matrices $H = [H_1^T \ H_2^T \ H_3^T]^T$ and $J = [J_1^T \ J_2^T \ J_3^T]^T$ in (18) with $\Omega_{11} = \mathrm{He}(A - H_1CA - J_1C) - \xi I_3, \Omega_{12} = B - H_1CB - A^TC^TH_2^T - C^TJ_2^T, \Omega_{13} = -J_1F - A^TC^TH_3^T - C^TJ_3^T, \Omega_{14} = I_3 - H_1C, \Omega_{22} = \mathrm{He}(-H_2CB) - \xi, \Omega_{23} = -J_2F - B^TC^TH_3^T, \Omega_{33} = \mathrm{He}(-J_3F) - \xi I_2, \Omega_{36} = I_2 - H_3F$.
4: The compensation-based gain and the interaction-based gain are calculated as $K_1 = [K_x \ 1 \ \mathbf{0}_{1\times2}]$ and $K_2 = \tilde{\tau}R^{-1}B^TPC^\dagger$ with $\tilde{\tau} \geq \lambda_2^{-1}(\mathrm{He}(\mathcal{L}))$ in the proposed distributed FTCC mechanism (11), and each threshold is designed as $\theta_i \in (0, \frac{\sqrt{2}}{2}\lambda_N^{-1}(\mathcal{L}))$ in the even-triggered control mechanism (15).
```

Hence, the event-triggered dormancy is set as $\cup_{r\in\mathbb{N}}[t^a_r, t^a_r + \Delta^a_r + \Delta^z_r)$ under each positive upper interexecution bound Δ^z_r.

Remark 3.4: In the threshold setting of the event-triggered function (15), a static event-triggered mechanism with the positive pre-defined threshold $\theta_i \in (0, \frac{\sqrt{2}}{2}\lambda_N^{-1}(\mathcal{L}))$ is used and even suitable for the special case of DoS attacks occurring at the triggering time instants, thus eliminating the requirement for periodic sampling of neighborhood information and instead effectively distributing the application of the latest successfully triggered interaction information.

Remark 3.5: A remarkable constraint involves the tradeoff between the convergence attenuation rates α_1 and α_2 of the mean-square consensus index, the uniform maximum threshold of attack frequency $\mathcal{F}_{\Gamma^a}(t_0,t)$, and the bottom limit of ADT τ_a of aperiodic DoS attacks. The result illustrates that, under sufficient conditions of attack frequency and ADT indicator, by using the proposed distributed event-triggered FTCC algorithm with anti-attack capabilities, the platoon systems can finally reach an exponential consensus. Furthermore, in contrast to the adaptive self-triggered [16] and time-dependent distributed event-triggered [35] strategies, an essentially constant threshold-based static event-triggered mechanism is employed through effectively utilizing distributed adjacency values (including output interaction and sensor fault estimation errors), thereby simply updating event triggers that lie within the

© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Vehicular Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TVT.2024.3406608

dormancy intervals of DoS attacks. The problem of confusing the dynamic nature of the bandwidth-aware event-triggered scheduling mechanism [36] with the intermittence of DoS attacks is avoided without effective discrimination.

IV. Simulation and Experiment Results

The five automatous vehicles in sequence are given in this section of platoon vehicles. Comparative vehicle platoon simulations and experiments in the short-cycle and long-cycle DoS attack scenarios are proposed to confirm the effectiveness of the event-triggered distributed FTCC algorithm.

The parameter values of the engine index and the vehicle length are chosen as $\tau = 0.1$ and $L = 2\text{m}$ in [34], respectively. The external disturbances in the five homogeneous vehicle channels are listed as $d_0^v(t) = d_1^v(t) = 0.03\cos 0.07\pi t\text{m.s}^{-2}$, $d_0^a(t) = d_1^a(t) = 0.05\sin 0.05\pi t\text{m.s}^{-2}$, $d_2^v(t) = d_3^v(t) = 0.02\cos 0.1\pi t\text{m.s}^{-2}$, $d_2^a(t) = d_3^a(t) = 0.03\cos 0.7\pi t\text{m.s}^{-2}$, $d_4^v(t) = 0.01\sin 0.02\pi t\text{m.s}^{-2}$, and $d_4^a(t) = 0.04\cos 0.03\pi t\text{m.s}^{-2}$.

The distinguishable boundaries of the healthy and faulty actuators or sensors are set as $\underline{\epsilon}_a = 0.002$ and $\underline{\epsilon}_s^1 = \underline{\epsilon}_s^2 = 0.001$. The sensor fault-induced gain is set as $F = [0.8\ 0; 0\ 0]$, and the actuator and sensor faults $f_{ai}(t)$ and $f_{si}(t)$ of the initial and subsequent vehicles are given as

$$\begin{aligned} &f_{a1}(t) = 0.05(1 - e^{-0.08t})\text{m/s}^2, 15\text{s} \le t \le 25\text{s} \\ &f_{s2}^1(t) = \begin{cases} 0.1(1 - e^{-0.5t})\text{m}, 15\text{s} \le t < 25\text{s} \\ 0.01(1 - e^{-0.05t})\text{m}, 25\text{s} \le t \le 40\text{s} \end{cases} \end{aligned} \tag{39}$$

The gain matrices in the UIO (8) and FTCC controller (11) are computed as

$$\begin{aligned} J &= \begin{bmatrix} 0.0923 & -0.0018 \\ -0.0045 & -0.0037 \\ -0.7005 & -0.0947 \\ -0.0025 & 1.2484 \\ 0.0125 & -2.1334 \\ 1.2921 & -49.0975 \end{bmatrix}, H = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0.8332 & 0.0597 \end{bmatrix}, \\ K_1 &= \begin{bmatrix} 6.6857 & 0.0762 & -6.5838 & 1 & 0 & 0 \end{bmatrix}, \\ K_2 &= \begin{bmatrix} 0.8445 & -16.3633 \end{bmatrix} \end{aligned} \tag{40}$$

Despite the involved incipient and abrupt actuator and sensor faults in the initial and subsequent vehicles, Fig. 3 - Fig. 5 in the simulation part provide the typical studies of the platoon vehicles under short-cycle aperiodic DoS attacks to confirm the viability and merit of the event-triggered distributed FTCC solution in preserving the desired platoon performance, fault tolerance, and attack resilience. Fig. 3 depicts the spacing metrics of the vehicle platoon systems for short-cycle aperiodic DoS activation periods (10s-11s, 21s-22s, 30s-31s, and 38s-40s) after simultaneous faults (15s and 25s) to balance the ideal spacing and prevent vehicle scraping phenomena. Fig. 4 and Fig. 5 illustrate the velocity and acceleration tracking curves over the same aperiodic short-cycle DoS activation periods, thus ensuring a safe platoon performance. Notably, the first vehicle suffers from an incipient bias fault at 15s and the second vehicle deals with composite incipient-/abrupt-type sensor faults at 15s and 25s, respectively, resulting in an oscillation phenomenon of the spacing, velocity, and acceleration response channels. The faults and attacks occur at different moments and provide different durations with individual nodes, finally resulting in staggered oscillations in the vehicle platoon consensus error responses. Hence, the platoon consensus control problem of the modeled cyber-physical platoon vehicle dynamics is effectively solved with the proposed event-triggered distributed FTCC mechanism.

The experimental testing platform in our lab (Fig. 6) consists of four main components: the ground control station, five

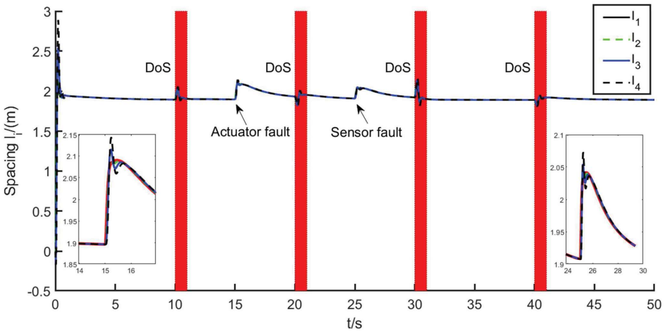

Fig. 3. The spacing $l_i, i = 1, \cdots, 4$ in the short-cycle DoS attack scenario.

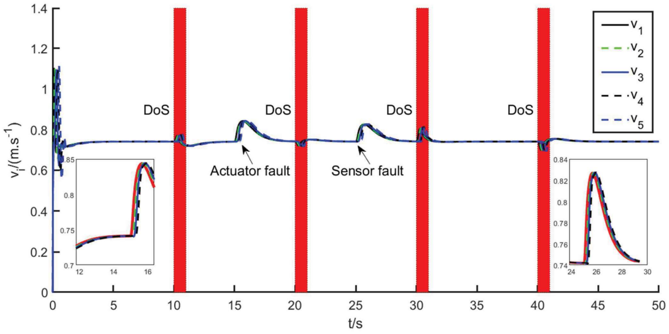

Fig. 4. Velocity tracking in the short-cycle DoS attack scenario.

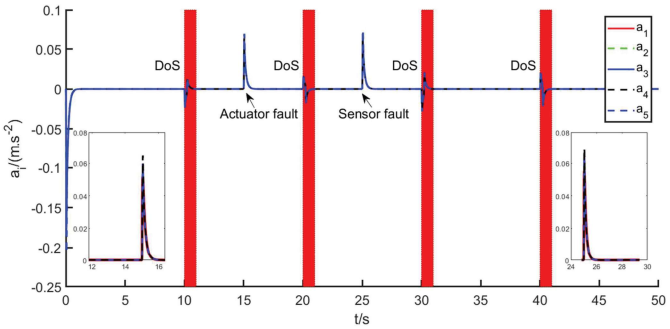

Fig. 5. Acceleration tracking in the short-cycle DoS attack scenario.

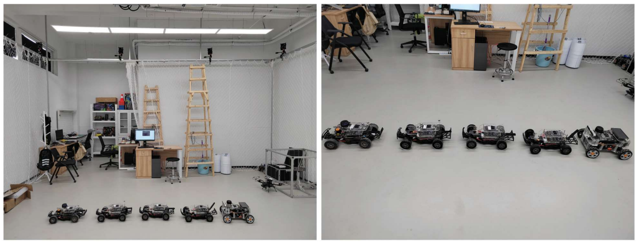

Fig. 6. The experimental testing platform.

© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Vehicular Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TVT.2024.3406608

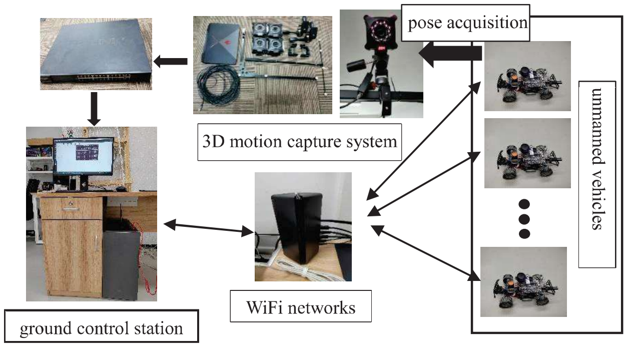

Fig. 7. The major components in the vehicle platoon platform.

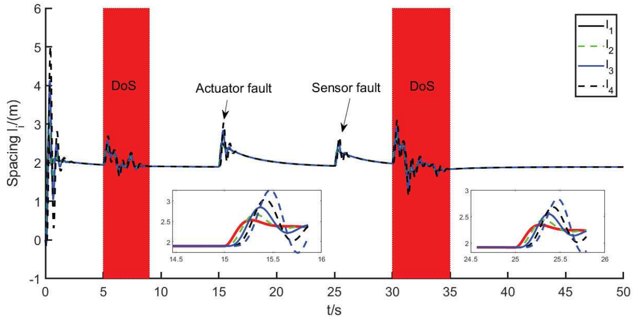

Fig. 8. The spacing $l_i, i = 1, \cdots, 4$ in the long-cycle DoS attack scenario.

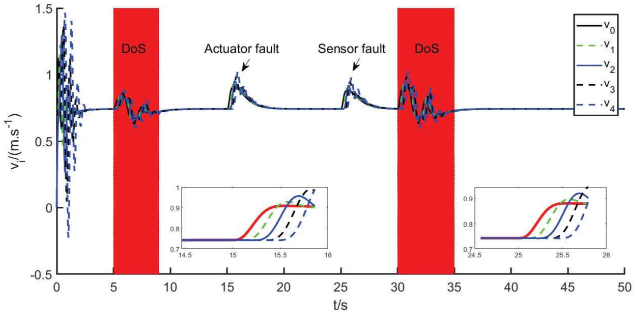

Fig. 9. Velocity tracking in the long-cycle DoS attack scenario.

unmanned vehicles, Nokov optical 3D motion capture system, and WiFi-based wireless communication network, as shown in Fig. 7. The vehicle positions are collected by the motion capture system, which envelops the entire capture area of the indoor space utilizing motion capture cameras arranged within the space, capturing the precise three-dimensional spatial position of reflective markers placed on the captured subject. This provides real-time information about the current position and posture of the unmanned vehicles. The wireless network created using the XIAOMI-AX3000 wireless router enables communication between the ground control station and unmanned vehicles with a strong wireless signal and anti-interference capability, operating at a frequency band of 2.4GHz. The ROS operating system used by unmanned vehicles provides many standard tools and libraries for building unmanned vehicle software and is designed as a distributed system using the standard TCP/IP protocol for communication between unmanned vehicles. Multiple ROS-based unmanned vehicles are configured in the same local area network on our experimental platform, with a host ROS master and several following nodes. Each unmanned vehicle interacts through publishing and subscribing, with different topics being used to specify network routing for messages. Messages are published by nodes in the network to the appropriate topic, and the vehicle nodes subscribe to the corresponding topic to obtain the required messages. Considering the reliability of network transmission during the experimental process, it is difficult to simulate short-period DoS attack intervals in real-time. Therefore, the long-cycle attack interval is chosen. Fig. 8 - Fig. 10 in the experiment part illustrate the platoon consensus performance of the platoon vehicles for the long-cycle DoS attack activation period (5s-9s and 30s-35s). The mean-square exponential consensus control problem for the five networked vehicles is effectively solved using a co-designed structure of the UIO scheme in decentralized fault-estimation and FTCC scheme in distributed anti-DoS-attack improvements. Regardless of the short-cycle and long-cycle DoS conditions, the consensus tracking for each spacing, velocity, and acceleration exhibits an excellent physical fault tolerance at each occurring instant of abrupt and incipient sensor and actuator faults, and network resilience at each DoS attack activation duration. However, compared to the smooth response and equal amplitude tracking under short-cycle DoS duration in Fig. 3 - Fig. 5, respectively, the response under the long-cycle DoS impacts in Fig. 8 - Fig. 10 retains a greater oscillation amplitude with denser fluctuations and more intense spikes, as well as a faster event update frequency, i.e., the wider DoS activation periods lead to denser triggering events for the remaining DoS dormancy periods. Furthermore, a platoon consisting of five interconnected vehicles is formed for a circular trajectory formation experiment. The experiment introduced long-cycle DoS attacks and compound actuator and sensor faults. For better observation, Fig. 11 only displays the trajectory of the middle vehicle in the platoon. During the periods of long-cycle DoS attacks (5s-9s and 30s-35s), the red curve (distributed FTCC algorithm) and the blue curve (distributed security algorithm [31]) exhibit similar tracking effects, indicating that both algorithms provide better network resilience against DoS attacks. In contrast, compared to the blue curve (without fault-tolerant modules, showing significant trajectory deviation), our distributed FTCC algorithm demonstrates better tracking speed and stability when faced with compound faults (15s and 25s), smoothly and quickly converging to the reference trajectory.

The triggering occurrences of the events in the respective short-cycle and long-cycle DoS attack scenarios are illustrated in Figs. 12 and 13, respectively. Notably, the event-triggering moments circumvent all possible DoS activation intervals and are triggered more frequently during the FTCC periods. In addition, the comparison curves in Fig. 14 and Fig. 15 reveal the superiority of the UIO protocol in decentralized fault-estimation design and provide a guideline for devising the back-end distributed anti-DoS-attack FTCC algorithm. To be specific, Fig. 14 depicts the estimated and rated curves of the incipient actuator fault $f_{a1}(t)$ at 15s. Fig. 15 illustrates

© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Vehicular Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TVT.2024.3406608

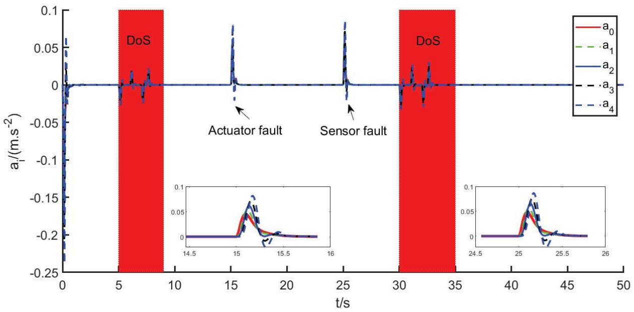

Fig. 10. Acceleration tracking in the long-cycle DoS attack scenario.

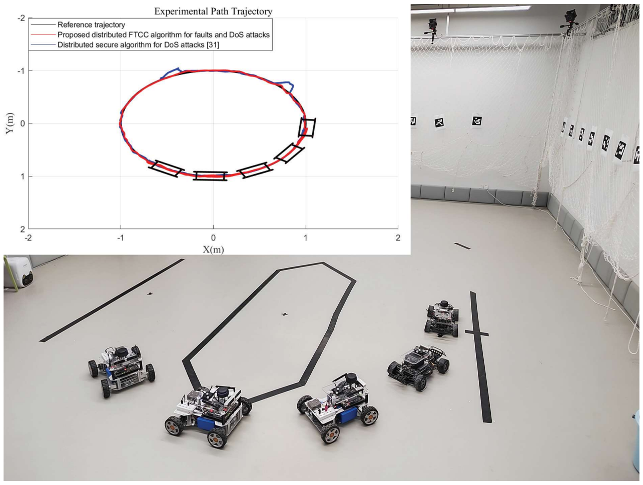
Experimental Path Trajectory
Reference trajectory
Proposed distributed FTCC algorithm for faults and DoS attacks
Distributed secure algorithm for DoS attacks [31]
Y(m)
X(m)
-2
-1
0
1
2

Fig. 11. Comparison experiment of path trajectories between distributed FTCC algorithm and distributed security control algorithm [31].

the abrupt sensor fault $f_{s2}^{1}(t)$ at 15s and incipient sensor fault at 25s in the second vehicle with rated and estimated curves. Compared with the accurate estimation of the complicated faults using the attack activation rate technique [34], the similarity lies in the fluctuation convergence on each fault moment as the distinguishable attack and fault detection cannot be effectively realized. The difference with the multi-metric evaluation (convergence speed, smoothness, and alignment) focuses on the irregular oscillation that does not track smoothly and quickly to the rated values under incipient faults of tiny and inconspicuous features. In this scenario, the proposed decentralized UIO in fault-estimation and FTCC hierarchy with the dual-constraint indicators (DoS attack frequency and ADT) can realize an accurate estimation of the platoon vehicles despite a continuous deviation or persistent non-dissipative oscillation.

V. Conclusions

A secure framework for the UIO in decentralized fault-estimation and FTCC strategy in a distributed anti-DoS-attack fashion has been developed to address cyber-physical threats in vehicle platoon dynamics, including exponential fault constraints (deviations caused by complicated incipient/abrupt actuator and sensor faults) and disconnected/paralyzed topologies (characteristics of aperiodic DoS attacks). A distributed control scheme based on both fault/state estimation reconstruction and sensing interaction error collection has been proposed for two cases, i.e., DoS attack dormancy with event triggering and DoS attack activation without event triggering. The developed dual criteria of DoS attack fre-

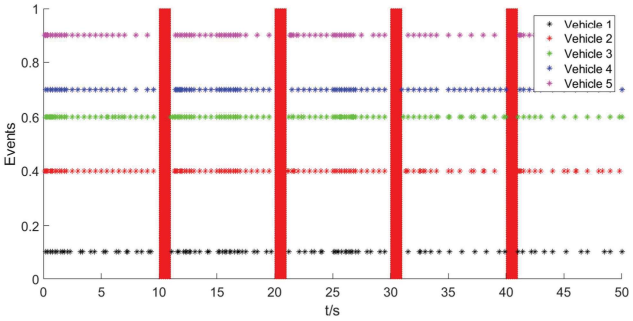

Fig. 12. Occurrences of the events in the short-cycle DoS attack scenario.

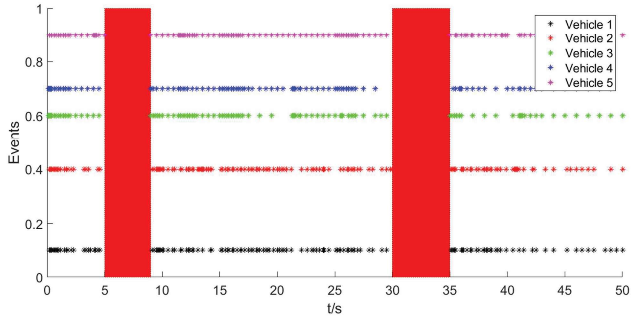

Fig. 13. Occurrences of the events in the long-cycle DoS attack scenario.

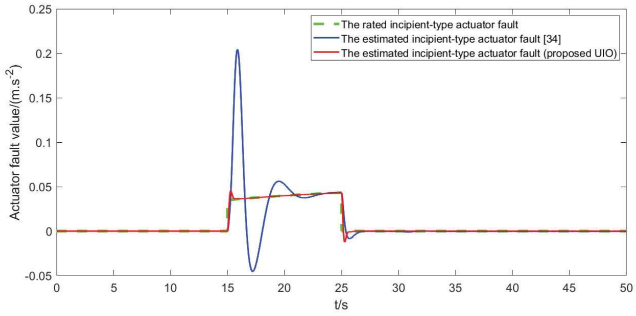

Fig. 14. Rated and estimated values of incipient-type actuator fault $f_{a1}(t)$.

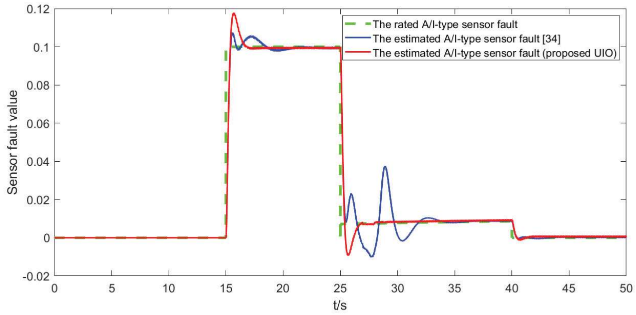

Fig. 15. Rated and estimated values of the complicated abrupt-/incipient-type sensor fault $f_{s2}^{1}(t)$.

© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Vehicular Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TVT.2024.3406608

quency and ADT techniques ensure that the distributed FTCC algorithm maintains the mean-square exponential consensus with the specified attack resistance and fault tolerance performance. Future research focuses on simultaneously solving component/system/task-based faults and deception/random DoS attacks. The novel event-based integration of fault identification, attack detection, and FTCC policies is urgently explored to improve dynamic queue reconfiguration, mission planning, and obstacle avoidance in vehicle platoon systems.

References

[1] 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.

[2] J. C. Zegers, E. S. Kazerooni, J. Ploeg, N. Wouw, and H. Nijmeijer, "Consensus control for vehicular platooning with velocity constraints," *IEEE Trans. Control Syst. Technol.*, vol. 26, no. 5, pp. 1592-1605, 2018.

[3] P. P. Zhu, S. T. Jin, X. H. Bu, and Z. S. Hou, "Distributed data-driven control for a connected heterogeneous vehicle platoon under quantized and switching topologies communication," *IEEE Trans. Veh. Technol.*, vol. 72, no. 8, pp. 9796-9807, 2023.

[4] Y. L. Shao and Z. X. Sun, "Vehicle speed and gear position co-optimization for energy-efficient connected and autonomous vehicles," *IEEE Trans. Control Syst. Technol.*, vol. 29, no. 4, pp. 1721-1732, 2021.

[5] D. Y. Jia, K. J. Lu, J. P. Wang, X. Zhang, and X. M. Shen, "A survey on platoon-based vehicular cyber-physical systems," *IEEE Commun. Surv. Tutor.*, vol. 18, no. 1, pp. 263-284, 2016.

[6] Z. Y. Gao, Y. Zhang, and G. Guo, "Finite-time fault-tolerant prescribed performance control of connected vehicles with actuator saturation," *IEEE Trans. Veh. Technol.*, vol. 72, no. 2, pp. 1438-1448, 2023.

[7] X. G. Guo, W. D. Xu, J. L. Wang, J. H. Park, and H. C. Yan, "BLF-based neuroadaptive fault-tolerant control for nonlinear vehicular platoon with time-varying fault directions and distance restrictions," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 12388-12398, 2022.

[8] L. Y. Hao, P. Li, and G. Guo, "String stability and flow stability for nonlinear vehicular platoons with actuator faults based on an improved quadratic spacing policy," *Nonlinear Dyn.*, vol. 102, pp. 2725-2738, 2020.

[9] D. Ichalal, B. Marx, J. Ragot, S. Mammar, and D. Maquin, "Sensor fault tolerant control of nonlinear Takagi–Sugeno systems. Application to vehicle lateral dynamics," *Int. J. Robust Nonlinear Control*, vol. 26, no. 7, pp. 1376-1394, 2016.

[10] J. L. Lan, D. Z. Zhao, and D. X. Tian, "Data-driven robust predictive control for mixed vehicle platoons using noisy measurement," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 6, pp. 6586-6596, 2023.

[11] W. B. Qin and G. Orosz, "Experimental validation of string stability for connected vehicles subject to information delay," *IEEE Trans. Control Syst. Technol.*, vol. 28, no. 4, pp. 1203-1217, 2020.

[12] J. Y. Wang, X. M. Deng, J. H. Guo, Y. G. Luo, and K. Q. Li, "A fully distributed antiwindup control protocol for intelligent-connected electric vehicles platooning with switching topologies and input saturation," *IEEE-ASME Trans. Mechatron.*, vol. 28, no. 3, pp. 1683-1694, 2023.

[13] S. X. Wen and G. Guo, "Control of leader-following vehicle platoons with varied communication range," *IEEE Trans. Intell. Veh.*, vol. 5, no. 2, pp. 240-250, 2020.

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

[15] J. C. Chen, H. Zhang, and G. D. Yin, "Distributed dynamic event-triggered secure model predictive control of vehicle platoon against DoS attacks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 3, pp. 2863-2877, 2023.

[16] 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.

[17] X. H. Cao, Y. T. Tian, X. W. Ji, and B. Qiu, "Fault-tolerant controller design for path following of the autonomous vehicle under the faults in braking actuators," *IEEE Trans. Transp. Electrif.*, vol. 7, no. 4, pp. 2530-2540, 2021.

[18] 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.

[19] E. Hashemi, M. Pirani, A. Khajepour, B. Fidan, S. Chen, and B. Litkouhi, "Fault-tolerant consensus for vehicle state estimation: a cyber-physical approach," *IEEE Trans. Ind. Inform.*, vol. 15, no. 9, pp. 5129-5138, 2019.

[20] J. H. Han, J. Z. Zhang, C. K. He, X. H. Hou, and Y. Ji, "Distributed finite-time safety consensus control of vehicle platoon with senor and actuator failures," *IEEE Trans. Veh. Technol.*, vol. 72, no. 1, pp. 162-175, 2023.

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

[22] 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.

[23] Y. X. Feng, B. T. Hu, H. Hao, Y. C. Gao, Z. W. Li, and J. R. Tan, "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.

[24] G. Guo, P. Li, and L. Y. Hao, "A new quadratic spacing policy and adaptive fault-tolerant platooning with actuator saturation," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 1200-1212, 2022.

[25] A. Petrillo, A. Pescape, 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. Y. 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.

[27] S. Y. Xiao, X. H. Ge, Q. L. Han, and Y. J. Zhang, "Secure and collision-free multi-platoon control of automated vehicles under data falsification attacks," *Automatica*, vol. 145, 110531, 2022.

[28] X. Jin, W. M. Haddad, Z. P. Jiang, A. Kanellopoulos, and K. G. Vamvoudakis, "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.

[29] R. Merco, F. Ferrante, and P. Pisu, "A hybrid controller for DOS-resilient string-stable vehicle platoons," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 3, pp. 1697-1707, 2021.

[30] Z. Y. Ju, H. Zhang, X. Li, X. G. Chen, J. P. Han, and M. Z. Yang, "A survey on attack detection and resilience for connected and automated vehicles: from vehicle dynamics and control perspective," *IEEE Trans. Intell. Veh.*, vol. 7, no. 4, pp. 815-837, 2022.

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

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

[33] B. H. 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.

[34] C. Liu, J. Zhao, and R. J. Patton, "Distributed anti-attack fault-tolerant tracking control for vehicle platoon systems under cyber-physical threats," *IEEE Trans. Ind. Inform.*, vol. 19, no. 6, pp. 7825-7834, 2023.

[35] G. Y. Wu, G. Chen, H. Zhang, and C. Huang, "Fully distributed event-triggered vehicular platooning with actuator uncertainties," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 6601-6612, 2021.

[36] X. H. Ge, S. Y. Xiao, Q. L. Han, X. M. Zhang, and D. R. Ding, "Dynamic event-triggered scheduling and platooning control co-design for automated vehicles over vehicular Ad-Hoc networks," *IEEE-CAA J. Automatica Sin.*, vol. 9, no. 1, pp. 31-46, 2022.

© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.